Journal officiel
de l'Union européenne

FR
Série L

2026/2394

6.11.2026

RECOMMANDATION (UE) 2026/2394 DE LA COMMISSION

du 29 octobre 2026

relative aux clauses contractuelles types non contraignantes concernant l'accès aux données et l'utilisation des données et aux clauses contractuelles standards non contraignantes pour les contrats d'informatique en nuage

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

vu le règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) [1], et notamment son article 41,

considérant ce qui suit:

(1) Des droits et obligations contractuels équitables sont propices à l'instauration d'un climat de confiance entre les acteurs du marché, peuvent contribuer à améliorer l'accès équitable aux données et l'utilisation équitable des données, et peuvent favoriser un marché plus concurrentiel pour les services de traitement de données, permettant ainsi de tirer pleinement parti d'une économie fondée sur les données dans l'Union.

(2) Afin de répondre aux besoins de l'économie numérique et d'éliminer les obstacles au bon fonctionnement du marché intérieur des données, le règlement (UE) 2023/2854 a établi un cadre harmonisé précisant qui dispose du droit d'utiliser les données relatives au produit ou les données relatives au service connexe, dans quelles conditions et sur quel fondement. L'outil central utilisé à cette fin par le règlement (UE) 2023/2854 est celui des contrats. Depuis l'application dudit règlement, l'utilisation des données n'est plus fondée sur un contrôle de facto des données, mais sur des contrats. L'objectif est de créer une sécurité juridique en ce qui concerne les droits et obligations des parties et, partant, de promouvoir le partage des données. En outre, le règlement (UE) 2023/2854 vise à garantir, au moyen de contrats équilibrés, une part équitable des avantages pour toutes les parties de la chaîne de valeur des données.

(3) Le règlement (UE) 2023/2854 prévoit les droits et obligations applicables aux parties qui interviennent dans l'accès aux données et dans l'utilisation des données, en fixant des règles relatives au partage obligatoire des données, tout en permettant aux parties de déterminer, au moyen de contrats, les modalités pratiques aux fins de l'exercice des droits et obligations respectifs en ce qui concerne l'accès aux données et l'utilisation des données en question.

(4) Les services de traitement de données sont un catalyseur fondamental de la transition numérique et un facteur clé de la compétitivité à l'ère numérique. La capacité d'un client à passer d'un service à un autre, ou à utiliser simultanément les services de plusieurs fournisseurs, est une condition essentielle pour garantir un marché plus concurrentiel dans lequel les barrières à l'entrée seront plus faibles pour les nouveaux fournisseurs. Le règlement (UE) 2023/2854 fixe des règles concernant les droits des clients de passer d'un fournisseur de services de traitement de données à un autre fournisseur ou à une infrastructure sur site, et prévoit des conditions et des procédures spécifiques, qui couvrent également la sécurité et la continuité des activités pendant le processus de changement de fournisseur. Le règlement (UE) 2023/2854 prévoit également l'utilisation simultanée de services de traitement de données multiples, favorisant le succès du déploiement de stratégies multinuages. En outre, le règlement (UE) 2023/2854 prévoit que toutes les parties concernées par un changement de fournisseur doivent coopérer de bonne foi.

(5) Les droits et obligations des clients et des fournisseurs de services de traitement de données sont définis dans les contrats de services de traitement de données. Le règlement (UE) 2023/2854 introduit l'obligation pour les fournisseurs de services de traitement de données de supprimer les obstacles susceptibles d'empêcher les clients de changer de fournisseur, y compris les obstacles contractuels.

(6) Conformément à l'article 41 du règlement (UE) 2023/2854, la Commission est chargée d'élaborer des clauses contractuelles types concernant l'accès aux données et l'utilisation des données, ainsi que des clauses contractuelles standards pour les contrats d'informatique en nuage, en tant qu'outil destiné à aider les parties à négocier et à conclure de tels contrats, ainsi qu'à promouvoir des modèles qui contiennent des droits et obligations contractuels équitables, raisonnables et non discriminatoires.

[1] JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj.

(7) Conformément au règlement (UE) 2023/2854, l'objectif premier de ces modèles est d'aider les entreprises, en particulier les PME, à rédiger, négocier et conclure de tels contrats. Le règlement (UE) 2023/2854 dispose également que, lorsqu'elles seront largement et intégralement utilisées, ces clauses contractuelles types devraient avoir pour effet bénéfique d'influencer la manière dont sont conçus les contrats en ce qui concerne l'accès aux données et l'utilisation des données, et mener ainsi plus généralement à des relations contractuelles plus équitables en matière d'accès aux données et de partage des données.

(8) Ces objectifs montrent que les clauses contractuelles types et les clauses contractuelles standards devraient jouer un rôle important dans l'application du règlement (UE) 2023/2854 et dans la manière dont des contrats équilibrés appliquant le règlement (UE) 2023/2854 pourraient être conçus, y compris pour les juridictions lors de l'application de la clause générale relative au contrôle du caractère abusif prévue par le règlement (UE) 2023/2854. En outre, ainsi que le prévoit le considérant 55 du règlement (UE) 2023/2854, les organes de règlement des litiges devraient tenir compte des clauses contractuelles types afin d'assurer l'application uniforme du règlement.

(9) La liberté contractuelle est un concept essentiel dans les relations interentreprises et, en tant que telle, est couverte par la liberté d'entreprise au titre de la charte des droits fondamentaux de l'Union européenne. La Commission fournit aux acteurs du marché des modèles aux fins de leurs relations contractuelles qui ne sont pas de nature contraignante et, si les parties contractantes choisissent de les utiliser, ces modèles peuvent être adaptés, comme expliqué également à l'annexe I, par l'introduction de clauses types. Ces clauses ont été principalement élaborées pour les relations interentreprises en tenant compte du règlement (UE) 2023/2854 et d'autres actes législatifs de l'Union. Comme c'est le cas pour tous les contrats, lorsque les parties nouent des relations contractuelles portant sur des données, elles sont tenues de respecter les dispositions impératives du droit de l'Union, telles que le règlement (UE) 2023/2854, le règlement (UE) 2016/679 du Parlement européen et du Conseil [2] ou les dispositions impératives du droit de la consommation, ainsi que les dispositions impératives du droit national qui sont applicables à ce contrat particulier.

(10) Des clauses contractuelles abusives pourraient rendre l'accès aux données ou le changement de fournisseur de services de traitement de données commercialement moins viable et parfois prohibitif sur le plan économique.

(11) Le règlement (UE) 2023/2854 introduit un contrôle du caractère abusif des clauses contractuelles régissant l'accès aux données, l'utilisation des données ou la responsabilité, ainsi que des voies de recours en cas de violation ou d'extinction des obligations liées aux données, lorsque celles-ci sont imposées unilatéralement par une partie dans les contrats conclus entre entreprises. Les clauses types et les clauses standards tiennent également compte des dispositions relatives à ce contrôle du caractère abusif.

(12) Il est nécessaire d'établir des clauses contractuelles types pour plusieurs contrats qui couvrent l'accès aux données et l'utilisation des données dans le cadre des chapitres II, III et IV du règlement (UE) 2023/2854. Le premier contrat type recommandé régit la relation juridique entre, d'une part, l'utilisateur d'un produit connecté ou d'un service connexe, qui a le droit, en vertu du règlement (UE) 2023/2854, d'accéder aux données et d'utiliser les données et, d'autre part, un détenteur de données (annexe II). Bien que ces clauses contractuelles types puissent être utilisées en tant que contrat distinct parallèlement à d'autres contrats, à savoir a) le contrat d'achat, de location ou de crédit-bail d'un produit connecté, b) le contrat de fourniture de services connexes ou c) tout contrat qu'il est nécessaire de conclure au titre du règlement (UE) 2016/679, elles peuvent également être intégrées dans un contrat global, couvrant par exemple l'achat du produit connecté. Le deuxième type de contrat couvert par les clauses contractuelles types est conclu entre l'utilisateur et un destinataire de données (annexe III). Le troisième contrat type couvert est conclu entre le détenteur de données et un destinataire de données, et concerne les cas dans lesquels un détenteur de données a l'obligation légale de mettre des données à la disposition d'un tiers, telle que l'obligation de mettre des données relatives à un produit connecté ou à des services connexes à la disposition d'un destinataire de données indiqué par l'utilisateur (annexe IV). Le quatrième contrat type couvert est conclu entre des entreprises partageant des données sur une base volontaire, et est soumis au contrôle du caractère abusif prévu par le règlement (UE) 2023/2854 (annexe V).

(13) Il est nécessaire d'établir des clauses contractuelles standards qui peuvent être incluses dans les contrats de services de traitement de données afin d'intégrer les droits et obligations des clients et des fournisseurs, à la lumière du chapitre VI du règlement (UE) 2023/2854 et compte tenu de la nécessité de supprimer les obstacles contractuels au changement de fournisseur et d'assurer des droits et obligations contractuels équitables, raisonnables et non discriminatoires (annexes VI à XII).

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(14) Afin de faciliter l'utilisation de clauses types et de clauses standards, il convient d'inclure des orientations et des explications sous la forme de cadres d'information. Les orientations et explications sont destinées à aider les parties en fournissant des références aux obligations juridiques pertinentes ainsi que des références croisées entre les clauses et, au besoin, en expliquant les conséquences des choix que les parties sont tenues de faire, tels que mentionnés dans les différentes options liées à une clause contractuelle donnée,

RECOMMANDE:

(1) Que les parties contractantes utilisent les clauses contractuelles types relatives à l'accès aux données et à l'utilisation des données telles que figurant aux annexes I à V.

(2) Que les parties contractantes utilisent les clauses contractuelles standards pour les contrats d'informatique en nuage telles que figurant aux annexes I et VI à XII.

(3) Que les États membres encouragent l'utilisation des clauses contractuelles types et des clauses contractuelles standards recommandées, y compris par l'intermédiaire des autorités compétentes et des organes de règlement des litiges désignés respectifs prévus par le règlement (UE) 2023/2854.

Fait à Bruxelles, le 29 octobre 2026.

Par la Commission
Michael McGRATH
Membre de la Commission

ANNEXE I

INTRODUCTION GÉNÉRALE

1. **Contexte**

En 2022, la Commission a mis en place un groupe composé d'experts nommés à titre personnel et chargés de l'aider à fournir des outils pratiques aux acteurs du marché qui seraient amenés à exercer de nouveaux droits et obligations au titre du règlement (UE) 2023/2854 (ci-après le «règlement sur les données»). Les experts ont rédigé des clauses contractuelles types (CCT) concernant l'accès aux données et l'utilisation des données ainsi que des clauses contractuelles standards (CCS) pour les services de traitement de données. Ces CCT et CCS ont été incluses dans un rapport publié en avril 2025 dans le registre des groupes d'experts. Le groupe d'experts était soutenu par un sous-groupe composé d'entreprises et d'organisations professionnelles européennes et nationales. Le sous-groupe a adressé ses observations aux experts tout au long du processus de rédaction.

Afin de fournir de la matière supplémentaire aux experts, les services de la Commission ont organisé non seulement des consultations ciblées en expérimentant les projets de modèles auprès des entreprises qui se sont portées volontaires pour cet exercice, mais aussi deux cycles de consultation publique (l'un portant sur la version des CCT et des CCS élaborée par les experts et l'autre sur les versions finalisées incluses dans le rapport du groupe d'experts).

Sur la base du rapport du groupe d'experts et des contributions reçues au cours des consultations publiques, et conformément à l'article 41 du règlement sur les données, la Commission a élaboré les CCT et les CCS, lesquelles sont jointes en tant qu'annexes de la présente recommandation.

Les CCT et les CCS ne sont pas contraignantes. Elles sont et ont été rédigées de manière à pouvoir être adaptées par les parties en fonction de leurs besoins contractuels. Toutefois, les parties doivent considérer que ces CCT et CCS ont été rédigées de manière à être conformes aux droits et obligations prévus par le règlement sur les données et qu'elles ont également été conçues pour être cohérentes entre elles. Elles comprennent des informations sur leur caractère facultatif ainsi que des conseils à l'intention des parties quant aux conséquences juridiques qui peuvent découler en cas de modifications. En outre, les organes de règlement des litiges désignés en application de l'article 10 du règlement sur les données devraient tenir compte des CCT et des CCS.

Les CCT et les CCS ont été rédigées principalement pour régir les relations contractuelles interentreprises. Toutefois, elles peuvent également être utilisées dans les relations entre les entreprises et les consommateurs. Dans ce cas, toutefois, il convient de prévoir des dispositions supplémentaires afin que le contrat respecte les règles impératives en matière de protection des consommateurs (par exemple, le droit de rétractation du consommateur dans le cas de contrats conclus en ligne/à distance).

L'utilisation de ces CCT et CCS ne dispense pas les parties de leur obligation de veiller au respect de toute disposition impérative applicable prévue par le droit de l'Union ou le droit national. L'utilisation des CCT et des CCS est laissée à l'entière discrétion des parties. La Commission n'est pas responsable des conséquences découlant de l'utilisation de ces clauses.

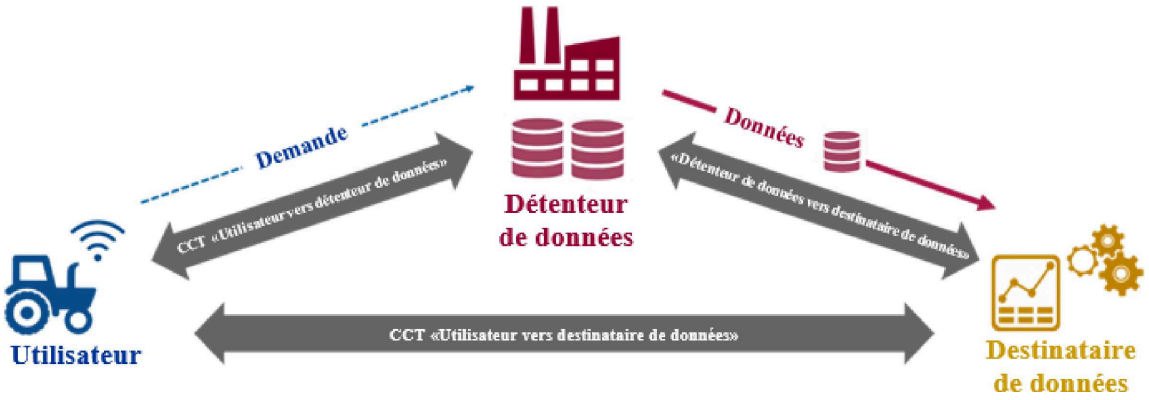
La Commission se réserve le droit de réexaminer ces clauses contractuelles types et clauses contractuelles standards à la lumière de leur application et de leurs effets sur les entreprises et les pratiques du marché.

2. **Clauses contractuelles types**

Les CCT figurant aux annexes II à V ont été élaborées pour aider les parties à rédiger et à négocier des contrats portant sur l'accès aux données et sur l'utilisation de données (à caractère personnel et non personnel). Ces contrats visent à garantir des droits et obligations contractuels équitables, raisonnables et non discriminatoires, notamment en ce qui concerne la garantie d'une compensation raisonnable et la protection des secrets d'affaires.

Les parties au contrat sont définies au début de chacune des CCT, en respectant, le cas échéant, les termes définis par le règlement sur les données: données, détenteur de données, utilisateur, destinataire de données, etc.

Quelles CCT utiliser pour quel type de partage de données?



Les CCT figurant à l'annexe II ont été conçues pour les contrats conclus entre un détenteur de données et l'utilisateur d'un produit connecté ou d'un service connexe, lorsque le détenteur de données souhaite utiliser des données générées à l'aide dudit produit/service.

Les CCT figurant à l'annexe III ont été conçues pour des contrats conclus entre l'utilisateur d'un produit connecté ou d'un service connexe et un destinataire de données tiers, lorsque l'utilisateur demande à un détenteur de données de mettre des données à la disposition d'un destinataire de données en vertu de l'article 5 du règlement sur les données.

Les CCT figurant à l'annexe IV ont été conçues pour les contrats conclus entre un détenteur de données et un destinataire de données tiers qui est une entreprise, lorsqu'un détenteur de données est tenu (en vertu de l'article 5 du règlement sur les données) de mettre des données à la disposition d'un destinataire à la demande d'un utilisateur du produit. Elles peuvent également être utilisées moyennant les modifications appropriées lorsqu'un détenteur de données est tenu de mettre des données à la disposition d'un destinataire de données tiers en vertu d'autres dispositions du droit de l'Union ou de la législation nationale adoptée en vertu du droit de l'Union.



Les CCT figurant à l'annexe V ont été conçues pour les contrats conclus entre un responsable du partage des données et un destinataire de données lorsque le responsable du partage des données souhaite mettre des données à la disposition d'un destinataire de données sur une base volontaire et indépendamment de toute demande émanant d'un utilisateur ou d'une partie similaire. Le terme «responsable du partage des données» a été choisi pour tenir compte des multiples scénarios possibles en l'espèce.

Les parties devraient identifier la situation qui leur est propre en se référant aux différents scénarios décrits ci-dessus et utiliser ensuite les CCT pertinentes.

Valeur juridique des CCT au regard du règlement sur les données et d'autres législations applicables

L'utilisation des CCT par les parties contractantes ne porte atteinte à aucun des droits et obligations qui leur incombent en vertu du règlement sur les données ou d'autres actes législatifs de l'Union ou des États membres adoptés conformément au droit de l'Union, notamment les obligations du responsable du traitement et les droits des personnes concernées au titre du règlement (UE) 2016/679, et en vertu du droit de la concurrence.

Les parties devraient accorder une attention particulière aux situations où le partage de données concerne des données à caractère personnel ou des ensembles de données mixtes. En particulier, les détenteurs de données sont tenus de mettre des données à caractère personnel à la disposition d'utilisateurs ou de tiers, tel que prévu par le règlement (UE) 2023/2854, mais pour autant uniquement qu'il existe une base juridique conformément au règlement (UE) 2016/679.

Comme pour tout contrat, l'utilisation des clauses contractuelles types par les parties n'empêche pas une juridiction compétente ou toute autorité administrative compétente de conclure à l'annulation d'un contrat ou de certaines de ses clauses pour non-respect du droit de l'Union ou du droit d'un État membre.

3. **Clauses contractuelles standards**

Les CCS sont conçues pour aider les parties dans la mise en œuvre contractuelle des droits et obligations découlant du règlement sur les données. Elles constituent un ensemble de clauses modulaires qui se complètent mutuellement, mais qui peuvent également être utilisées séparément. Elles sont destinées à être insérées dans les contrats de services de traitement de données.

Les CCS visent à aider les clients et les fournisseurs de tout service de traitement de données relevant du règlement sur les données, qu'il soit public, privé ou autre, et quelle que soit sa taille (petit, moyen ou grand).

Conformément à la définition d'un service de traitement de données figurant dans le règlement sur les données, ces CCS s'appliquent à tous les modèles de services en nuage, y compris les infrastructures à la demande (IaaS), les plateformes à la demande (PaaS) et les logiciels à la demande (SaaS), lorsque ces services présentent les caractéristiques énoncées à l'article 2, point 8), dudit règlement.

Les CCS au titre du règlement sur les données n'intègrent pas les exigences du RGPD ([1]). Il y a lieu d'inclure dans l'accord des dispositions contractuelles visant à garantir le respect du RGPD. La Commission a adopté des clauses contractuelles standards régissant la relation entre le responsable du traitement et le sous-traitant, non seulement pour contribuer au respect du RGPD mais aussi aux fins du transfert de données à caractère personnel vers des pays situés en dehors de l'EEE ([2]).

Les clauses contractuelles standards prévues par le RGPD permettent aux entités qui les utilisent de garantir et de démontrer le respect de certaines exigences du RGPD. Ces clauses contractuelles standards ne peuvent pas être modifiées par les parties mais peuvent être incluses dans un contrat plus large ou être utilisées en tant qu'accord autonome.

Comment utiliser les CCS?

S'il est recommandé d'utiliser l'ensemble des CCS, il est important de noter que ces clauses ne constituent pas l'intégralité du contrat de services de traitement de données susceptible de s'appliquer entre un client et un fournisseur. D'autres sujets non abordés par le règlement sur les données et par les CCS doivent faire partie d'un tel accord.

Un ensemble de «définitions» utilisées dans les différentes CCS et conformes au règlement sur les données figure à l'annexe XII. Si des définitions autres que celles proposées dans les CCS sont utilisées, il convient d'adapter ces clauses en conséquence. Il ne s'agit là que d'un exemple d'adaptations qui sont possibles tout en utilisant l'intégralité ou une partie des CCS.

Par souci de clarté, les CCS contiennent des références croisées reliant certaines de leurs dispositions à des dispositions pertinentes du règlement sur les données ou à d'autres CCS.

Il se peut que des règles et exigences supplémentaires applicables aux services de traitement de données dans des secteurs spécifiques doivent également être prises en considération (par exemple, dans les secteurs financier, de la santé, des télécommunications, de l'industrie, de l'énergie ou du secteur public). Le règlement sur les données prévoit des exceptions à certaines obligations liées aux processus de changement de fournisseur et de sortie. De plus amples explications figurent dans les sections des CCS relatives au changement de fournisseur et à la sortie.

Le règlement sur les données prévoit des possibilités spécifiques pour le règlement des litiges:

le client et le fournisseur ont accès à un organe de règlement des litiges désigné par les États membres conformément à l'article 10, paragraphe 4, du règlement sur les données; et

chacune des parties peut introduire une réclamation auprès de l'autorité compétente de son État membre conformément à l'article 37, paragraphe 5, point b), du règlement sur les données.

([1]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([2]) Publications sur les clauses contractuelles standard (CCS) — Commission européenne.

Toutefois, au moment de la désignation, les États membres définissent les tâches et les pouvoirs de l'autorité compétente concernée, lesquels peuvent varier dans une certaine mesure d'un État membre à l'autre. Il est possible que cette autorité ne soit pas compétente pour régler tous les litiges opposant un client et son fournisseur. Les parties doivent évaluer la manière la plus appropriée de contraindre l'autre partie à s'acquitter de ses obligations légales et contractuelles, ainsi que les modalités de règlement des litiges.

Les parties peuvent convenir d'englober plusieurs services dans un seul accord, lequel peut être appelé «accord-cadre de services» ou être intitulé différemment (l'«accord»). C'est une autre raison pour laquelle il est recommandé d'ajouter les CCS à l'accord. Si ledit accord couvre l'ensemble des services et que le client décide de changer de fournisseur pour un service ou pour un nombre donné de services, l'accord restera en vigueur pour les autres services.

Si les parties envisagent de n'utiliser que partiellement ces CCS ou d'y apporter des modifications, elles devraient examiner attentivement les effets que cela pourrait avoir sur les droits et obligations contractuels. Il est toujours recommandé en pareilles situations de recourir à des conseils juridiques ou à d'autres conseils professionnels.

ANNEXE II

CLAUSES CONTRACTUELLES TYPES

pour les contrats relatifs à l'accès aux données et à leur utilisation conclus entre les détenteurs de données et les utilisateurs de produits connectés et de services connexes

Les présentes clauses contractuelles types sont destinées à traiter de l'accès aux données et de leur utilisation, ainsi que des questions contractuelles connexes susceptibles de survenir entre un détenteur de données et des utilisateurs, tels que définis par le règlement (UE) 2023/2854 (ci-après le «règlement sur les données»).

La principale nouveauté du règlement sur les données à cet égard est la suivante:

— les utilisateurs se voient accorder le droit d'accéder aux données générées par leurs produits connectés et/ou leurs services connexes (avec des mesures de protection des données protégées en tant que secrets d'affaires);

— les utilisateurs peuvent également partager ces données avec des tiers, par exemple pour bénéficier de services après-vente;

— le détenteur de données doit conclure un contrat avec l'utilisateur pour utiliser et partager des données à caractère non personnel;

— les clauses contractuelles abusives concernant l'accès aux données et l'utilisation des données, ou la responsabilité et les voies de recours en cas de violation ou d'extinction d'obligations liées aux données, ne sont pas contraignantes si elles ont été imposées unilatéralement à une entreprise par une autre entreprise.

Le présent contrat a une structure modulaire et, s'il peut être utilisé comme contrat complet, les parties peuvent également sélectionner certaines clauses qui correspondent à leur situation particulière. Certains termes peuvent ne pas être pertinents pour tous les produits et tous les contrats, par exemple ceux concernant la protection des secrets d'affaires ou l'application de mesures techniques de protection. Celles-ci ne devraient être incluses par les parties dans le contrat que s'il y a lieu. De même, des limitations de l'accès aux données, de leur utilisation ou de leur partage ne devraient être prévues dans les contrats que si nécessaire, c'est-à-dire si les exigences de sécurité du produit étaient autrement compromises, entraînant de graves effets indésirables pour la santé, la sûreté ou la sécurité des personnes physiques.

Plusieurs clauses contiennent des options, et les parties doivent ici réfléchir à leurs besoins, relations commerciales et intérêts spécifiques afin de déterminer l'option la mieux adaptée à leur contrat.

Certaines clauses sont également marquées (*le cas échéant*) et devraient être incluses si certaines conditions sont remplies.

Bien que les clauses contractuelles types soient recommandées par la Commission, elles ne sont pas contraignantes et peuvent toujours faire l'objet d'une dérogation de la part des parties.

1. Parties et produit / service(s) connexe(s)

1.1. Parties au contrat

Le présent contrat relatif à l'accès aux données et à leur utilisation est conclu

entre

(insérer le nom, les coordonnées et d'autres références) (ci-après le «détenteur de données»)

Conformément au règlement sur les données, on entend par «détenteur de données» «une personne physique ou morale qui, conformément au règlement sur les données, aux dispositions applicables du droit de l'Union ou à la législation nationale adoptée conformément au droit de l'Union, a le droit ou l'obligation d'utiliser et de mettre à disposition des données, y compris, lorsqu'il en a été convenu par contrat, des données relatives au produit ou des données relatives au service connexe qu'elle a extraites ou générées au cours de la fourniture d'un service connexe».

Dans la plupart des cas, le détenteur de données peut être le fabricant du produit ou le fournisseur du service connexe concerné, ou une autre partie coopérant avec le fabricant ou le fournisseur qui peut extraire les données à partir du produit ou du service connexe.

Si plusieurs parties peuvent être considérées comme un détenteur de données, cela peut être traité de différentes manières, par exemple:

(a) chacune des parties conclut son propre accord avec l'utilisateur en tant que détenteur de données indépendant; ou
(b) l'une des parties conclut un accord avec l'utilisateur et agit donc en tant que détenteur de données; en l'absence d'accord avec l'utilisateur, les autres parties sont considérées comme des tiers au sens de la clause 3.2. Sur la base du contrat conclu avec l'utilisateur et des contrats conclus avec ces tiers, le détenteur de données peut coordonner l'accès aux données et leur utilisation.

La préférence accordée à l'une ou l'autre de ces deux possibilités dans un cas donné dépend de nombreux facteurs. Les parties peuvent souhaiter examiner, par exemple, si les utilisateurs préfèrent n'avoir qu'un seul partenaire contractuel et un seul contrat. Les parties devraient tenir compte du fait qu'il existe un lien étroit entre le choix entre les deux options et la manière dont les parties formulent la clause 3.2.1.

et

[OPTION 1] [(*insérer le nom, les coordonnées et d'autres références*) (ci-après l'«utilisateur»)]

[OPTION 2] [toute partie qui s'identifie comme utilisateur au sens du règlement sur les données et qui déclare accepter les termes du présent contrat en suivant les étapes suivantes: (*indiquer les étapes techniques à suivre par toute partie pouvant être considérée comme un utilisateur, telles que les informations à fournir et les confirmations à effectuer via une interface utilisateur*) (ci-après l'«utilisateur»)]

dénommés collectivement dans le présent contrat «les parties» et individuellement «la partie».

Conformément au règlement sur les données, on entend par «utilisateur» «une personne physique ou morale à laquelle appartient un produit connecté ou à laquelle des droits temporaires d'utilisation de ce produit connecté ont été cédés contractuellement, ou qui reçoit des services connexes». Le présent contrat peut s'appliquer à un large éventail de situations différentes. D'un côté, nous trouvons des situations où l'utilisateur est connu du détenteur de données et où les avocats de chaque partie négocient un contrat sur mesure concernant l'accès aux données et leur utilisation (par exemple, une compagnie aérienne qui achète des avions à un constructeur aéronautique). De l'autre, nous trouvons des situations où des produits et services de masse sont proposés à des millions de consommateurs qui ne sont pas connus individuellement (et dont nous ne souhaitons peut-être même pas divulguer l'identité pour des raisons de protection des données) et où les négociations individuelles sont tout simplement impossibles (par exemple, les machines à café connectées).

Dans ce dernier type de situations, et dans de nombreuses autres situations intermédiaires, il peut être utile d'identifier l'utilisateur non pas par son nom, mais par les étapes qu'il a suivies (par exemple, la création d'un compte utilisateur ou le simple branchement d'une machine à café connectée et l'acceptation des conditions générales fournies en cliquant sur «OK» à l'écran). Les parties devraient tenir compte du fait que, en particulier dans les affaires impliquant des consommateurs, les tribunaux évalueront si la procédure est conçue d'une manière conforme aux règles du droit général des contrats et du droit de la consommation applicables, selon lesquelles certaines conditions peuvent devoir être incluses dans le contrat.

1.2. **Produit / service(s) connexe(s)**

Le présent contrat porte sur:

(a) le ou les produits connectés suivants (ci-après le «produit»): (insérer le nom et d'autres spécifications du produit connecté spécifique ou du type de produits couverts par le présent contrat);

(b) le ou les services connexes suivants (ci-après le ou les «services connexes»): (insérer le nom et d'autres spécifications des services connexes spécifiques ou du type de services connexes couverts par le présent contrat, le cas échéant).

1.2.1. L'utilisateur déclare qu'il est soit propriétaire du produit, soit contractuellement autorisé à utiliser le produit dans le cadre d'un contrat de location ou de crédit-bail ou d'un contrat similaire et/ou à recevoir le ou les services connexes dans le cadre d'un contrat de services.

[OPTION 1] [L'utilisateur s'engage à fournir au détenteur de données, sur demande dûment justifiée, toute documentation pertinente à l'appui de ces déclarations, si nécessaire.]

[OPTION 2] [La documentation à l'appui de ces déclarations ainsi que des précisions sur les personnes qui doivent être considérées comme l'utilisateur au titre du présent contrat figurent à l'**appendice 9**.]

En vertu du règlement sur les données, le détenteur de données ne doit pas exiger d'une personne physique ou morale qu'elle fournisse d'autres informations que celles qui sont nécessaires afin de vérifier si une personne peut être considérée comme un utilisateur aux fins du règlement sur les données. Dans de nombreuses situations, en particulier pour les produits de grande consommation ou les équipements à usage professionnel dont les données générées sont relativement peu sensibles (par exemple, les machines à café connectées, voir ci-dessus), il sera généralement disproportionné de procéder à des recherches supplémentaires.

2. **Données couvertes par le contrat**

Les données couvertes par le présent contrat comprennent toutes les données relatives à un produit ou les données relatives à un ou des services connexes facilement accessibles au sens du règlement sur les données, et comprennent à la fois des données à caractère non personnel et des données à caractère personnel (ci-après les «données»).

Le détenteur de données énumère les données à l'**appendice 1**, avec une description du type ou de la nature, du volume estimé, de la fréquence de collecte, du lieu de stockage et de la durée de conservation des données.

Si, au cours du présent contrat, des données autres que celles spécifiées à l'appendice 1 doivent être mises à la disposition de l'utilisateur, l'**appendice 1** sera modifié en conséquence.

Conformément au règlement sur les données, on entend par «**données relatives au produit**» les données générées par l'utilisation d'un produit connecté que le fabricant a conçu pour qu'elles puissent être extraites, au moyen d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré, par un utilisateur, un détenteur de données ou un tiers, y compris, le cas échéant, le fabricant».

On entend par «**données relatives au service connexe**» les «données représentant la numérisation des actions de l'utilisateur ou des événements liés au produit connecté, enregistrées intentionnellement par l'utilisateur ou générées en tant que produit annexe de l'action de l'utilisateur lors de la fourniture d'un service connexe par le fournisseur».

Les données relatives au produit et aux services connexes peuvent être à la fois des données à caractère personnel et des données à caractère non personnel. Il s'agit notamment des «données sous forme brute» ainsi que des «données qui ont été prétraitées dans le but de les rendre compréhensibles et utilisables avant leur traitement et leur analyse ultérieurs». Toutefois, il ne s'agit pas des «informations dérivées ou déduites de ces données, qui sont le résultat d'investissements supplémentaires dans l'attribution de valeurs ou d'informations tirées des données» (considérant 15).

On entend par «**données facilement accessibles**» les «données relatives à un produit et les données relatives à un service connexe qu'un détenteur de données obtient légalement ou peut obtenir légalement à partir du produit connecté ou du service connexe, sans effort disproportionné allant au-delà d'une simple opération».

Comme expliqué dans les considérants, cette définition exclut les «données générées par l'utilisation d'un produit connecté lorsque la conception du produit connecté ne prévoit pas que ces données sont stockées ou transmises en dehors du composant dans lequel elles sont générées ou du produit connecté dans son ensemble» (considérant 20). «Les choix de conception des fabricants et, le cas échéant, les dispositions du droit de l'Union ou du droit national qui répondent aux besoins et aux objectifs propres à un secteur ou les décisions pertinentes des autorités compétentes devraient déterminer les données qu'un produit connecté peut mettre à disposition» (considérant 14).

3. **Utilisation et partage des données par le détenteur de données**

3.1. **Utilisation convenue de données à caractère non personnel par le détenteur de données**

3.1.1. Sans préjudice de tout droit légal d'utiliser les données, le détenteur de données s'engage à n'utiliser les données qui ne sont pas des données à caractère personnel que pour les finalités convenues avec l'utilisateur, comme suit:

(a) exécuter un accord avec l'utilisateur ou des activités liées à cet accord (par exemple, émission de factures, production et fourniture de rapports ou d'analyses, projections financières, analyses d'impact, calcul des avantages du personnel);

(b) fournir une assistance, une garantie ou des activités similaires ou évaluer les réclamations des utilisateurs, des détenteurs de données ou de tiers (par exemple, concernant des dysfonctionnements du produit) liées au produit ou au service connexe;

(c) surveiller et maintenir le fonctionnement, la sûreté et la sécurité du produit ou du service connexe et assurer le contrôle de la qualité;

(d) améliorer le fonctionnement de tout produit ou service connexe proposé par le détenteur de données;

(e) développer de nouveaux produits ou services par le détenteur de données, par des tiers agissant pour le compte du détenteur de données (c'est-à-dire lorsque le détenteur de données décide des tâches qui seront confiées à ces parties et qui en bénéficient), en collaboration avec d'autres parties ou par l'intermédiaire de sociétés ad hoc (telles que des entreprises communes);

(f) agréger ces données avec d'autres données ou créer des données dérivées, à toutes fins licites, y compris dans le but de vendre ces données agrégées ou dérivées à des tiers ou de les mettre à leur disposition d'une autre manière, à condition que ces données ne permettent pas d'identifier des données spécifiques transmises au détenteur de données à partir du produit connecté ou ne permettent pas à un tiers d'obtenir ces données à partir de l'ensemble de données.

Les parties devraient préciser les finalités et toutes les conditions dans lesquelles le détenteur de données peut utiliser les données à caractère non personnel. La liste comprend les principales utilisations communes, mais les parties sont libres de choisir parmi celles énumérées dans la présente clause ou d'en ajouter.

Lorsqu'elles conviennent de l'utilisation des données, les parties peuvent regrouper les données en catégories, le cas échéant. Les catégories plus larges peuvent comprendre les éléments suivants:

— des données relatives à l'état du produit ou du service (par exemple, configuration, version, messages de diagnostic, données de consommation, données d'entretien);

— des données relatives à l'utilisation par les clients (par exemple, temps d'activité, types d'activité, géolocalisation du produit) — il convient de noter que ces données peuvent, dans certains cas, constituer des données à caractère personnel et ne seront pas couvertes par la présente clause, mais par la clause 3.3 et d'autres dispositions du contrat;

— des données relatives à l'environnement des utilisateurs (par exemple, l'état des sols, la superficie);

— des données générales relatives à l'environnement (par exemple, données météorologiques).

Les parties devraient tenir compte du fait que la formulation par défaut donnée ci-dessus dans cet ensemble de conditions suppose que les finalités qui y sont énumérées sont celles poursuivies par le détenteur de données qui est partie au présent contrat. En ce qui concerne le développement de nouveaux produits ou services, par exemple, il est supposé que les activités de développement sont menées par le détenteur de données, bien que cela puisse se faire en collaboration avec d'autres parties, telles que des fabricants de composants. Le partage de données avec ces parties devrait donc être autorisé par défaut, comme le prévoit la clause 3.2.1, point a) i) et ii).

L'utilisation des données à des fins indépendantes par des tiers nécessiterait soit que ces tiers concluent un contrat distinct avec l'utilisateur, soit que la clause facultative 3.2.1, point a) iii) permettant au détenteur de données de vendre ou de donner des données à ces tiers à leurs propres fins s'applique.

L'utilisateur doit évaluer les conséquences de telles utilisations par le détenteur de données ou des tiers sur ses activités et ses intérêts, notamment s'il doit être rémunéré par le détenteur de données, par exemple lorsque celui-ci vend à des tiers les données générées par l'utilisateur.

3.1.2. Le détenteur de données s'engage à ne pas utiliser les données:

(a) pour obtenir des informations sur la situation économique, les actifs et les méthodes de production de l'utilisateur, ou sur l'utilisation du produit ou du service connexe qu'en fait ce dernier d'une quelconque autre manière susceptible de porter atteinte à la position commerciale de l'utilisateur sur les marchés sur lesquels il exerce ses activités;

(b) [OPTION] (*veuillez préciser les utilisations de données qui, par exemple, portent gravement atteinte aux intérêts légitimes de l'utilisateur*)].

Les parties peuvent souhaiter fournir davantage de précisions sur le type d'utilisation des données qu'elles considèrent comme tellement préjudiciable qu'il doit être exclu. Cela dépendra du secteur concerné et d'autres circonstances. En particulier, l'utilisateur peut souhaiter exclure:

— l'utilisation de catégories particulières de données hautement sensibles; et/ou

— l'utilisation des données à des fins particulières.

Aucune des utilisations de données convenues en vertu de la clause 3.1.1 ne peut être en contradiction avec la présente clause, et le détenteur de données s'engage à veiller, par des moyens contractuels, organisationnels et techniques appropriés, à ce qu'aucun tiers, au sein de l'organisation du détenteur de données, ne se livre à une telle utilisation de données.

3.2. **Partage de données à caractère non personnel avec des tiers et utilisation de services de traitement**

3.2.1. Sans préjudice des exigences légales prévues par le droit de l'Union ou le droit national pour qu'un détenteur de données mette des données à disposition, il peut partager avec des tiers des données à caractère non personnel si:

(a) les données sont utilisées par le tiers exclusivement aux fins suivantes:

i) aider le détenteur de données à atteindre les objectifs autorisés en vertu de la clause 3.1.1;

ii) atteindre, en collaboration avec le détenteur de données ou par l'intermédiaire d'entreprises ad hoc, les objectifs autorisés en vertu de la clause 3.1.1;

iii) [OPTION] [(préciser les finalités que les tiers peuvent poursuivre pour leurs propres besoins, indépendamment du détenteur de données, et si les données sont partagées à ces fins en échange d'une compensation ou gratuitement);] et

(b) le détenteur de données oblige contractuellement le tiers:

i) à ne pas utiliser les données à des fins ou d'une manière allant au-delà de l'utilisation autorisée conformément à la clause 3.2.1, point a);

ii) à respecter le contenu de la clause 3.1.2;

iii) à appliquer les mesures de protection requises en vertu de la clause 3.4.1; et

iv) [OPTION 1] [à ne pas partager ces données sauf si l'utilisateur donne son accord général ou spécifique pour un tel transfert ultérieur. Le détenteur de données doit obliger le tiers avec lequel il partage des données à inclure les clauses correspondant aux points i) à iv) dans ses contrats avec les destinataires.] [OPTION 2] [à ne pas partager ultérieurement ces données, sauf dans les cas prévus à l'appendice 5.]

[OPTION] [De plus amples informations, notamment en ce qui concerne l'identité ou les catégories de tiers avec lesquels les données peuvent être partagées, les restrictions à l'utilisation des données par des tiers, ainsi que d'autres conditions et mesures de protection, sont exposées en détail à l'**appendice 5**.]

3.2.2. Nonobstant la clause 3.2.1, le détenteur de données peut utiliser des services de traitement, par exemple des services d'informatique en nuage (y compris une infrastructure à la demande, une plateforme à la demande et un logiciel à la demande), des services d'hébergement ou des services similaires pour atteindre, pour son propre compte et sous sa propre responsabilité, les finalités convenues en vertu de la clause 3.1.1. Les tiers peuvent également utiliser ces services pour atteindre, pour leur propre compte et sous leur propre responsabilité, les finalités convenues en vertu de la clause 3.2.1, point a).

3.3. **Utilisation et partage de données à caractère personnel par le détenteur de données**

3.3.1. Le détenteur de données ne peut utiliser, partager avec des tiers ou traiter d'une autre manière des données à caractère personnel que s'il existe une base juridique prévue et dans les conditions autorisées par le règlement (UE) 2016/679 du Parlement européen et du Conseil [1] (RGPD) et, le cas échéant, la directive 2002/58/CE (directive vie privée et communications électroniques).

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

3.4. **Mesures de protection prises par le détenteur de données**

3.4.1. Le détenteur de données s'engage à appliquer les mesures de protection visant à prévenir la perte de données et l'accès non autorisé aux données [OPTION 1] [qui sont raisonnables et adaptées aux circonstances, compte tenu de l'état de la science et de la technologie, du préjudice potentiel subi par l'utilisateur et des coûts associés aux mesures de protection.] [OPTION 2] [qui sont exposées en détail à l'appendice 6.]

Les parties devraient examiner si elles souhaitent inclure, si nécessaire dans un appendice distinct, toutes les mesures permettant de protéger efficacement les intérêts importants de l'utilisateur. Les mesures peuvent être à la fois de nature technique (par exemple, cryptage, pare-feu, stockage fractionné) et organisationnelle (par exemple, participation d'un tiers de confiance). Étant donné que les mesures doivent être proportionnées, leur contenu variera considérablement en fonction de la nature des données et des intérêts en jeu.

4. **(le cas échéant) Accès de l'utilisateur aux données sur demande**

Les présentes clauses 4 s'appliquent si l'utilisateur ne peut pas accéder directement aux données à partir du produit ou du service connexe conformément à l'article 3 du règlement sur les données. Dans ce cas, l'utilisateur a le droit d'obtenir l'accès aux données du détenteur sur demande, conformément à l'article 4 du règlement sur les données. Si l'utilisateur souhaite donner accès aux données à un destinataire de données, les clauses 7 ci-dessous s'appliquent.

4.1. **Obligation de mettre les données à disposition**

4.1.1. Les données, ainsi que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, doivent être mises à la disposition de l'utilisateur par le détenteur de données, à la demande de l'utilisateur ou d'une partie agissant pour son compte. La demande peut être communiquée par l'intermédiaire de (*décrire la procédure de demande simple par voie électronique lorsque cela est techniquement possible*). Afin de vérifier que la demande est faite par l'utilisateur, le détenteur de données n'exige pas d'autres informations que celles qui sont nécessaires. (*le cas échéant*) [Si la demande est présentée par une partie agissant pour le compte de l'utilisateur, la preuve de son mandat est jointe à la demande.]

L'appendice 2 indique les renseignements qu'une demande peut contenir.

4.1.2. Lorsque l'utilisateur n'est pas la personne concernée, le détenteur de données ne met les données à caractère personnel à la disposition de l'utilisateur que s'il existe un fondement juridique valable pour la mise à disposition de données à caractère personnel en vertu de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, si les conditions énoncées à l'article 9 dudit règlement et à l'article 5, paragraphe 3, de la directive 2002/58/CE (directive vie privée et communications électroniques) sont remplies.

À cet égard, lorsque l'utilisateur n'est pas la personne concernée, il doit indiquer au détenteur de données, dans chaque demande présentée au titre de la clause précédente, la base juridique du traitement au titre de l'article 6 du règlement (UE) 2016/679 (et, le cas échéant, la dérogation applicable au titre de l'article 9 dudit règlement et de l'article 5, paragraphe 3, de la directive 2002/58/CE) sur laquelle se fonde la demande de mise à disposition de données à caractère personnel.

4.2. **Caractéristiques des données et modalités d'accès**

4.2.1. Le détenteur de données doit mettre les données à la disposition de l'utilisateur gratuitement, les données étant au moins de la même qualité que lorsqu'elles sont mises à la disposition du détenteur de données et, en tout état de cause, dans un format complet, structuré, couramment utilisé et lisible par machine.

On entend par «métadonnées» une description structurée du contenu ou de l'utilisation des données qui facilite la découverte ou l'utilisation de ces données. Conformément à l'article 4, paragraphe 1, du règlement sur les données, les métadonnées doivent être mises à disposition avec les données, dans la mesure où elles sont «*nécessaires à l'interprétation et à l'utilisation*» de ces données.

Bien que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données ne soient pas définies et doivent donc être déterminées au cas par cas, le règlement sur les données précise que «[l]*es données qui doivent être mises à disposition devraient inclure les métadonnées pertinentes, y compris leur contexte de base et leur horodatage, pour rendre les données utilisables, combinées à d'autres données, telles que les données triées et classifiées avec d'autres points de données les concernant, ou reformatées dans un format couramment utilisé*» (considérant 15).

Le détenteur de données et l'utilisateur peuvent utiliser les services d'un tiers [y compris un tiers fournissant des services d'intermédiation de données au sens de l'article 2 du règlement (UE) 2022/868 du Parlement européen et du Conseil ([2])] pour permettre l'exercice des droits de l'utilisateur en vertu de la clause 4.1 du présent contrat. Ce tiers ne sera pas considéré comme un destinataire de données en vertu du règlement sur les données et ces services peuvent être proposés par un fournisseur considéré comme un contrôleur d'accès en vertu de l'article 3 du règlement (UE) 2022/1925, sauf s'il traite les données pour ses propres finalités commerciales.

Un tiers qui fournit un service pour le compte du détenteur de données ou de l'utilisateur ne sera pas considéré comme un destinataire de données en vertu du règlement sur les données et ces services peuvent être proposés par un fournisseur considéré comme un contrôleur d'accès en vertu de l'article 3 du règlement (UE) 2022/1925 du Parlement européen et du Conseil ([3]), sauf s'il traite les données pour ses propres finalités commerciales.

4.2.2. L'utilisateur doit avoir accès aux données demandées:

a) de manière aisée et sécurisée;

b) sans retard injustifié;

(*le cas échéant*) [c) en continu et en temps réel].

4.2.3. Afin de satisfaire aux exigences des clauses 4.2.1 et 4.2.2, le détenteur de données précise ces modalités d'accès à l'appendice 1.

En vertu de l'article 4, paragraphe 1, du règlement sur les données, les données doivent être mises à disposition sans retard injustifié et, lorsque cela est pertinent et techniquement réalisable, en continu et en temps réel.

Étant donné qu'il existe différents moyens de mettre en œuvre ces exigences légales, le détenteur de données devrait préciser toutes les conditions dans lesquelles l'accès doit être fourni à l'appendice 1. Les conditions d'accès ne doivent pas porter atteinte aux droits accordés à l'utilisateur en vertu du règlement sur les données ou d'une autre législation applicable.

Compte tenu de cette restriction, le détenteur de données devrait, dans un premier temps, décider s'il souhaite:

— prévoir le transfert complet des données, c'est-à-dire qu'une copie des données est transférée sur un support placé sous le contrôle de l'utilisateur:

— par une transmission déclenchée par le détenteur de données («push»), telle qu'une transmission en ligne, un téléchargement dans l'espace en nuage de l'utilisateur ou la livraison d'un support matériel sur lequel les données sont stockées; ou

— par une récupération déclenchée par l'utilisateur («pull»), par exemple en lui fournissant une interface de programmation (API), un accès à l'espace en nuage du détenteur de données ou à des outils similaires lui permettant d'accéder aux données et de les extraire; ou

— donner accès aux données là où elles sont stockées, c'est-à-dire que les données sont consultées et traitées sur un support placé sous le contrôle du détenteur de données ou d'un tiers de confiance, par exemple en se connectant à un espace dédié sur les serveurs du détenteur de données ou du tiers de confiance, mais que les données ne sont pas transférées sur un support placé sous le contrôle de l'utilisateur, sauf si des dispositions particulières sont prises.

Le transfert complet donne à l'utilisateur une liberté maximale, tandis que l'accès à l'endroit où les données sont stockées augmente les risques pour les utilisateurs que leurs idées commerciales soient divulguées. En outre, en vertu de l'article 13, paragraphe 5, point e), du règlement sur les données, «une clause contractuelle est présumée être abusive si elle a pour objet ou pour effet [...] d'empêcher la partie à laquelle la clause a été imposée unilatéralement d'obtenir une copie des données qu'elle a fournies ou générées pendant la durée du contrat ou dans un délai raisonnable après la résiliation de celui-ci». Par conséquent, le transfert complet devrait être la règle par défaut.

([2]) Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

([3]) Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

Toutefois, le transfert complet réduit considérablement la capacité du détenteur de données à prévenir les abus et à protéger ses intérêts, par exemple les secrets d'affaires. Par conséquent, l'accès à l'endroit où les données sont stockées et leur traitement devraient également être possibles. Afin de concilier cet accès avec les intérêts de l'utilisateur, l'accès à l'endroit où les données sont stockées sur un support contrôlé par un tiers de confiance sera souvent préférable à l'accès sur un support contrôlé par le détenteur de données. L'accès à l'endroit où les données sont stockées devrait normalement toujours signifier un accès à distance, et l'accès sur place devrait être limité aux situations extrêmes présentant le degré de sensibilité le plus élevé.

Si un accès est accordé à l'endroit où les données sont stockées, un certain nombre de détails doivent être réglés, notamment comment s'assurer que les idées commerciales de l'utilisateur ne sont pas divulguées et quelles données l'utilisateur est autorisé à extraire et à transférer sur un support sous son propre contrôle (par exemple, les données dérivées ou déduites résultant des activités de traitement de l'utilisateur).

Conformément à l'article 4, paragraphe 1, du règlement sur les données, les données doivent être mises à disposition sans retard injustifié et, lorsque cela est pertinent et techniquement réalisable, en continu et en temps réel. Par conséquent, le détenteur de données doit préciser dans l'appendice si l'accès peut être fourni en continu et en temps réel, et si tel n'est pas le cas, à quelle fréquence.

Le détenteur de données devrait également examiner toute une série d'autres questions, telles que les identifiants d'accès requis ainsi que le nombre et l'identité des employés de l'utilisateur qui peuvent accéder aux données.

4.2.4. Le détenteur de données doit fournir à l'utilisateur, sans frais supplémentaires, les informations nécessaires pour accéder aux données conformément à l'article 4 du règlement sur les données.

Cela inclut, en particulier, la fourniture d'informations facilement accessibles au détenteur de données concernant tout droit que des tiers pourraient avoir à l'égard des données, tels que les droits des personnes concernées découlant du règlement (UE) 2016/679, ou les faits susceptibles de donner lieu à de tels droits.

Le détenteur de données précise ces informations à l'**appendice 1**.

Les parties restent libres de convenir de tout soutien supplémentaire, allant au-delà des exigences du règlement sur les données, gratuit ou payant.

4.2.5. Le détenteur de données s'engage à ne conserver aucune autre information sur l'accès de l'utilisateur aux données demandées que celles qui sont nécessaires:

(a) à la bonne exécution i) de la demande d'accès de l'utilisateur et ii) du présent contrat;

(b) à la sécurité et à la maintenance de l'infrastructure de données;

(c) au respect des obligations légales incombant au détenteur de données de conserver ces informations.

4.3. **Boucles de rétroaction**

Si l'utilisateur détecte un incident lié à la clause 2 sur les données couvertes par le contrat, aux exigences des clauses 4.2.1 ou 4.2.2 ou de l'**appendice 1** sur les caractéristiques des données et les modalités d'accès et si l'utilisateur fournit au détenteur de données une description détaillée de l'incident, ces derniers doivent coopérer de bonne foi pour déterminer la raison de l'incident.

Si l'incident a été causé par un manquement du détenteur de données à ses obligations, il doit remédier à la violation sans retard injustifié. Si le détenteur de données ne le fait pas, cela est considéré comme une inexécution essentielle et l'utilisateur peut invoquer la clause 12 du présent contrat. Si l'utilisateur estime que son droit d'accès au titre de l'article 4, paragraphe 1, du règlement sur les données est violé, il est également en droit d'introduire une réclamation auprès de l'autorité compétente, désignée conformément à l'article 37, paragraphe 5, point b), du règlement sur les données.

Cette clause donne au détenteur de données la possibilité de remédier à tout manquement à ses obligations légales ou contractuelles. Si le détenteur de données ne le fait pas sans retard injustifié, il permet à l'utilisateur d'utiliser les recours contractuels prévus par le contrat en cas d'inexécution essentielle de celui-ci.

Si l'utilisateur estime que son droit d'accès au titre de l'article 4, paragraphe 1, du règlement sur les données est violé, il est également en droit d'introduire une réclamation auprès de l'autorité compétente, désignée conformément à l'article 37, paragraphe 5, point b), du règlement sur les données. Toutefois, l'utilisateur devrait tenir compte du fait que les tâches et les pouvoirs précis des autorités compétentes désignées conformément à l'article 37 peuvent varier d'un État membre à l'autre.

L'utilisateur a toujours le droit de former un recours effectif devant la juridiction compétente ou de soumettre le litige à tout organisme de règlement extrajudiciaire des litiges.
L'utilisateur doit donc évaluer soigneusement quel est le moyen le plus approprié d'obliger le détenteur de données à respecter ses obligations légales et contractuelles.

4.4. **Modifications unilatérales apportées par le détenteur de données**

4.4.1. Le détenteur de données peut modifier unilatéralement les spécifications des caractéristiques des données ou les modalités d'accès énoncées à l'**appendice 1**, si cela est objectivement justifié par l'exercice normal des activités du détenteur de données, par exemple par une modification technique due à une vulnérabilité immédiate en matière de sécurité dans la gamme de produits ou de services connexes ou par une modification de l'infrastructure du détenteur de données. Toute modification doit répondre aux exigences des clauses 4.2.1 et 4.2.2.

Le détenteur de données doit notifier la modification à l'utilisateur au moins (*indiquer un délai raisonnable*) avant qu'elle ne prenne effet.

Un délai de notification plus court peut suffire:

(a) lorsque la modification n'a pas d'incidence négative sur l'accès aux données et leur utilisation par l'utilisateur; ou

(b) lorsqu'une telle notification serait impossible ou déraisonnable compte tenu des circonstances, par exemple lorsque des changements immédiats sont nécessaires en raison d'une vulnérabilité en matière de sécurité qui vient d'être détectée.

5. **(si les données mises à disposition par le détenteur de données à la demande de l'utilisateur doivent être protégées en tant que secrets d'affaires) Protection des secrets d'affaires**

1. **Transmission de secret d'affaires** — Les détenteurs de données ne peuvent pas, en principe, refuser une demande d'accès aux données présentée au titre du règlement sur les données au seul motif que certaines données sont considérées comme étant des secrets d'affaires, car cela irait à l'encontre des effets attendus dudit règlement.

Voir les clauses 5.1.

Secrets d'affaires — Toutefois, si le détenteur de données constate que certaines données couvertes par le présent contrat sont protégées en tant que secrets d'affaires, tels que défini par la directive (UE) 2016/943 ([4]) (ci-après la «directive sur les secrets d'affaires»), il bénéficie de certains droits, principalement le droit de continuer à préserver la confidentialité des secrets en question.

Aux termes de l'article 2, point 1), de la directive sur les secrets d'affaires, on entend par «secret d'affaires» des informations qui répondent aux trois conditions suivantes: a) elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, elles ne sont pas généralement connues de personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles; b) elles ont une valeur commerciale parce qu'elles sont secrètes; et c) elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes.

On entend par «détenteur de secrets d'affaires» toute personne physique ou morale qui a le contrôle d'un secret d'affaires de façon licite.

([4]) Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Les données ne peuvent être définies comme secrets d'affaires que si elles sont protégées en tant que telles par le détenteur de données ou le détenteur de secrets d'affaires lorsqu'une demande d'accès aux données est présentée conformément à l'article 4 du règlement sur les données.

Voir la clause 5.1.1.

2. **Identification initiale des secrets d'affaires** — Les droits des détenteurs de données en matière de secrets d'affaires ne sont — dans un premier temps — applicables que si et dans la mesure où les données protégées en tant que secrets d'affaires sont identifiées dans le contrat.

Voir la clause 5.1.2.

3. **Pendant la durée du contrat** — Les droits des détenteurs de données en matière de secrets d'affaires pourraient toutefois également s'appliquer pendant la durée du contrat, en ce qui concerne les nouvelles données à mettre à disposition.

Voir la clause 5.1.3.

4. **Droits d'audit** — Afin de préserver la confidentialité des données protégées en tant que secrets d'affaires, sans interférer avec les activités des autres, certains droits d'audit peuvent être envisagés en associant des tiers indépendants, y compris des mécanismes en cas de désaccord sur les résultats du rapport d'audit. Les parties peuvent recourir à d'autres mesures que les audits.

Voir la clause 5.2.3.

5. **Droits du détenteur de secrets d'affaires (1/4)** — Le détenteur de données (ou le détenteur de secrets d'affaires tiers) peut convenir avec l'utilisateur des exigences visant à préserver la confidentialité des secrets d'affaires comme condition préalable à la transmission de ces secrets d'affaires définis, telles que la prise de certaines mesures techniques et organisationnelles proportionnées.

Voir les clauses 5.2 et 5.3.

6. **Droits du détenteur de secrets d'affaires (2/4)** — Si les mesures initiales ne suffisent pas, le détenteur de secrets d'affaires peut, au cas par cas, pour des données spécifiques constituant des secrets d'affaires et protégées en tant que telles, soit augmenter unilatéralement le niveau des mesures, soit demander que des mesures supplémentaires soient convenues avec l'utilisateur. En l'absence d'accord sur les mesures nécessaires, le détenteur de données peut suspendre le partage de données spécifiques protégées en tant que secrets d'affaires, dans les conditions énoncées dans le règlement sur les données.

Voir la clause 5.4.1.

7. **Droits du détenteur de secrets d'affaires (3/4)** — Le détenteur de secrets d'affaires peut également, au cas par cas, refuser de partager des secrets d'affaires définis spécifiques, uniquement dans des circonstances exceptionnelles et dans les conditions énoncées dans le règlement sur les données.

Voir la clause 5.4.2.

8. **Droits du détenteur de secrets d'affaires (4/4)** — Le détenteur de secrets d'affaires peut bloquer ou suspendre le partage de données si l'utilisateur manque à ses obligations en matière de protection des secrets d'affaires.

Voir la clause 5.4.3.

9. **Conservation de données contenant des secrets d'affaires définis** — Si le détenteur de données bloque ou suspend le partage de données conformément aux clauses 5.4.1, 5.4.2 ou 5.4.3, il sera toujours tenu de maintenir les données connexes contenant des secrets d'affaires définis facilement accessibles en les conservant jusqu'à ce qu'elles puissent être partagées dans le cadre du contrat.

Voir la clause 5.6.

10. **Détenteur tiers de secrets d'affaires définis** — Si le détenteur de secrets d'affaires est un tiers, le détenteur de données doit veiller à ce que la clause 5 protège également ses secrets d'affaires et obtenir toutes les autorisations pertinentes dudit détenteur de secrets d'affaires tiers.

Voir la clause 5.1.2.

5.1. **Applicabilité des accords relatifs aux secrets d'affaires**

5.1.1. Les mesures de protection convenues dans les clauses 5.2 et 5.3 du présent contrat, ainsi que les droits connexes convenus dans la clause 5.4, s'appliquent exclusivement aux données ou métadonnées figurant dans les données que le détenteur de données doit mettre à la disposition de l'utilisateur et qui sont protégées en tant que secrets d'affaires (tels que définis dans la directive sur les secrets d'affaires), détenus par le détenteur de données ou un autre détenteur de secrets d'affaires (tel que défini dans ladite directive).

5.1.2. La définition des données protégées comme secrets d'affaires et l'identité du détenteur de secret d'affaires figurent à l'appendice 4.

Le détenteur de données déclare à l'utilisateur qu'il dispose de tous les droits pertinents de la part de tout détenteur de secrets d'affaires tiers pour conclure le présent contrat en ce qui concerne les données protégées en tant que secrets d'affaires.

Conformément à l'article 4, paragraphe 6, du règlement sur les données, le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires, recense les données protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes.

Par conséquent, le détenteur de données devrait recenser les données protégées en tant que secrets d'affaires à l'**appendice 4**. Toutefois, le détenteur de données ne devrait pas être tenu de décrire lui-même le secret d'affaires. Il suffit de déterminer les données qui doivent être protégées pour garantir la confidentialité du secret d'affaires, si l'analyse de ces données est susceptible de révéler le secret d'affaires.

5.1.3. Si, au cours du présent contrat, de nouvelles données protégées en tant que secrets d'affaires sont mises à la disposition de l'utilisateur conformément à la clause 5.1.1, à la demande du détenteur de données, l'appendice 4 sera modifié en conséquence.

Tant que l'**appendice 4** n'a pas été modifié et approuvé par les parties, le détenteur de données peut bloquer ou suspendre temporairement le partage des nouvelles données protégées en tant que secrets d'affaires. La décision du détenteur de données est dûment motivée et communiquée par écrit à l'utilisateur sans retard injustifié. Le détenteur de données notifie également à l'autorité compétente désignée en vertu de l'article 37 du règlement (UE) 2023/2854 qu'il a bloqué ou suspendu le partage de données et indique quelles mesures n'ont pas été convenues ou mises en œuvre.

5.1.4. Les obligations énoncées aux clauses 5.2 et 5.3 restent en vigueur après toute résiliation du contrat, sauf si les parties en conviennent autrement.

5.2. **Mesures de protection prises par l'utilisateur**

5.2.1. L'utilisateur doit appliquer les mesures de protection énoncées à l'**appendice 4** (ci-après les «mesures de protection de l'utilisateur»).

Les parties devraient, dans un appendice distinct, exposer toutes les modalités de ces mesures, y compris pour les situations dans lesquelles l'utilisateur partage les données avec des tiers. Les mesures peuvent être à la fois techniques (par exemple, cryptage, pare-feu, stockage fractionné, etc.) et organisationnelles (par exemple, gouvernance interne, gestion appropriée de l'identité et contrôles d'accès, participation d'un tiers de confiance, accords de confidentialité).

Étant donné que les mesures doivent être proportionnées, leur contenu variera en fonction de la nature du ou des secrets d'affaires applicables. Les mesures dépendront également de la question de savoir si i) l'accès doit être fourni à l'endroit où les données sont stockées ou si ii) les données doivent être entièrement transférées à l'utilisateur. Dans le premier cas, le détenteur de données a un degré de contrôle plus élevé et peut appliquer lui-même une partie des mesures de protection, tandis que l'utilisateur peut avoir un niveau d'utilisation des données moins élevé. Dans tous les cas, les deux parties devront s'attacher à produire les effets escomptés du règlement sur les données. Pour cette raison, les différents intérêts doivent être conciliés sans porter atteinte à ces effets recherchés.

5.2.2. Si l'utilisateur est autorisé à mettre les données à la disposition d'un tiers, il peut partager des données protégées en tant que secrets d'affaires dans les conditions suivantes:

(a) i) s'il informe le détenteur de données, sans retard injustifié, du fait que les données protégées en tant que secrets d'affaires seront mises à la disposition d'un tiers; ii) s'il précise les données en question et iii) s'il indique au détenteur de données l'identité, le lieu d'établissement et les coordonnées du tiers;

(b) le tiers applique les mesures de protection prévues à l'appendice 4.

5.2.3. [OPTION] [Afin de vérifier si et dans quelle mesure l'utilisateur a mis en œuvre et maintient les mesures de protection de l'utilisateur, l'utilisateur accepte soit i) d'obtenir chaque année, aux frais de l'utilisateur, un rapport d'évaluation de la conformité en matière de sécurité auprès d'un tiers indépendant choisi par l'utilisateur; soit ii) d'autoriser chaque année, aux frais du détenteur de données, un audit de l'évaluation de la conformité en matière de sécurité effectué par un tiers indépendant choisi par le détenteur de données, sous réserve que ce tiers indépendant ait signé un accord de confidentialité tel que fourni par l'utilisateur. Ce rapport d'audit de sécurité doit démontrer la conformité de l'utilisateur avec les clauses 5 et l'appendice 4 applicables à ce moment-là. Les résultats des rapports d'audit seront communiqués aux deux parties dans les meilleurs délais.

L'utilisateur peut choisir entre les options i) et ii). Si une partie estime que le rapport d'audit de sécurité obtenu aux frais de l'autre partie est incorrect, elle conserve le droit d'obtenir un rapport d'audit de sécurité d'un autre tiers indépendant à ses propres frais. Si ce droit est exercé, les deux auditeurs tiers indépendants, conjointement avec les parties, examineront toute différence entre ces deux rapports et s'efforceront de résoudre toute question en suspens dans le respect de l'exigence de bonne foi.]

La présente clause est indiquée comme une option, car les parties peuvent convenir d'autres mesures afin de vérifier le respect par l'utilisateur de ses obligations de mettre en œuvre et de maintenir les mesures de protection de l'utilisateur.

5.3. **Mesures de protection prises par le détenteur de secret d'affaires**

5.3.1. Le détenteur de données peut appliquer les mesures convenues à l'**appendice 4** pour préserver la confidentialité des données protégées en tant que secrets d'affaires (ci-après les «mesures de protection du détenteur de données»).

5.3.2. Le détenteur de données peut mettre en œuvre unilatéralement des solutions de protection techniques et organisationnelles appropriées, telles qu'une mise à jour logicielle, si elles n'ont pas d'incidence négative sur l'utilisateur au titre du présent contrat.

5.3.3. L'utilisateur s'engage à ne pas modifier ni supprimer les mesures de protection du détenteur de données ni les mesures prises conformément à la clause 5.3.2, sauf si les parties en conviennent autrement.

5.4. **Obligation de partager et droit de refuser, de bloquer ou de résilier**

5.4.1. Lorsque les mesures de protection de l'utilisateur identifié et du détenteur de données ne suffisent pas matériellement à protéger de manière appropriée des données spécifiques protégées en tant que secret d'affaires, le détenteur de données peut, en adressant à l'utilisateur une notification décrivant en détail l'insuffisance des mesures, demander que des mesures de protection supplémentaires soient convenues; en l'absence d'accord sur les mesures supplémentaires nécessaires après un délai raisonnable et si la nécessité de telles mesures est dûment justifiée, par exemple dans un rapport d'audit de sécurité, le détenteur de données peut bloquer ou suspendre le partage des données spécifiques en question; dans ce cas, le détenteur de données doit adresser une notification à l'utilisateur; la notification doit être dûment motivée, indiquer quelles mesures n'ont pas été convenues, le cas échéant, les secrets d'affaires concernés, et être faite par écrit sans retard injustifié; le détenteur de données doit continuer à partager toutes les données protégées en tant que secrets d'affaires autres que ces données spécifiques.

5.4.2. Si, dans des circonstances exceptionnelles, il est hautement probable que le détenteur de données subisse un préjudice économique grave du fait de la divulgation à l'utilisateur de certaines données protégées en tant que secret d'affaires malgré la mise en œuvre des mesures de protection de l'utilisateur et des mesures de protection du détenteur de données, ce dernier peut refuser ou suspendre le partage des données spécifiques en question.

Le détenteur de données doit adresser, sans retard injustifié, une notification dûment motivée à l'utilisateur et à l'autorité compétente désignée en vertu de l'article 37 du règlement sur les données.

Toutefois, le détenteur de données doit continuer à partager toutes les données protégées en tant que secrets d'affaires autres que ces données spécifiques.

Le refus ou la suspension du partage de données au titre de l'article 4 du règlement (UE) 2023/2854 est limité à des circonstances exceptionnelles. Par conséquent, la notification doit être dûment motivée. Les aspects à prendre en compte peuvent être, par exemple, l'absence d'applicabilité de la protection des secrets d'affaires dans les pays tiers, la nature et le niveau de confidentialité du secret d'affaires en question ou le caractère unique et novateur du produit connecté concerné.

5.4.3. Si l'utilisateur ne met pas en œuvre et ne maintient pas les mesures de protection de l'utilisateur et si ce manquement est dûment justifié par le détenteur de données, par exemple dans un rapport d'audit de sécurité, le détenteur de données a le droit de bloquer ou de suspendre la transmission des secrets d'affaires définis spécifiques jusqu'à ce que l'utilisateur ait résolu l'incident.

Dans ce cas, le détenteur de données doit adresser, sans retard injustifié et par écrit, une notification dûment motivée à l'utilisateur et à l'autorité compétente désignée en vertu de l'article 37 du règlement sur les données.

5.4.4. La clause 5.4.1 n'autorise pas le détenteur de données à résilier le présent contrat.

Les clauses 5.4.2 ou 5.4.3 autorisent le détenteur de données à résilier le présent contrat uniquement en ce qui concerne les secrets d'affaires définis spécifiques, et si:

(a) toutes les conditions de la clause 5.4.2 ou de la clause 5.4.3 sont remplies;

(b) aucune solution n'a été trouvée par les parties après un délai raisonnable, malgré une tentative de trouver une solution à l'amiable, y compris après l'intervention de l'autorité compétente désignée en vertu de l'article 37 du règlement sur les données; et

(c) l'utilisateur n'a pas obtenu d'une juridiction compétente une décision de justice obligeant le détenteur de données à mettre les données à disposition et aucune procédure judiciaire n'est en cours pour obtenir une telle décision.

5.5. **Fin de la production et destruction de biens non conformes**

Sans préjudice d'autres voies de recours dont dispose le détenteur de données conformément au présent contrat ou au droit applicable, si l'utilisateur modifie ou supprime les mesures techniques de protection appliquées par le détenteur de données ou ne maintient pas les mesures techniques et organisationnelles qu'il a prises en accord avec le détenteur de données conformément aux clauses 5.2 et 5.3, le détenteur de données peut demander à l'utilisateur:

(a) d'effacer les données mises à disposition par le détenteur de données ou les éventuelles copies de celles-ci; et/ou

(b) de mettre fin à la production, à l'offre ou à la mise sur le marché ou à l'utilisation de biens, de données dérivées ou de services produits sur la base des connaissances obtenues au moyen des secrets d'affaires définis, ou à l'importation, à l'exportation ou au stockage de biens non conformes destinés aux fins précitées, et de détruire tout bien non conforme, lorsqu'il existe un risque grave que l'utilisation illicite de ces données cause un préjudice important au détenteur de données ou au détenteur de secrets d'affaires ou lorsqu'une telle mesure ne serait pas disproportionnée au regard des intérêts du détenteur de données ou du détenteur de secrets d'affaires; et/ou

(c) d'indemniser une partie lésée par l'utilisation abusive ou la divulgation de ces données auxquelles il a été accédé illégalement ou qui ont été utilisées illégalement.

5.6. **Conservation de données protégées en tant que secrets d'affaires définis**

5.6.1. Lorsque le détenteur de données exerce le droit de refuser, de bloquer ou de suspendre le partage de données avec l'utilisateur conformément aux clauses 5.4.1, 5.4.2 et 5.4.3, il devra veiller à ce que les données en question soient conservées, de sorte que lesdites données soient mises à la disposition de l'utilisateur:

(a) une fois que les protections appropriées ont été convenues et mises en œuvre; ou

(b) une fois qu'une décision contraignante est rendue par une autorité ou une juridiction compétente exigeant du détenteur de données qu'il fournisse les données à l'utilisateur.

Cette obligation de conservation prend fin lorsqu'une autorité compétente ou une juridiction, dans une décision contraignante, autorise la suppression de ces données conservées ou lorsque le contrat prend fin.

5.6.2. Le détenteur de données supportera les coûts nécessaires à la conservation des données en vertu de la clause 5.6.1. Toutefois, l'utilisateur couvrira ces coûts dans la mesure où le blocage ou la suspension du partage des données a lieu conformément à la clause 5.4.3.

6. **(si les données sont mises à disposition par le détenteur de données à la demande de l'utilisateur) Utilisation des données par l'utilisateur**

6.1. **Utilisation et partage licites des données**

6.1.1. L'utilisateur peut utiliser les données mises à disposition par le détenteur de données à sa demande pour toute finalité licite et/ou, dans la mesure où les données sont transférées à l'utilisateur ou peuvent être récupérées par celui-ci, partager librement les données, sous réserve des limitations prévues à la clause 6.2.

6.2. **Restrictions à l'utilisation et au partage des données**

6.2.1. L'utilisateur s'engage à:

(a) ne pas se servir des données pour mettre au point un produit connecté concurrençant le produit, ni partager les données avec un tiers à cette fin;

(b) ne pas utiliser ces données pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du fabricant ou, le cas échéant, du détenteur de données;

(c) s'abstenir d'avoir recours à des moyens coercitifs ou de tirer avantage de lacunes dans l'infrastructure technique du détenteur de données qui est destinée à protéger les données pour obtenir l'accès aux données;

(d) partager les données avec un tiers considéré comme contrôleur d'accès en vertu de l'article 3 du règlement (UE) 2022/1925.

6.2.2. [OPTION] [En outre, et conformément à l'article 4, paragraphe 2, du règlement sur les données, l'utilisateur et le détenteur de données conviennent de limiter ou d'interdire comme suit le traitement suivant (*veuillez préciser le traitement concerné: accès, utilisation et/ou partage ultérieur des données*), ayant pour conséquence de compromettre les exigences de sécurité applicables au produit, telles qu'elles sont prévues par le droit de l'Union (*veuillez préciser l'exigence de sécurité juridique concernée*), entraînant de graves effets indésirables pour la santé, la sûreté ou la sécurité des personnes physiques.

L'utilisateur s'engage à ne pas (veuillez préciser les restrictions ou interdictions pertinentes liées au traitement susmentionné).]

7. **Partage de données à la demande de l'utilisateur avec un destinataire de données**

7.1. **Mise des données à la disposition d'un destinataire de données**

7.1.1. Les données, ainsi que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, doivent être mises à la disposition d'un destinataire de données par le détenteur de données, sans frais pour l'utilisateur, sur demande présentée par l'utilisateur ou une partie agissant pour son compte. La demande peut être introduite au moyen du formulaire figurant à l'**appendice 3**, envoyé à (*décrire la procédure de demande simple par voie électronique lorsque cela est techniquement possible*). Afin de vérifier que la demande est faite par l'utilisateur, le détenteur de données n'est pas tenu de fournir d'autres informations que celles qui sont nécessaires.

7.1.2. Lorsque l'utilisateur n'est pas la personne concernée, le détenteur de données ne met les données qui sont des données à caractère personnel à la disposition d'un tiers à la suite d'une demande de l'utilisateur que s'il existe un fondement juridique valable pour la mise à disposition de données à caractère personnel au titre de l'article 6 du règlement (UE) 2016/679 (RGPD) et, le cas échéant, si les conditions énoncées à l'article 9 dudit règlement et à l'article 5, paragraphe 3, de la directive 2002/58/CE (directive vie privée et communications électroniques) sont remplies.

À cet égard, lorsque l'utilisateur n'est pas la personne concernée, il doit indiquer au détenteur de données, dans chaque demande présentée au titre de la clause précédente, la base juridique du traitement au titre de l'article 6 du règlement (UE) 2016/679 (et, le cas échéant, la dérogation applicable au titre de l'article 9 dudit règlement et de l'article 5, paragraphe 3, de la directive 2002/58/CE) sur laquelle se fonde la demande de mise à disposition de données à caractère personnel.

7.1.3. Le détenteur de données doit mettre les données à la disposition d'un destinataire de données, les données étant au moins de la même qualité que lorsqu'elles ont été mises à la disposition du détenteur de données et, en tout état de cause, dans un format complet, structuré, couramment utilisé et lisible par machine, de manière aisée et sécurisée.

7.1.4. Lorsque l'utilisateur soumet une telle demande, le détenteur de données convient avec le destinataire de données des modalités de mise à disposition des données conformément aux chapitres III et IV du règlement sur les données.

7.1.5. L'utilisateur reconnaît qu'une demande au titre de la clause 7.1.1 ne peut bénéficier à un tiers considéré comme un contrôleur d'accès en vertu de l'article 3 du règlement (UE) 2022/1925 [OPTION] [et ne peut pas être présentée dans le cadre de l'expérimentation de nouveaux produits, substances ou processus connectés qui ne sont pas encore mis sur le marché].

7.1.6. L'utilisateur reconnaît que le tiers ne traite les données mises à sa disposition conformément à la clause 7.1.1 que pour les finalités et dans les conditions convenues avec l'utilisateur. Le détenteur de données ne peut être tenu responsable envers l'utilisateur de l'absence d'un tel accord entre l'utilisateur et le tiers, sauf s'il a eu ou aurait dû avoir connaissance de cette absence.

8. **[OPTION si l'utilisateur est une entité commerciale] Limitations des droits de l'utilisateur**

L'utilisateur accepte (*veuillez préciser la finalité, la nature et la durée de la limitation du droit de l'utilisateur d'utiliser ou de partager les données et indiquer la partie des données concernée par ces limitations*).

Conformément à l'article 7, paragraphe 2, du règlement sur les données, «toute clause contractuelle qui, au détriment de l'utilisateur, exclut l'application des droits de l'utilisateur au titre du [chapitre II], y déroge ou en modifie les effets, n'est pas contraignante pour l'utilisateur».

Il convient de lire cette disposition à la lumière du considérant 25 qui précise que cela «n'empêche pas les utilisateurs, dans le cas de relations entre entreprises, de mettre des données à la disposition de tiers ou de détenteurs de données en vertu de toute disposition contractuelle légale, y compris en acceptant de limiter ou de restreindre le partage ultérieur de ces données, ou d'être indemnisés proportionnellement, par exemple en échange d'une renonciation à leur droit d'utiliser ou de partager ces données».

Par conséquent, ces limitations ne seront valables que si elles ne causent aucun préjudice à l'utilisateur, ce qui signifie que les limitations ne devraient pas nuire aux intérêts légitimes de l'utilisateur.

En outre, cette clause ne devrait pas être utilisée pour priver entièrement l'utilisateur de ses droits légaux au titre des articles 4 et 5 du règlement sur les données, par exemple en renonçant complètement à son droit d'accès aux données. L'utilisateur ne peut accepter des limitations de ses droits que lorsque celles-ci sont limitées dans leur portée et dans le temps. Elles ne doivent pas porter préjudice à l'utilisateur. Il pourrait s'agir, par exemple, de limitations spécifiques de l'utilisation des données auxquelles l'accès a été accordé, ou d'un engagement à ne pas partager ultérieurement les données avec un tiers, comme indiqué au considérant 25, ou à ne pas laisser un destinataire de données partager ultérieurement les données avec un tiers.

Cette clause pourrait être utilisée lorsque l'utilisateur est intéressé par de telles limitations, par exemple lorsque le détenteur de données et l'utilisateur participent à un projet industriel conjoint.

Elle pourrait également s'appliquer si l'utilisateur est indemnisé. Toutefois, le simple fait de recevoir une compensation ne suffirait pas en soi à considérer que les limitations ne portent pas préjudice à l'utilisateur. Cette compensation devrait être proportionnée aux limitations.

L'utilisateur peut, à sa seule discrétion, accepter ou refuser la ou les limitations prévues par la présente clause.

9. **Compensation de l'utilisateur**

9.1. **Compensation**

Le détenteur de données s'engage à accorder une compensation à l'utilisateur comme indiqué en détail à l'**appendice 7** (*le cas échéant*), y compris pour les limitations des droits de l'utilisateur conformément à la clause 8.

Les parties peuvent convenir d'une compensation pour l'utilisation et le partage des données par le détenteur de données, lorsqu'elles le jugent équitable et raisonnable. Elles peuvent, par exemple, envisager une telle compensation si le détenteur de données utilise les données pour mettre au point de nouveaux produits ou services ou si le détenteur de données crée des données agrégées ou dérivées à des fins commerciales. À l'inverse, si, par exemple, les données sont utilisées exclusivement pour les besoins de tout accord conclu avec l'utilisateur ou pour assurer le fonctionnement, la sûreté et la sécurité du produit ou du service connexe, aucune compensation ne sera prévue.

Toutefois, les parties devraient tenir compte du fait que si, par exemple, l'utilisateur limite ses droits conformément à la clause 8, il devrait recevoir une compensation, comme expliqué dans l'encadré explicatif de la clause 8, et que celle-ci devrait être proportionnée à la gravité de la limitation.

De même, une compensation pourrait être nécessaire pour garantir le traitement équitable de l'utilisateur, si celui-ci accepte que le détenteur de données puisse vendre les données à des tiers conformément à la clause 3.2.1, point a) iii).

Si une compensation est due, les parties doivent s'accorder sur sa nature, qui peut être monétaire ou non.

9.2. **(applicable à une compensation financière) Intérêts en cas de retard de paiement**

En cas de retard dans le paiement de la compensation, le détenteur de données devrait verser à l'utilisateur des intérêts sur la compensation exigible à compter de la date d'échéance du paiement jusqu'à la date du paiement, conformément au droit applicable.

10. **Transfert de l'utilisation et utilisateurs multiples**

L'utilisateur initial peut transférer de manière permanente la propriété du produit ou son droit d'utiliser le produit à un utilisateur ultérieur, par exemple lorsque l'utilisateur vend le produit (transfert de l'utilisation).

L'utilisateur initial peut également accorder des droits afin d'utiliser le produit et/ou de recevoir des services connexes à des utilisateurs supplémentaires, tout en conservant son rôle d'utilisateur (utilisateurs multiples), par exemple dans les cas suivants:

— lorsqu'une entreprise sous-loue sa camionnette à une autre entreprise pendant certaines périodes de l'année;

— lorsqu'une société de location de voitures loue ses voitures à des clients.

Droit du détenteur de données d'utiliser les données

Dans ce cas, le détenteur de données doit conclure un contrat avec les utilisateurs ultérieurs ou supplémentaires afin de pouvoir utiliser les données générées par l'utilisation du produit ou des services connexes par ces utilisateurs. Les clauses ci-dessous proposent des solutions possibles pour la conclusion d'un tel contrat, afin que les parties puissent choisir la solution la plus adaptée aux spécificités de la situation.

En cas de transfert, les parties pourraient par exemple convenir que l'utilisateur initial notifie au détenteur de données le transfert, l'identité et les coordonnées de l'utilisateur ultérieur afin que le détenteur de données puisse contacter l'utilisateur ultérieur et conclure un contrat avec lui.

Dans le cas d'utilisateurs multiples, une telle solution pourrait être trop lourde pour le détenteur de données. Si l'utilisateur initial est en mesure d'agir pour le compte du détenteur de données, il est donc possible qu'il obtienne l'accord des utilisateurs supplémentaires sur les conditions d'accès aux données et d'utilisation de celles-ci énoncées dans le présent contrat.

Dans d'autres cas, il peut toujours être possible et préférable que l'utilisateur initial communique au détenteur de données les coordonnées d'un utilisateur supplémentaire, de sorte que le détenteur de données puisse conclure un contrat directement avec l'utilisateur supplémentaire.

Il est également possible que le détenteur de données n'ait pas besoin d'être informé de l'existence d'un utilisateur ultérieur ou supplémentaire par l'utilisateur initial afin de conclure un contrat, car les circonstances sont telles qu'il peut conclure un contrat sans aucune intervention de la part de l'utilisateur initial. Par exemple, il peut arriver que la création d'un compte identifiant l'utilisateur soit nécessaire pour utiliser le produit et/ou le service connexe. Si tel est le cas, le détenteur de données sera en mesure de conclure un contrat avec l'utilisateur ultérieur ou supplémentaire lorsque celui-ci créera son propre compte. Toutefois, cela pourrait exiger de l'utilisateur initial qu'il veille à ce que l'utilisateur ultérieur ou supplémentaire n'utilise pas son compte.

Droits d'accès des parties en cas de transfert de l'utilisation et d'utilisateurs multiples

En cas de transfert de l'utilisation ou d'utilisateurs multiples, le contrat devrait permettre de déterminer avec certitude qui peut accéder aux données et à quelles conditions. Par exemple, lorsqu'une entreprise (l'utilisateur initial) loue des machines agricoles connectées à des agriculteurs individuels (utilisateurs supplémentaires) sur une base quotidienne ou hebdomadaire, les données générées par les machines agricoles peuvent divulguer des informations commerciales sensibles de ces agriculteurs. Le fabricant (le détenteur de données) ne peut pas simplement mettre des données au titre de la clause 4 du présent contrat à la disposition de l'utilisateur initial (la société propriétaire des machines) sans s'assurer que, ce faisant, aucune information confidentielle ni aucun droit des agriculteurs individuels (les utilisateurs supplémentaires) ne sont violés.

Les droits d'accès de l'utilisateur supplémentaire ou ultérieur peuvent notamment dépendre d'une catégorisation contractuelle des données, par exemple:

— données supprimables de l'utilisateur — les produits ou services connexes permettent souvent à l'utilisateur de supprimer les données générées au cours de leur utilisation. En cas de transfert, l'utilisateur devrait supprimer ces données. Dans le cas contraire, ces données peuvent être accessibles à l'utilisateur supplémentaire ou ultérieur;

— données toujours supprimables — les données que le détenteur de données ne devrait pas rendre accessibles à l'utilisateur supplémentaire ou ultérieur;

— données résiduelles — les données autres que les données supprimables ou toujours supprimables de l'utilisateur; ces données ne seront pas supprimables et ne feront pas l'objet d'un accord de confidentialité (autrement dit, les données seront également accessibles aux nouveaux utilisateurs ultérieurs). Ces données peuvent comprendre les données qui doivent être accessibles à l'utilisateur supplémentaire ou ultérieur en vertu de la loi ou dans la pratique (par exemple, en ce qui concerne les mises à jour effectuées dans un véhicule connecté).

Le détenteur de données doit classer les données dans ces catégories, en particulier dans les informations visées à l'article 3, paragraphes 2 et 3, du règlement sur les données, dans le présent contrat (par exemple, à l'appendice 1) ou dans la documentation relative au produit ou au service connexe.

La présente clause 10 porte sur le règlement sur les données; elle n'a pas d'incidence sur d'autres législations, notamment les législations sectorielles, qui pourraient réglementer le transfert d'un produit connecté ou d'un service connexe (par exemple, le retraitement des dispositifs médicaux).

10.1. **Transfert de l'utilisation**

Lorsque l'utilisateur transfère contractuellement i) la propriété du produit, ou ii) ses droits temporaires d'utilisation du produit, et/ou iii) ses droits de recevoir des services connexes à une personne ultérieure (l'«utilisateur ultérieur») et perd le statut d'utilisateur après le transfert, les parties s'engagent à respecter les exigences énoncées dans la présente clause.

[OPTION 1] [L'utilisateur initial doit notifier le transfert au détenteur de données et fournir les coordonnées nécessaires de l'utilisateur ultérieur, afin que le détenteur de données puisse conclure avec lui un contrat concernant l'utilisation des données par le détenteur de données.]

[OPTION 2] [Le détenteur de données prend les mesures nécessaires pour conclure un contrat avec l'utilisateur ultérieur concernant l'utilisation des données par le détenteur de données. (*le cas échéant*) L'utilisateur initial doit veiller à ce que l'utilisateur ultérieur ne puisse pas utiliser le compte de l'utilisateur initial.]

Les droits du détenteur de données d'utiliser les données relatives au produit ou les données relatives aux services connexes générées avant le transfert ne seront pas altérés par un transfert, c'est-à-dire que les droits et obligations relatifs aux données transférées en vertu du contrat avant le transfert se poursuivront après celui-ci.

10.2. **Utilisateurs multiples**

Lorsque l'utilisateur initial accorde le droit d'utiliser le produit et/ou le ou les services connexes à une autre partie (ci-après l'«utilisateur supplémentaire») tout en conservant son statut d'utilisateur, les parties s'engagent à se conformer aux exigences énoncées dans la présente clause.

10.2.1. Accord de l'utilisateur supplémentaire sur l'utilisation et le partage des données par le détenteur de données

[OPTION 1] [Dans le contrat entre l'utilisateur initial et l'utilisateur supplémentaire, l'utilisateur initial prévoit, pour le compte du détenteur de données, des clauses reflétant en substance le contenu du présent contrat entre l'utilisateur initial et le détenteur de données, et notamment la clause 3 sur l'utilisation et le partage des données relatives au produit et/ou au service connexe par le détenteur de données, pendant la durée de l'utilisation temporaire du produit et/ou du service connexe.]

[OPTION 2] [L'utilisateur initial notifie au détenteur de données l'existence et la durée des droits de l'utilisateur supplémentaire d'utiliser le produit et/ou le service connexe et communique ses coordonnées, afin que le détenteur de données puisse conclure un accord avec l'utilisateur supplémentaire sur l'utilisation et le partage de ces données par le détenteur de données.]

[OPTION 3] [Le détenteur de données prend les mesures nécessaires pour conclure un accord avec l'utilisateur supplémentaire. (*le cas échéant*) L'utilisateur initial doit veiller à ce que l'utilisateur supplémentaire ne puisse pas utiliser le compte de l'utilisateur initial.]

10.2.2. Accès aux données par l'utilisateur supplémentaire

[OPTION] [L'utilisateur initial fait office de premier point de contact pour l'utilisateur supplémentaire, si celui-ci présente une demande d'accès aux données en vertu des articles 4 ou 5 du règlement sur les données. Le détenteur de données doit collaborer avec l'utilisateur initial pour répondre à la demande, comme spécifié à l'**appendice 10**.]

10.3. **Responsabilité de l'utilisateur initial**

Dans la mesure où le non-respect par l'utilisateur initial des obligations qui lui incombent en vertu des clauses 10.1 et 10.2 entraîne l'utilisation et le partage des données relatives au produit ou aux services connexes par le détenteur de données en l'absence de contrat avec l'utilisateur ultérieur ou supplémentaire, l'utilisateur initial indemnisera le détenteur de données pour toute demande d'indemnisation introduite par l'utilisateur ultérieur ou supplémentaire à l'encontre du détenteur de données pour son utilisation des données après le transfert ou l'utilisation temporaire du produit et/ou du ou des services connexes.

11. **Date d'application, durée du contrat et résiliation**

11.1. **Date d'application et durée**

Le présent contrat n'existerait généralement pas en tant que contrat autonome, mais serait conclu parallèlement au contrat transférant la propriété du produit à l'utilisateur, lui conférant des droits temporaires d'utilisation du produit et/ou au contrat relatif à un service connexe.

En règle générale, le présent contrat doit rester en vigueur aussi longtemps que cet autre contrat permet à l'utilisateur d'utiliser le produit ou le service connexe. De même, ni le détenteur de données ni l'utilisateur ne devraient pouvoir résilier le présent contrat, sauf en cas de violation substantielle des obligations par l'autre partie, car cela aboutirait à une situation dans laquelle l'utilisateur utiliserait le produit et/ou le service connexe sans aucun cadre contractuel concernant les droits et obligations au titre du règlement sur les données.

11.1.1. Le présent contrat [OPTION 1] [prend effet immédiatement] [OPTION 2] [prend effet à compter du (*préciser la date*)].

11.1.2. Le contrat est conclu pour [OPTION 1] [une durée indéterminée] [OPTION 2] [une durée déterminée de (*préciser*)], sous réserve de tout motif d'expiration ou de résiliation en vertu du présent contrat.

11.2. **Résiliation**

Indépendamment de la période contractuelle convenue en vertu de la clause 11.1, le présent contrat prend fin:

(a) lors de la destruction du produit ou de l'arrêt définitif du service connexe, ou lorsque le produit ou le service connexe perd sa capacité à générer les données de manière irréversible; ou

(b) lorsque l'utilisateur perd la propriété du produit ou lorsque les droits de l'utilisateur à l'égard du produit dans le cadre d'un contrat de location, de crédit-bail ou d'un accord similaire ou les droits de l'utilisateur à l'égard du service connexe prennent fin; ou

(c) lorsque les deux parties en conviennent.

Les points b) et c) sont sans préjudice du contrat restant en vigueur entre le détenteur de données et tout utilisateur ultérieur ou supplémentaire.

11.3. **Effets de l'expiration et de la résiliation**

11.3.1. L'expiration de la période contractuelle ou la résiliation du présent contrat libère les deux parties de leur obligation d'exécuter et de recevoir une exécution future, mais n'a pas d'incidence sur les droits et obligations acquis jusqu'au moment de la résiliation.

L'expiration ou la résiliation n'a pas d'incidence sur les dispositions du présent contrat qui restent applicables même après la fin du contrat, en particulier la clause 13.1 relative à la confidentialité, la clause 13.4 relative au droit applicable et la clause 13.6 relative au règlement des litiges.

11.3.2. La résiliation ou l'expiration du contrat aura les effets suivants:

(a) le détenteur de données cesse d'extraire les données générées ou enregistrées à la date de résiliation ou d'expiration;

(b) le détenteur de données conserve le droit d'utiliser et de partager les données générées ou enregistrées avant la date de résiliation ou d'expiration prévue dans le présent contrat.

12. **Voies de recours en cas de violation du contrat**

Les parties peuvent souhaiter s'entendre non seulement sur les droits et obligations spécifiques aux données (dont beaucoup découlent déjà du règlement sur les données), mais aussi sur des questions de droit général des contrats, telles que les droits et voies de recours d'une partie contractante en cas d'inexécution de la part de l'autre partie contractante.

En ce qui concerne ces questions de droit général des contrats, les parties peuvent souhaiter se fonder sur des règles légales par défaut ou sur d'autres modèles de contrat. Si elles souhaitent utiliser les présentes clauses contractuelles types, elles doivent s'assurer qu'elles sont compatibles avec toute autre loi nationale impérative susceptible d'être applicable au contrat.

12.1. **Cas d'inexécution**

12.1.1. L'inexécution d'une obligation par une partie est essentielle pour le présent contrat si:

(a) elle prive substantiellement l'autre partie de ce qu'elle était en droit d'attendre du présent contrat, à moins que la partie défaillante n'ait pas prévu et n'ait pas pu raisonnablement prévoir ce résultat; ou

(b) il ressort clairement des circonstances que l'on ne peut pas compter dans l'avenir sur une exécution par la partie défaillante.

12.1.2. Une partie est exonérée des conséquences de l'inexécution lorsque celle-ci est due à un empêchement qui lui échappe et que l'on ne pouvait raisonnablement attendre de cette partie qu'elle le prenne en considération au moment de la conclusion du présent contrat, ou qu'elle le prévienne ou le surmonte ou qu'elle en prévienne ou en surmonte les conséquences.

Lorsque l'empêchement exonératoire n'est que temporaire, l'exonération d'inexécution vaut pour la durée de l'empêchement. Cependant, si le retard équivaut à une inexécution essentielle, l'autre partie peut le traiter comme telle.

La partie défaillante doit faire en sorte que l'autre partie reçoive, sans retard excessif, notification de l'empêchement et de ses effets sur sa capacité de s'exécuter à partir du moment où la partie défaillante a eu, ou a pu avoir raisonnablement connaissance de ces circonstances. L'autre partie a droit à des dommages et intérêts en réparation du préjudice économique résultant de la non-réception de cette notification.

12.2. **Voies de recours**

12.2.1. En cas d'inexécution par une partie, l'autre partie dispose des voies de recours énumérées dans les clauses suivantes, sans préjudice des voies de recours prévues par le droit applicable.

12.2.2. Les moyens d'action qui ne sont pas incompatibles peuvent être cumulés.

12.2.3. Une partie ne peut recourir à aucun moyen d'action dans la mesure où elle a provoqué l'inexécution de l'autre partie, par exemple lorsqu'une défaillance dans sa propre infrastructure de données n'a pas permis à l'autre partie de s'acquitter dûment de ses obligations. Une partie ne peut pas non plus introduire une demande de dommages et intérêts dans la mesure où elle aurait pu réduire son préjudice en prenant des mesures raisonnables.

12.2.4. La partie lésée peut:

(a) demander à la partie défaillante de se conformer, sans retard injustifié, aux obligations qui lui incombent en vertu du présent contrat, à moins que cela ne soit illicite ou impossible ou qu'une exécution spécifique n'entraîne pour la partie défaillante des coûts disproportionnés par rapport au bénéfice que l'autre partie en retirerait;

(b) demander à la partie défaillante d'effacer les données auxquelles elle a eu accès ou qui ont été utilisées en violation du présent contrat et les éventuelles copies de celles-ci;

(c) demander des dommages et intérêts pour le préjudice économique qui lui a été causé par l'inexécution de l'autre partie et qui ne bénéficie pas d'une exonération en vertu de la clause 12.1.2. La partie défaillante n'est responsable que des dommages qu'elle avait prévus ou qu'elle aurait raisonnablement dû prévoir au moment de la conclusion du présent contrat en raison de son inexécution, sauf si celle-ci était intentionnelle ou résultait d'une négligence grave.

12.2.5. Le détenteur de données peut également suspendre le partage de données avec l'utilisateur jusqu'à ce que ce dernier se conforme à ses obligations ou à ses restrictions, en adressant à l'utilisateur une notification dûment motivée sans retard injustifié:

a) si l'inexécution des obligations de l'utilisateur est essentielle;

b) *(le cas échéant)* pour autant que toutes les autres conditions énoncées à la clause 5.4.3 soient remplies, dans les cas décrits à la clause 5.4.3.

12.2.6. L'utilisateur peut également:

(a) suspendre l'accord donné au détenteur de données en vertu de la clause 3 ou son accord sur les limitations des droits de l'utilisateur convenues en vertu de la clause 8, jusqu'à ce que le détenteur de données se conforme à ses obligations, à moins que cela ne cause au détenteur de données un préjudice manifestement disproportionné par rapport à l'inexécution ou à ses effets;

(b) retirer l'autorisation donnée au détenteur de données en vertu de la clause 3 et/ou son accord sur les limitations des droits de l'utilisateur convenues en vertu de la clause 8, en adressant une notification au détenteur de données, si:

i) l'inexécution du détenteur de données est essentielle; ou

ii) dans le cas d'une inexécution qui n'est pas essentielle, l'utilisateur a, par notification, imparti un délai raisonnable pour remédier à l'inexécution et ce délai a expiré sans que le détenteur de données ne se soit exécuté. Le délai est considéré comme étant raisonnable si le détenteur de données ne le conteste pas sans retard excessif.

12.2.7. [OPTION] [Lorsqu'une partie n'exécute pas les obligations qui lui incombent en vertu du présent contrat, elle s'acquitte, en tout état de cause, des pénalités exposées en détail à l'appendice 8, que les parties considèrent comme des dommages et intérêts au sens de la clause 12.2.4, point c). La partie défaillante a le droit de demander que la pénalité soit réduite à un montant raisonnable lorsqu'elle peut prouver que celle-ci est manifestement excessive par rapport au préjudice résultant de l'inexécution.]

Les parties peuvent souhaiter définir des sanctions pour certains types d'inexécution, car il peut être trop onéreux pour la partie lésée de prouver le montant du préjudice réel causé, par exemple, par un défaut de fourniture de données. Les sanctions devraient être proportionnées.

13. **Disposition générale**

13.1. **Confidentialité**

13.1.1. Les informations suivantes seront considérées comme confidentielles:

(a) les informations relatives aux secrets d'affaires, à la situation financière ou à tout autre aspect des activités d'une partie, sauf si cette partie a rendu ces informations publiques;

(b) les informations relatives à l'utilisateur et à tout tiers, sauf s'ils ont déjà rendu ces informations publiques.

13.1.2. Les deux parties conviennent de prendre toutes les mesures raisonnables pour conserver en toute sécurité les informations confidentielles et de ne pas les mettre à la disposition d'un tiers, sauf dans les cas suivants:

(a) si l'une des parties a l'obligation légale de fournir ou de mettre à disposition les informations pertinentes;

(b) s'il est nécessaire que l'une des parties mette à disposition les informations pertinentes pour s'acquitter des obligations qui lui incombent en vertu du présent contrat; ou

(c) si l'une des parties a obtenu le consentement préalable de l'autre partie ou de la partie qui a fourni les informations confidentielles ou qui est concernée par leur divulgation.

13.1.3. Ces obligations de confidentialité restent applicables après la résiliation du contrat pendant une durée de (*préciser la durée*).

13.1.4. Ces obligations de confidentialité ne suppriment aucune des obligations plus strictes au titre i) du règlement (UE) 2016/679 (RGPD), ii) des dispositions mettant en œuvre la directive 2002/58/CE ou la directive (UE) 2016/943, ou iii) de toute autre disposition du droit de l'Union ou du droit d'un État membre, iv) (le cas échéant) de la clause 6 du présent contrat.

13.2. **Moyens de communication**

Toute notification ou autre communication requise par le présent contrat doit être effectuée par écrit et peut être remise en main propre, envoyée par courrier prépayé ou transmise par voie électronique, y compris par courrier électronique, à condition que l'expéditeur conserve la preuve de l'envoi aux adresses énumérées ci-dessous:

Partie	Personne de contact	Adresse électronique	Numéro de téléphone	Adresse
Utilisateur	[Nom]/[Fonction]	[Adresse électronique]	[Numéro de téléphone]	[Adresse]
Destinataire de données	[Nom]/[Fonction]	[Adresse électronique]	[Numéro de téléphone]	[Adresse]

Toute notification ou communication de ce type est réputée reçue:

(a) en cas de remise en main propre, à la date de livraison;

(b) en cas d'envoi par courrier prépayé, le troisième jour ouvrable suivant l'envoi;

(c) en cas d'envoi par voie électronique, à la date de transmission, à condition qu'aucun message d'erreur indiquant un défaut de transmission n'ait été reçu par l'expéditeur.

13.3. **Contrat indivisible, modifications et caractère détachable**

13.3.1. Le présent contrat (ainsi que ses appendices et tout autre document visé dans le contrat) constitue le contrat indivisible conclu entre les parties concernant l'objet du présent contrat et annule et remplace tous les contrats ou accords et protocoles antérieurs, oraux et écrits, entre les parties concernant l'objet du présent contrat.

13.3.2. Toute modification du présent contrat n'est valable que si elle est approuvée par écrit, y compris sous une forme électronique.

13.3.3. Si une disposition du présent contrat est déclarée nulle, invalide, annulable ou inapplicable pour quelque raison que ce soit, et si cette disposition est détachable des autres clauses du contrat, ces autres dispositions resteront valables et exécutoires. Toute lacune ou ambiguïté qui en résulterait dans le présent contrat sera traitée conformément à la clause 13.5.

13.4. **Droit applicable**

13.4.1. Le présent contrat est régi par le droit de (*préciser l'État membre*).

13.5. **Interprétation**

13.5.1. Le présent contrat est conclu par les parties dans le cadre de leurs droits et obligations au titre du règlement sur les données. Les dispositions du présent contrat doivent être interprétées dans le sens de leur conformité avec le règlement sur les données et d'autres dispositions du droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union, ainsi qu'avec toute disposition du droit national applicable qui est compatible avec le droit de l'Union et auquel il ne peut être dérogé par accord.

13.5.2. Si une lacune ou une ambiguïté dans le présent contrat ne peut être résolue de la manière visée à la clause 13.5.1, le présent contrat doit être interprété à la lumière des règles d'interprétation prévues par le droit applicable (voir clause 13.4).

13.6. **Règlement des litiges**

13.6.1. Les parties conviennent de tout mettre en œuvre pour régler les litiges à l'amiable et, avant de porter une affaire devant une juridiction, de soumettre leur litige à (*insérer le nom et les coordonnées d'un organisme particulier de règlement des litiges; pour les litiges relevant de leur compétence telle que définie à l'article 10, paragraphe 1, du règlement sur les données, il peut s'agir de tout organisme de règlement des litiges d'un État membre qui remplit les conditions énoncées à l'article 10 du règlement sur les données).*

13.6.2. La soumission d'un litige à un organisme de règlement des litiges conformément à la clause 13.6.1 ne porte toutefois pas atteinte au droit de l'utilisateur de déposer une plainte auprès de l'autorité nationale compétente désignée en vertu de l'article 37 du règlement sur les données, ni au droit d'une partie de former un recours effectif devant une juridiction d'un État membre.

13.6.3. [OPTION, si l'utilisateur est une entreprise] [Les tribunaux de (*préciser l'État membre*) seront seuls compétents pour connaître de l'affaire concernant le présent contrat.]

Appendice 1

Présentation détaillée des données couvertes par le présent contrat et des modalités d'accès

Dans le présent appendice, les parties doivent présenter de manière détaillée les données couvertes par le présent contrat, les modalités d'accès et les moyens et informations nécessaires pour accéder aux données et les utiliser, conformément aux clauses 2 et 3.

A. **Spécification du contenu des données**

L'appendice devrait d'abord trier et énumérer les données relatives au produit et les données relatives au service connexe couvertes par le contrat, en indiquant le contenu des données et la fréquence de collecte, afin que l'utilisateur soit informé de manière précise des informations contenues dans les données (liste structurée de points de données ou catégories précises de données).

B. **Durée de conservation**

L'appendice devrait ensuite indiquer la durée de conservation, afin que l'utilisateur soit informé de la durée de disponibilité des données. Cela peut se faire de manière détaillée pour chaque point de données ou groupe de points de données.

C. **Régime des données**

L'appendice devrait préciser ici si tout ou partie des données sont des données particulières régies par un régime particulier. L'appendice pourrait, par exemple, indiquer si les données peuvent être considérées comme des données à caractère personnel et, le cas échéant, lesquelles.

D. **Structure et format des données**

L'appendice devrait préciser ici dans quel format structuré, couramment utilisé et lisible par machine les données sont mises à disposition.

E. **Politique en matière d'accès**

Il peut arriver que l'utilisateur transfère ses droits d'utiliser le produit ou de recevoir des services connexes à un utilisateur ultérieur ou que plusieurs utilisateurs partagent ces droits. Dans de tels cas, les parties devraient préciser ici les droits d'accès aux données en cas de transfert de l'utilisation du produit ou en cas d'utilisateurs multiples. L'appendice pourrait notamment énumérer:

— les données supprimables de l'utilisateur — les produits ou services connexes permettent souvent à l'utilisateur de supprimer les données générées au cours de leur utilisation. En cas de transfert, l'utilisateur devrait supprimer ces données. Dans le cas contraire, ces données peuvent être accessibles à l'utilisateur ultérieur;

— les données toujours supprimables — les données que le détenteur de données ne devrait pas rendre accessibles à l'utilisateur ultérieur;

— les données résiduelles — les données autres que les données supprimables ou toujours supprimables de l'utilisateur; ces données ne seront pas supprimables et ne feront pas l'objet d'un accord de confidentialité (autrement dit, les données seront également accessibles aux nouveaux utilisateurs ultérieurs). Ces données peuvent comprendre les données qui doivent être accessibles à l'utilisateur ultérieur en vertu de la loi ou dans la pratique (par exemple, en ce qui concerne les mises à jour effectuées dans un véhicule connecté).

F. **Moyen de transfert/d'accès**

L'appendice devrait indiquer ici par quel moyen électronique sécurisé et pratique les données peuvent être mises à la disposition de l'utilisateur par le détenteur de données, soit par transfert, soit par accès.

G. **Informations nécessaires à l'exercice des droits d'accès de l'utilisateur**

L'appendice peut préciser ici les informations nécessaires à l'exercice des droits d'accès de l'utilisateur. Il peut s'agir d'une personne de contact chargée de résoudre les problèmes techniques, tant du côté du détenteur de données que du côté de l'utilisateur.

Appendice 2

Contenu d'une demande d'accès de l'utilisateur

Le présent formulaire concerne une demande particulière. Il est possible de faire plusieurs demandes et cela est même recommandé, par exemple pour segmenter certains flux de données afin qu'ils puissent être gérés de flux de données en flux de données et de finalité en finalité, de cycle de vie des données en cycle de vie des données (comme, par exemple, les flux de données à caractère personnel, etc.).

Bien que ce formulaire énumère les éléments clés d'une demande, il peut être adapté, en particulier aux différentes procédures électroniques.

Identification de l'utilisateur	Nom: veuillez préciser Numéro de contrat: *veuillez préciser*
Identification de la personne qui introduit la demande pour le compte de l'utilisateur (le cas échéant)	Nom: veuillez préciser Lien avec l'utilisateur: *veuillez préciser* Veuillez joindre la preuve du pouvoir d'agir pour le compte de l'utilisateur
Produits et/ou services concernés par la demande	Produit/service n° 1: veuillez préciser (numéro de série, par exemple) Produit/service n° 2: veuillez préciser (numéro de série, par exemple)
Points de données concernés par la demande	☐ Toutes les données qui sont facilement accessibles au détenteur de données ☐ Autre: veuillez préciser les points de données couverts par la demande
Nature des données demandées	☐ Y compris les données à caractère personnel Si l'utilisateur n'est pas la personne concernée, préciser le fondement juridique valable pour le traitement au titre de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, la manière dont les conditions de l'article 9 dudit règlement et de l'article 5, paragraphe 3, de la directive 2002/58/CE sont remplies. ☐ Uniquement les données à caractère non personnel
Date des données concernées par la demande	☐ Données passées: veuillez préciser la période ☐ Données futures: veuillez préciser la période
Calendrier de l'accès aux données (en fonction de ce qui est spécifié à l'appendice 1)	☐ En continu ☐ En temps réel ☐ Autre: veuillez préciser
Modalités d'accès aux données (en fonction de ce qui est spécifié à l'appendice 1)	☐ Transfert des données ☐ Accès aux données à l'endroit où elles sont stockées
Destination du transfert:	veuillez préciser en fonction de la réponse au point précédent
Date de la demande:	veuillez préciser

Appendice 3

Formulaire de demande d'accès de l'utilisateur pour mettre des données à la disposition d'un tiers

Le présent formulaire concerne une demande particulière. Il est possible de faire plusieurs demandes et cela est même recommandé, par exemple pour segmenter certains flux de données afin qu'ils puissent être gérés par un destinataire de données donné, désigné par l'utilisateur, de flux de données en flux de données et de finalité en finalité.

Identification de l'utilisateur	Nom: veuillez préciser Numéro de contrat: *veuillez préciser*
Identification de la personne qui introduit la demande pour le compte de l'utilisateur (le cas échéant)	Nom: veuillez préciser Lien avec l'utilisateur: *veuillez préciser*
Produits et/ou services concernés par la demande	Produit/service n° 1: *veuillez préciser* Produit/service n° 2: *veuillez préciser*
Données concernées par la demande N.B.: ne s'applique pas dans le cadre de l'expérimentation de nouveaux produits, substances ou processus connectés qui ne sont pas encore mis sur le marché.	☐ Option n° 1: toutes les données qui sont facilement accessibles au détenteur de données ☐ Option n° 2: veuillez préciser, conformément à l'appendice 1 du contrat entre l'utilisateur et le destinataire de données, les données à partager avec le destinataire de données ☐ Option n° 3: tel que spécifié par le destinataire de données à l'appendice 2 du contrat conclu entre le détenteur de données et le destinataire de données
Si les données comprennent des données à caractère personnel:	veuillez préciser le fondement juridique valable pour le traitement au titre de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, la manière dont les conditions de l'article 9 dudit règlement et de l'article 5, paragraphe 3, de la directive 2002/58/CE sont remplies.
Identification du tiers N.B.: ne peut pas être un contrôleur d'accès visé à l'article 3 du règlement (UE) 2022/1925	Nom: veuillez préciser Coordonnées: *veuillez préciser*

Appendice 4

Présentation détaillée des mesures de protection des secrets d'affaires

(à rédiger par les parties)

[OPTION] Appendice 5

Précisions sur le partage de données avec des tiers

(à rédiger par les parties)

Appendice 6

Présentation détaillée des mesures de protection

(à rédiger par les parties)

[OPTION] Appendice 7

Précisions sur la compensation de l'utilisateur

(à rédiger par les parties)

[OPTION] Appendice 8

Précisions sur les sanctions

(à rédiger par les parties)

[OPTION] Appendice 9

Documentation relative à la propriété du produit ou aux droits contractuels d'utilisation du produit ou des services connexes

(Documentation à joindre par les parties)

[OPTION] Appendice 10

Précisions sur les modalités d'accès aux données par les utilisateurs supplémentaires

(à rédiger par les parties)

ANNEXE III

CLAUSES CONTRACTUELLES TYPES

pour les contrats entre utilisateurs et destinataires de données

Les présentes clauses contractuelles types ont été conçues pour les contrats conclus entre un utilisateur d'un produit connecté et/ou d'un service connexe et un destinataire de données avec lequel l'utilisateur doit ou souhaite partager ses données en vertu de l'article 5 du règlement (UE) 2023/2854 (ci-après le «règlement sur les données»).

La principale nouveauté du règlement sur les données à cet égard est la suivante:

— l'utilisateur peut obliger le détenteur de données à partager des données avec un destinataire de données de son choix;

— l'utilisateur détermine dans un contrat avec le destinataire de données pour quelles finalités et dans quelles conditions il peut utiliser et partager des données;

— les clauses contractuelles abusives concernant l'accès aux données et l'utilisation des données, ou la responsabilité et les voies de recours en cas de violation ou d'extinction d'obligations liées aux données, ne sont pas contraignantes si elles ont été imposées unilatéralement à une entreprise par une autre entreprise.

Le présent contrat suivrait souvent le contrat conclu entre le détenteur de données et l'utilisateur, et précéderait le contrat qui doit également être conclu entre le détenteur de données et le destinataire de données.

Le présent contrat a une structure modulaire et, bien qu'il puisse exister en tant que contrat autonome en utilisant toutes les clauses (lorsque le partage de données est l'objet principal du contrat), les parties peuvent également sélectionner certaines clauses qui correspondent à leur situation particulière. Si le partage de données n'était qu'une condition préalable à l'exécution d'un contrat conclu à une autre fin, par exemple un contrat de réparation et d'entretien d'une machine industrielle, il pourrait suffire d'utiliser les clauses 1.2, 1.3, 2, 3 et 4 [à l'exception de la clause 4.1.1, point b)], étant donné que le contenu des autres clauses du présent contrat serait probablement couvert par le contrat de réparation et d'entretien.

1. Parties et produit / services connexes

1.1. Parties au contrat

Le présent contrat relatif à l'accès aux données et à leur utilisation est conclu entre

(insérer le nom, les coordonnées et d'autres références) (ci-après l'«utilisateur»)

et

(insérer le nom, les coordonnées et d'autres références) (ci-après le «destinataire de données»)

dénommés collectivement dans le présent contrat «les parties» et individuellement «la partie».

L'«**utilisateur**» est une personne physique ou morale à laquelle appartient un produit connecté ou à laquelle des droits temporaires d'utilisation de ce produit connecté ont été cédés contractuellement, ou qui reçoit des services connexes.

Le «**destinataire de données**» est un tiers du choix de l'utilisateur. Il peut s'agir d'une personne physique ou morale, autre que l'utilisateur d'un produit connecté ou d'un service connexe, agissant à des fins qui sont liées à son activité commerciale, industrielle, artisanale ou libérale, à la disposition duquel le détenteur de données met des données, y compris un tiers lorsque l'utilisateur a adressé une demande au détenteur de données ou conformément à une obligation légale découlant du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union.

Le destinataire de données peut être en concurrence avec le détenteur de données concerné. Toutefois, un contrôleur d'accès ne peut pas devenir ou être un destinataire de données.

1.2. Éligibilité du destinataire de données

Le destinataire de données déclare qu'il n'est pas désigné comme contrôleur d'accès conformément à l'article 3 du règlement (UE) 2022/1925 ([1]) (ci-après le «règlement sur les marchés numériques»).

([1]) Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

1.3. **Demande adressée au détenteur de données et coopération des parties**

1.3.1. Les parties conviennent ce qui suit:

[OPTION 1] [l'utilisateur demandera à

(*insérer le nom, les coordonnées et d'autres références)* (ci-après le «détenteur de données»)

de mettre les données spécifiées dans la clause 2 à la disposition du destinataire de données.]

[OPTION 2] [l'utilisateur charge le destinataire de données de demander à

(insérer le nom, les coordonnées et d'autres références) (ci-après le «détenteur de données»)

pour le compte de l'utilisateur, de mettre les données spécifiées dans la clause 2 à la disposition du destinataire de données.]

1.3.2. L'utilisateur et le destinataire de données coopéreront de bonne foi afin d'assurer un contact et un dialogue adéquats avec le détenteur de données. En particulier, le destinataire de données conclura un accord contractuel distinct avec le détenteur de données (ci-après le «contrat H2R»), [OPTION: en étroite consultation avec l'utilisateur] et conformément au droit applicable, y compris, mais sans s'y limiter, le règlement sur les données. Le destinataire de données doit veiller à ce que le contrat H2R soit conforme au présent contrat.

1.3.3. Le présent contrat porte sur:

(a) le ou les produits connectés suivants (ci-après le «produit»): (*insérer le nom et d'autres spécifications du produit connecté spécifique couvert par le présent contrat*);

(b) le ou les services connexes suivants (ci-après le ou les «services connexes»): (*insérer le nom et d'autres spécifications des services connexes spécifiques ou du type de services connexes couverts par le présent contrat, le cas échéant*).

L'utilisateur déclare qu'il est soit propriétaire du produit, soit contractuellement autorisé à utiliser le produit dans le cadre d'un contrat de location ou de crédit-bail ou d'un contrat similaire et/ou à recevoir le ou les services connexes dans le cadre d'un contrat de services.

[OPTION 1] [[L'utilisateur s'engage à fournir au destinataire de données, sur demande dûment justifiée, toute documentation pertinente à l'appui de cette déclaration, si nécessaire.]

[OPTION 2] [La documentation à l'appui de cette déclaration ainsi que des précisions sur les personnes qui doivent être considérées comme l'utilisateur au titre du présent contrat figurent à l'**appendice 5.]**

2. **Données couvertes par le contrat**

Les données couvertes par le présent contrat comprennent toutes les données relatives à un produit ou les données relatives à un ou des services connexes facilement accessibles générées par l'utilisation du produit ou par les services connexes:

[OPTION 1] [au sens du règlement sur les données.]

[OPTION 2] [au sens du règlement sur les données, telles qu'énumérées à l'appendice 1.]

[OPTION 3] [au sens du règlement sur les données, dans la mesure nécessaire pour les finalités convenues en vertu de la clause 3 et énumérées plus en détail par le destinataire de données à l'appendice 2 du contrat H2R.]

L'utilisateur n'est pas responsable de la qualité, des caractéristiques et de la quantité des données, ni de leur adéquation à un objet particulier.

Conformément au règlement sur les données, on entend par «**données relatives au produit**» les données générées par l'utilisation d'un produit connecté que le fabricant a conçu pour qu'elles puissent être extraites, au moyen d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré, par un utilisateur, un détenteur de données ou un tiers, y compris, le cas échéant, le fabricant.

On entend par «**données relatives aux services connexes**» les données représentant la numérisation des actions de l'utilisateur ou des événements liés au produit connecté, enregistrées intentionnellement par l'utilisateur ou générées en tant que produit annexe de l'action de l'utilisateur lors de la fourniture d'un service connexe par le fournisseur.

Les données relatives au produit et aux services connexes peuvent être à la fois des données à caractère personnel et des données à caractère non personnel.

Les **données facilement accessibles** correspondent aux données relatives à un produit et aux données relatives à un service connexe qu'un détenteur de données obtient légalement ou peut obtenir légalement à partir du produit connecté ou du service connexe, sans effort disproportionné allant au-delà d'une simple opération.

Comme expliqué dans les considérants, cette définition exclut les «données générées par l'utilisation d'un produit connecté lorsque la conception du produit connecté ne prévoit pas que ces données sont stockées ou transmises en dehors du composant dans lequel elles sont générées ou du produit connecté dans son ensemble» (considérant 20). «Les choix de conception des fabricants et, le cas échéant, les dispositions du droit de l'Union ou du droit national qui répondent aux besoins et aux objectifs propres à un secteur ou les décisions pertinentes des autorités compétentes devraient déterminer les données qu'un produit connecté peut mettre à disposition» (considérant 14).

3. Utilisation des données par le destinataire de données

Les accords de partage de données entre les utilisateurs et les destinataires de données pourraient, par exemple, constituer une nouvelle relation ou un complément à une relation existante entre les parties, qu'il s'agisse d'un partage de données à des fins commerciales ou non. Ces accords devraient être non exclusifs, sauf dans les cas bien délimités, spécifiques aux données, spécifiques au marché, spécifiques à la finalité, limités dans le temps et bien rémunérés.

3.1. Utilisation convenue des données

Il appartient à l'utilisateur d'examiner quelle partie de ses données et à quelles fins il autoriserait le destinataire de données à utiliser les données, et en particulier dans quelle mesure celui-ci devrait être autorisé à partager les données avec d'autres tiers.

Par exemple, l'utilisateur peut demander au destinataire de données de surveiller le fonctionnement du produit ou du service connexe et d'agir en tant qu'intermédiaire pour notifier les demandes de garantie au vendeur de l'équipement pour le compte de l'utilisateur.

L'utilisateur devrait également examiner s'il convient d'autoriser le destinataire à partager les données avec des entités commerciales ou non commerciales. Le partage de données à des fins non commerciales peut inclure le partage et l'utilisation altruistes ou sans but lucratif dans l'intérêt public, à des fins scientifiques, statistiques ou à d'autres fins de recherche analytique [lorsque cela est applicable et requis, ou lorsque cela n'est pas applicable ou requis, mais envisagé conformément à l'article 89 du RGPD, à la directive (UE) 2019/1024 sur les données ouvertes, au règlement (UE) 2023/138 sur les ensembles de données de forte valeur, au règlement (UE) 2022/868 sur la gouvernance des données, au règlement (UE) 2025/327 sur les espaces des données de santé, etc.], par le destinataire de données ou par son intermédiaire avec les communautés, municipalités, régions, nations, ONG et autres organisations non commerciales concernées. En ce qui concerne le partage de données commerciales, il est recommandé de ne pas faire référence au terme «vente» ni de l'utiliser, car cela pourrait signifier pour certaines parties prenantes que la propriété/le contrôle des données concernées est transféré, ou que ces données sont transmises d'une autre manière exclusivement au destinataire de données. Cela n'est ni nécessaire ni recommandé, d'autant plus que les données sont à la fois un actif numérique et un moyen numérique, et qu'elles peuvent être utilisées pour de nombreuses finalités tout au long de leur cycle de vie — y compris à des fins commerciales multiples — tout en continuant à accorder au destinataire de données un avantage commercial ou une autre valeur ajoutée qui justifie également une rémunération équitable de l'utilisateur pour l'octroi d'une telle licence d'utilisation (ou de réutilisation) des données.

L'utilisateur devrait évaluer les conséquences de l'octroi au destinataire de données du droit d'utiliser et, le cas échéant, de partager les données, et également déterminer si ces droits devraient être accordés en échange d'une compensation.

3.1.1. Le destinataire de données ne peut utiliser les données que pour les finalités suivantes, qui ne peuvent être en contradiction avec les pratiques énumérées à la clause 3.2: (*insérer les finalités convenues*).

Exemples de finalités convenues par le destinataire de données:

— offrir à l'utilisateur des services réguliers de maintenance/d'après-vente du produit;

— mener des recherches dans des domaines spécifiques;

— mettre au point de nouveaux services ou améliorer, mettre à niveau ou soutenir de nouveaux produits ou services, y compris des solutions d'intelligence artificielle (IA);

— agréger les données avec d'autres données ou créer des données dérivées, à toutes fins licites, y compris dans le but de vendre ces données agrégées ou dérivées à des tiers ou de les mettre à leur disposition d'une autre manière.

3.1.2. Le destinataire de données doit effacer les données lorsque celles-ci ne sont plus nécessaires pour les finalités convenues.

3.2. **Utilisation non autorisée des données**

Le destinataire de données ne peut pas utiliser les données:

(a) pour toute autre finalité que celles convenues dans la clause 3.1;

(b) pour toute fin contraire au droit de l'Union ou au droit national applicable;

(c) pour le profilage de personnes physiques au sens de l'article 4, paragraphe 4, du RGPD, sauf s'il est nécessaire pour fournir le service demandé par l'utilisateur;

(d) pour mettre au point un produit en concurrence avec le produit;

(e) pour obtenir des informations sur la situation économique, les actifs et les méthodes de production de l'utilisateur, ou sur l'utilisation du produit ou du service connexe qu'en fait ce dernier d'une quelconque autre manière susceptible de porter atteinte à la position commerciale de l'utilisateur sur les marchés sur lesquels il exerce ses activités, sauf si l'utilisateur a autorisé une telle utilisation;

(f) d'une manière qui nuit à la sécurité du produit ou du service connexe;

(g) [OPTION] [autre: *(veuillez préciser, en particulier, les utilisations qui portent* gravement atteinte aux intérêts légitimes de l'utilisateur)].

3.3. **Utilisation des données à caractère personnel par le destinataire de données**

Le destinataire de données n'utilise ou ne traite d'une autre manière des données qui sont des données à caractère personnel que s'il existe une base juridique prévue à cet effet et uniquement dans les conditions prévues par le règlement (UE) 2016/679 (RGPD) et, le cas échéant, la directive 2002/58/CE (directive vie privée et communications électroniques).

Lorsqu'elles réglementent le traitement des données à caractère personnel conformément à la législation applicable en matière de protection des données [y compris, mais sans s'y limiter, le règlement (UE) 2016/679], les parties doivent examiner si l'utilisateur est la personne concernée par tout ou partie des données à caractère personnel contenues dans les données.

3.4. **Application de mesures de protection**

Le destinataire de données s'engage à appliquer les mesures de protection visant à prévenir la perte de données et l'accès non autorisé aux données [OPTION 1] [qui sont raisonnables compte tenu des circonstances, de l'état de la science et de la technologie, du préjudice potentiel subi par l'utilisateur et des coûts associés aux mesures de protection.] [OPTION 2] [qui sont exposées en détail à l'**appendice 2**.]

Les parties devraient examiner si elles souhaitent inclure dans un appendice distinct toutes les mesures permettant de protéger efficacement les intérêts importants de l'utilisateur. Les mesures peuvent être à la fois de nature technique (par exemple, cryptage, pare-feu, stockage fractionné) et organisationnelle (par exemple, participation d'un tiers de confiance). Étant donné que les mesures doivent être proportionnées, leur contenu variera considérablement en fonction de la nature des données et des intérêts en jeu.

4. **Partage de données avec des tiers et utilisation de services de traitement de données**

Conformément à l'article 6, paragraphe 2, point c), du règlement sur les données, le destinataire de données ne peut pas «mettre les données qu'il reçoit à la disposition d'un autre tiers, à moins que les données ne soient mises à disposition sur le fondement d'un contrat avec l'utilisateur, et à condition que l'autre tiers prenne toutes les mesures nécessaires convenues entre le détenteur de données et le tiers pour préserver la confidentialité des secrets d'affaires».

Par conséquent, si l'utilisateur choisit de donner ce droit au destinataire de données, cette clause devrait être insérée, éventuellement en échange d'une compensation.

4.1. **Conditions de partage des données**

4.1.1. Le destinataire de données peut partager des données qui ne sont pas des données à caractère personnel avec des tiers si:

(a) les données sont utilisées par le tiers exclusivement aux fins suivantes:

i) aider le destinataire de données à atteindre les objectifs convenus à la clause 3.1;

ii) atteindre, en collaboration avec le destinataire de données ou par l'intermédiaire d'entreprises ad hoc, les objectifs convenus à la clause 3.1; et

iii) [OPTION] [(*veuillez préciser les finalités particulières que les tiers peuvent poursuivre pour leurs propres besoins, indépendamment du destinataire de données, et si les données sont partagées à ces fins en échange d'une compensation ou gratuitement*); et]

(b) le tiers n'est pas désigné comme contrôleur d'accès conformément à l'article 3 du règlement (UE) 2022/1925 (règlement sur les marchés numériques); et

(c) le destinataire de données oblige contractuellement le tiers:

i) à ne pas utiliser les données à d'autres fins que celles convenues à la clause 4.1.1, point a);

ii) à ne pas obtenir des informations sur la situation économique, les actifs et les méthodes de production de l'utilisateur, ou sur l'utilisation du produit ou du service connexe qu'en fait ce dernier d'une quelconque autre manière susceptible de porter atteinte à la position commerciale de l'utilisateur sur les marchés sur lesquels il exerce ses activités;

iii) à ne pas utiliser les données d'une manière qui porte gravement atteinte aux intérêts légitimes de l'utilisateur, en particulier lorsque ces données contiennent des données commercialement sensibles ou sont protégées par des secrets d'affaires ou des droits de propriété intellectuelle;

iv) à appliquer les mesures de protection requises en vertu de la clause 3.4; et

v) à effacer les données lorsque celles-ci ne sont plus nécessaires aux fins convenues à la clause 4.1.1, point a);

vi) à ne pas partager ultérieurement ces données.

4.1.2. De plus amples informations, notamment l'identité des tiers, les restrictions à l'utilisation des données par des tiers, ainsi que d'autres conditions et mesures de protection, sont exposées en détail à l'**appendice 3**.

4.1.3. Nonobstant les clauses 4.1.1 et 4.1.2, le destinataire de données peut utiliser des services de traitement, par exemple des services d'informatique en nuage (y compris une infrastructure à la demande, une plateforme à la demande et un logiciel à la demande), des services d'hébergement ou des services similaires pour atteindre, pour son propre compte et sous sa propre responsabilité, les finalités convenues à la clause 3.2.1, point a). Les tiers peuvent également utiliser ces services pour atteindre les finalités convenues à la clause 4.1.1, point a), pour leur propre compte et sous leur propre responsabilité. Le destinataire de données ne partage avec des tiers ou ne traite d'une autre manière des données qui sont des données à caractère personnel que s'il existe une base juridique prévue à cet effet et dans les conditions autorisées par le règlement (UE) 2016/679 (RGPD) et, le cas échéant, la directive 2002/58/CE (directive vie privée et communications électroniques).

5. **Compensation**

Le destinataire de données s'engage à indemniser l'utilisateur comme indiqué en détail à l'**appendice 4**.

Les parties peuvent convenir d'une compensation pour l'utilisation et le partage des données par le destinataire de données, lorsqu'elles le jugent équitable et raisonnable. Elles peuvent, par exemple, envisager une telle compensation si le destinataire de données utilise celles-ci pour mettre au point de nouveaux produits ou services ou si le destinataire de données crée des données agrégées ou dérivées à des fins commerciales. À l'inverse, si, par exemple, les données sont utilisées exclusivement pour les besoins de tout accord conclu avec l'utilisateur, aucune compensation ne sera prévue.

De même, une compensation pourrait être nécessaire pour garantir le traitement équitable de l'utilisateur, si celui-ci accepte que le destinataire de données puisse vendre les données à des tiers conformément à la clause 4.1.1, point a) iii). Si une compensation est due, les parties doivent s'accorder sur sa nature, qui peut être monétaire ou non.

6. **Date d'application, durée du contrat et résiliation**

6.1. **Date d'application et durée**

6.1.1. Le présent contrat [OPTION 1] [prend effet immédiatement] [OPTION 2] [prend effet à compter du *(préciser la date)*].

6.1.2. [OPTION] [Le présent contrat est conclu pour [OPTION 1] [une durée indéterminée] [OPTION 2] [une durée déterminée de (préciser)], sous réserve de tout motif d'expiration ou de résiliation en vertu du présent contrat.]

6.2. **Résiliation**

6.2.1. Le bénéficiaire des données peut résilier le présent contrat en donnant un préavis à l'utilisateur de (*préciser le délai de préavis*) si le contrat H2R a été résilié.

6.2.2. Si l'utilisateur perd son statut d'utilisateur, le présent contrat prend fin. L'utilisateur donnera un préavis au destinataire de données de (*préciser le délai de préavis*).

6.2.3. [OPTION en cas de durée indéterminée ou si les parties souhaitent autoriser la résiliation pour convenance] [Chaque partie peut résilier le présent contrat à tout moment avant le début ou pendant la durée du contrat en donnant un préavis (*préciser le délai*) à l'autre partie.] [OPTION] Si l'utilisateur résilie le présent contrat en vertu de la présente clause avant (*indiquer la date ou la durée minimale du contrat*), l'utilisateur indemnise l'autre partie pour les coûts supportés dans le cadre de la mise en œuvre du présent contrat, comme suit: *(biffer les mentions inutiles).*

Dans les cas où l'utilisateur est contractuellement tenu de partager des données avec le destinataire de données, la présente clause ne devrait pas être incluse car elle pourrait entraîner la rupture d'un autre contrat.

6.3. **Effets de l'expiration ou de la résiliation**

6.3.1. L'expiration de la période contractuelle ou la résiliation du présent contrat libère les deux parties de leur obligation d'exécuter et de recevoir une exécution dans l'avenir, mais n'affecte pas les droits et obligations acquis jusqu'au moment de l'expiration ou de la résiliation.

L'expiration ou la résiliation n'affecte pas les dispositions qui restent applicables même après la fin du contrat, en particulier les éventuelles limitations de l'utilisation et du partage autorisés des données par le destinataire de données en vertu des clauses 3 et 4, de la clause 8.1 relative à la confidentialité, de la clause 8.3 relative au droit applicable et de la clause 8.6 relative au règlement des litiges.

6.3.2. En particulier, la résiliation ou l'expiration du contrat aura les effets suivants:

(a) le destinataire de données cesse immédiatement d'extraire les données générées ou enregistrées à la date de résiliation ou d'expiration;

(b) [OPTION] le destinataire de données conserve le droit d'utiliser et de partager les données générées ou enregistrées avant la date de résiliation ou d'expiration, comme indiqué aux clauses 3 et 4 [OPTION pour une période de *(préciser la durée)*].

Il peut arriver que le destinataire de données doive investir dans le partage de données, par exemple en adaptant son infrastructure numérique; l'investissement sera amorti au fil du temps. Dans ce cas, les parties peuvent souhaiter s'assurer que le destinataire de données reçoit une compensation de la partie résiliant le contrat. Le montant de la compensation devrait être déterminable.

7. Voies de recours en cas d'inexécution

7.1. Cas d'inexécution

7.1.1. L'inexécution d'une obligation par une partie est essentielle si:

(a) elle prive substantiellement l'autre partie de ce qu'elle était en droit d'attendre du présent contrat, à moins que la partie défaillante n'ait pas prévu et n'ait pas pu raisonnablement prévoir ce résultat; ou

(b) il ressort clairement des circonstances que l'on ne peut pas compter dans l'avenir sur une exécution par la partie défaillante.

7.1.2. Une partie est exonérée des conséquences de l'inexécution lorsque celle-ci est due à un empêchement qui lui échappe et si l'on ne pouvait raisonnablement attendre de cette partie qu'elle le prenne en considération au moment de la conclusion du présent contrat, ou qu'elle le prévienne ou le surmonte ou qu'elle en prévienne ou en surmonte les conséquences.

7.1.3. Lorsque l'empêchement exonératoire n'est que temporaire, l'exonération d'inexécution de la partie vaut pour la durée de l'empêchement. Cependant, si le retard équivaut à une inexécution essentielle, l'autre partie peut le traiter comme telle.

La partie défaillante doit faire en sorte que l'autre partie reçoive, sans retard excessif, notification de l'empêchement et de ses effets sur sa capacité de s'exécuter à partir du moment où la partie défaillante a eu, ou a pu avoir raisonnablement connaissance de ces circonstances. L'autre partie a droit à des dommages et intérêts en réparation du préjudice économique résultant de la non-réception de cette notification.

7.2. Voies de recours en cas d'inexécution

7.2.1. En cas d'inexécution par une partie, l'autre partie dispose des voies de recours énumérées dans les clauses suivantes, sans préjudice des voies de recours prévues par le droit applicable.

7.2.2. Les moyens d'action qui ne sont pas incompatibles peuvent être cumulés.

7.2.3. Une partie ne peut recourir à aucun moyen d'action dans la mesure où elle a provoqué l'inexécution de l'autre partie, par exemple lorsqu'une défaillance dans sa propre infrastructure de données n'a pas permis à l'autre partie de s'acquitter dûment de ses obligations. Une partie ne peut pas non plus introduire une demande de dommages et intérêts dans la mesure où elle aurait pu réduire son préjudice en prenant des mesures raisonnables.

7.2.4. La partie lésée peut:

(a) résilier le présent contrat avec effet immédiat et sans pénalité, en adressant une notification à l'autre partie, si:

i) l'inexécution de l'autre partie est une inexécution essentielle; ou

ii) dans le cas d'une inexécution qui n'est pas essentielle, la partie lésée a, par notification, imparti un délai raisonnable pour remédier à l'inexécution et ce délai a expiré sans que l'autre partie ne se soit exécutée;

(b) demander des dommages et intérêts pour le préjudice économique qui lui a été causé par l'inexécution de l'autre partie et qui ne bénéficie pas d'une exonération en vertu de la clause 7.1.2; la partie défaillante n'est responsable que des dommages qu'elle avait prévus ou qu'elle aurait raisonnablement dû prévoir au moment de la conclusion du présent contrat comme pouvant résulter de son inexécution, sauf si celle-ci était intentionnelle ou résultait d'une négligence grave;

(c) demander à la partie défaillante de se conformer, sans retard injustifié, aux obligations qui lui incombent en vertu du présent contrat, à moins que cela ne soit illicite ou impossible ou qu'une exécution spécifique n'entraîne pour la partie défaillante des coûts disproportionnés par rapport au bénéfice que l'autre partie en retirerait; [OPTION] [lorsqu'une partie n'exécute pas les obligations qui lui incombent en vertu du présent contrat, elle s'acquitte, en tout état de cause, des pénalités exposées en détail à l'appendice 6, que les parties considèrent comme des dommages et intérêts au sens de la clause 7.2.4, point b); la partie défaillante a le droit de demander que la pénalité soit réduite à un montant raisonnable lorsqu'elle peut prouver que celle-ci est manifestement excessive par rapport au préjudice résultant de l'inexécution.]

8. Dispositions générales

8.1. Confidentialité

8.1.1. Les informations suivantes doivent être considérées comme confidentielles:

(a) les informations relatives aux secrets d'affaires, à la situation financière ou à tout autre aspect des activités d'une partie, sauf si l'autre partie a rendu ces informations publiques;

(b) (*le cas échéant*) les informations exposant la base de calcul de la compensation;

(c) les informations relatives au détenteur de données et à tout autre tiers protégé, sauf si le tiers protégé a rendu ces informations publiques.

8.1.2. Les deux parties conviennent de prendre toutes les mesures raisonnables pour conserver en toute sécurité et en toute confidentialité les informations visées à la clause 8.1.1 et de ne pas les divulguer ou les mettre à la disposition d'un tiers, sauf dans les cas suivants:

(a) si l'une des parties a l'obligation légale de divulguer ou de mettre à disposition les informations pertinentes; ou

(b) s'il est nécessaire que l'une des parties divulgue ou mette à disposition les informations pertinentes pour s'acquitter des obligations qui lui incombent en vertu du présent contrat; ou

(c) si l'une des parties a obtenu le consentement préalable de l'autre partie ou de la partie qui a fourni les informations confidentielles ou qui est concernée par leur divulgation.

8.1.3. Dans tous les cas, l'utilisateur et le destinataire de données peuvent divulguer ou mettre à la disposition du détenteur de données les informations nécessaires pour identifier ou contacter le destinataire de données ou l'utilisateur afin de conclure le contrat H2R visé à la clause 1.3.2.

8.1.4. Ces obligations de confidentialité restent applicables après la résiliation du contrat pendant une durée de (*préciser la durée*).

8.1.5. Ces obligations de confidentialité ne suppriment aucune des obligations plus strictes au titre i) du règlement (UE) 2016/679 (RGPD), ii) des dispositions mettant en œuvre la directive 2002/58/CE ou la directive (UE) 2016/943, ou iii) de toute autre disposition du droit de l'Union ou du droit d'un État membre.

8.2. Moyens de communication

Toute notification ou autre communication requise ou autorisée par le présent contrat doit être effectuée par écrit et peut être remise en main propre, envoyée par courrier prépayé ou transmise par voie électronique, y compris par courrier électronique, à condition que l'expéditeur conserve la preuve de l'envoi aux adresses énumérées ci-dessous:

Partie	Personne de contact	Adresse électronique	Numéro de téléphone	Adresse
Utilisateur	[Nom]/[Fonction]	[Adresse électronique]	[Numéro de téléphone]	[Adresse]
Destinataire de données	[Nom]/[Fonction]	[Adresse électronique]	[Numéro de téléphone]	[Adresse]

Toute notification ou communication de ce type est réputée reçue:

(a) en cas de remise en main propre, à la date de livraison;

(b) en cas d'envoi par courrier prépayé, le troisième jour ouvrable suivant l'envoi;

(c) en cas d'envoi par voie électronique, à la date de transmission, à condition qu'aucun message d'erreur indiquant un défaut de transmission n'ait été reçu par l'expéditeur.

8.3. **Contrat indivisible, modifications et caractère détachable**

8.3.1. Le présent contrat (ainsi que ses appendices et tout autre document visé dans le contrat) constitue le contrat indivisible conclu entre les parties concernant l'objet du présent contrat et annule et remplace tous les accords ou contrats et protocoles antérieurs, oraux ou écrits, entre les parties concernant l'objet du présent contrat.

8.3.2. Toute modification du présent contrat ne sera valable que si les parties en conviennent par écrit, y compris sous une forme électronique.

8.3.3. Si une disposition du présent contrat est déclarée nulle, invalide, annulable ou inapplicable pour quelque raison que ce soit, et si cette disposition est détachable des autres clauses du contrat, ces autres dispositions n'en seront pas affectées et resteront valables et applicables, sauf si la disposition n'est pas détachable des autres dispositions du présent contrat. Toute lacune ou ambiguïté qui en résulterait dans le présent contrat sera traitée conformément à la clause 8.4.

8.4. **Droit applicable**

Le présent contrat est régi par le droit de (*préciser l'État membre*).

8.5. **Interprétation**

8.5.1. Le présent contrat est conclu par les parties dans le cadre de leurs droits et obligations au titre du règlement sur les données. Les dispositions du présent contrat doivent être interprétées dans le sens de leur conformité avec le règlement sur les données et d'autres dispositions du droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union, ainsi qu'avec toute disposition du droit national applicable qui est compatible avec le droit de l'Union et auquel il ne peut être dérogé par accord.

8.5.2. Si une lacune ou une ambiguïté dans le présent contrat ne peut être résolue de la manière visée à la clause 8.5.1, le présent contrat doit être interprété à la lumière des règles d'interprétation prévues par le droit applicable (voir clause 8.4).

8.6. **Règlement des litiges**

8.6.1. Les parties conviennent de tout mettre en œuvre pour régler les litiges à l'amiable et, avant de porter une affaire devant une juridiction, de soumettre leur litige à (*insérer le nom et les coordonnées d'un organisme particulier de règlement des litiges; pour les litiges relevant de leur compétence telle que définie à l'article 10, paragraphe 1, du règlement sur les données, il peut s'agir de tout organisme de règlement des litiges d'un État membre qui remplit les conditions énoncées à l'article 10 du règlement sur les données*).

8.6.1. [OPTION, si l'utilisateur est une entreprise] [Les tribunaux de (*préciser l'État membre*) seront seuls compétents pour connaître de l'affaire concernant le présent contrat.]

L'**appendice 1** contient une description des données

[À rédiger par les parties]

L'**appendice 2** énumère les mesures de protection à prendre par le destinataire de données

[À rédiger par les parties]

L'**appendice 3** contient des informations sur le partage des données avec des tiers par le destinataire de données

[À rédiger par les parties]

L'**appendice 4** contient des informations sur la compensation accordée à l'utilisateur pour l'utilisation et le partage des données par le destinataire de données

[À rédiger par les parties]

L'**appendice 5** contient la documentation relative à la propriété du produit ou aux droits contractuels d'utilisation du produit ou des services connexes

[À rédiger par les parties]

[OPTION] L'appendice 6 contient des précisions sur les sanctions

[À rédiger par les parties]

ANNEXE IV

CLAUSES CONTRACTUELLES TYPES

pour les contrats conclus entre les détenteurs de données et les destinataires de données concernant la mise à disposition de données à la demande des utilisateurs de produits connectés et de services connexes

Les présentes clauses contractuelles types ont été conçues pour les contrats conclus entre un détenteur de données et un destinataire de données qui est une entreprise, lorsqu'un détenteur de données est tenu [en vertu de l'article 5 du règlement (UE) 2023/2854 — ci-après le «règlement sur les données»] de mettre les données provenant d'un produit connecté et/ou d'un service connexe à la disposition d'un destinataire de données à la demande de l'utilisateur.

La principale nouveauté du règlement sur les données à cet égard est la suivante:

— le détenteur de données est tenu de partager des données avec le destinataire de données dès réception d'une demande de l'utilisateur à cet effet (avec des mesures de protection des données protégées en tant que secrets d'affaires);

— le détenteur de données peut demander une compensation raisonnable au destinataire de données;

— les clauses contractuelles abusives concernant l'accès aux données et l'utilisation des données, ou la responsabilité et les voies de recours en cas de violation ou d'extinction d'obligations liées aux données, ne sont pas contraignantes si elles ont été imposées unilatéralement à une entreprise par une autre entreprise.

Le présent contrat a une structure modulaire et, s'il peut être utilisé comme contrat complet, les parties peuvent également sélectionner certaines clauses qui correspondent à leur situation particulière. Plusieurs clauses contiennent des options, et, les parties doivent ici réfléchir à leurs besoins, relations commerciales et intérêts spécifiques afin de déterminer l'option la mieux adaptée à leur contrat.

Certaines clauses sont également marquées (*le cas échéant*) et devraient être incluses si certaines conditions sont remplies.

Bien que les clauses contractuelles types soient recommandées par la Commission, elles ne sont pas contraignantes et peuvent toujours faire l'objet d'une dérogation de la part des parties.
Les présentes clauses contractuelles types peuvent également être utilisées avec des modifications appropriées lorsqu'un détenteur de données est tenu de mettre des données à la disposition d'un destinataire de données en vertu d'autres dispositions du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union.

1. Parties, utilisateur demandeur et produit/service(s) connexe(s)

1.1. Parties au contrat

Le présent contrat relatif à l'accès aux données et à leur utilisation est conclu

entre

(*insérer le nom, les coordonnées et d'autres références*) (ci-après le «détenteur de données»)

et

(*insérer le nom, les coordonnées et d'autres références*) (ci-après le «destinataire de données»)

dénommés collectivement dans le présent contrat «les parties» et individuellement «la partie».

Les parties doivent indiquer ici qui est le détenteur de données et qui est le destinataire de données, au sens de l'article 2, points 13) et 14), du règlement sur les données.

Conformément au règlement sur les données, on entend par «détenteur de données» «une personne physique ou morale qui, conformément au règlement sur les données, aux dispositions applicables du droit de l'Union ou à la législation nationale adoptée conformément au droit de l'Union, a le droit ou l'obligation d'utiliser et de mettre à disposition des données, y compris, lorsqu'il en a été convenu par contrat, des données relatives au produit ou des données relatives au service connexe qu'elle a extraites ou générées au cours de la fourniture d'un service connexe».

Conformément au règlement sur les données, on entend par «destinataire de données» une personne physique ou morale, autre que l'utilisateur d'un produit connecté ou d'un service connexe, agissant à des fins qui sont liées à son activité commerciale, industrielle, artisanale ou libérale, à la disposition duquel le détenteur de données met des données, y compris un tiers lorsque l'utilisateur a adressé une demande au détenteur de données ou conformément à une obligation légale découlant du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union. Conformément à l'article 1er, paragraphe 3, point d), du règlement sur les données, les détenteurs de données sont uniquement tenus de mettre des données à la disposition des «destinataires de données dans l'Union». Ils ne sont pas tenus de le faire pour les destinataires de données dont le lieu d'établissement se situe en dehors de l'Union.

1.2. **Utilisateur demandeur, produit/service(s) connexe(s)**

1.2.1. Le présent contrat repose sur l'hypothèse commune des parties selon laquelle le détenteur de données est tenu, en vertu de l'article 5 du règlement sur les données, de mettre des données à la disposition du destinataire de données lorsque ce dernier ou une partie agissant pour le compte de

(*insérer le nom, les coordonnées et d'autres références*) (ci-après l'«utilisateur demandeur») en fait la demande

et que l'utilisateur demandeur est un utilisateur [au sens de l'article 2, point 12), du règlement sur les données]:

du produit suivant: (*insérer le nom et d'autres spécifications du produit connecté spécifique ou du type de produits couverts par le présent contrat*); et/ou

du ou des services connexes suivants: (*insérer le nom et d'autres spécifications du ou des services connexes spécifiques ou du type de services connexes couverts par le présent contrat, le cas échéant*).

Les parties doivent indiquer ici qui est l'utilisateur au sens de l'article 2, point 12), du règlement sur les données, qui présente une demande au détenteur de données, conformément à l'article 5 du règlement sur les données.

Un **utilisateur** est une personne physique ou morale à laquelle appartient un produit connecté ou à laquelle des droits temporaires d'utilisation de ce produit connecté ont été cédés contractuellement, ou qui reçoit des services connexes.

Les parties doivent également indiquer quel produit connecté et, le cas échéant, quel service connexe est utilisé par l'utilisateur demandeur.

Conformément au règlement sur les données, on entend par «**produit connecté**» un article:
i) qui obtient, génère ou recueille des données concernant son utilisation ou son environnement;
ii) qui est en mesure de communiquer des données relatives au produit par l'intermédiaire d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré;
iii) dont la fonction première n'est pas de stocker, de traiter ou de transmettre des données pour le compte de toute partie autre que l'utilisateur.

On entend par «**service connexe**» un service numérique (autre qu'un service de communications électroniques, y compris un logiciel):
i) qui est connecté au produit au moment de l'achat, ou de la mise en location ou en crédit-bail, de telle sorte que son absence empêcherait le produit connecté d'exécuter une ou plusieurs de ses fonctions; ou
ii) qui est ensuite connecté au produit par le fabricant ou un tiers pour ajouter, mettre à jour ou adapter les fonctions du produit connecté.

2. **Base du contrat**

2.1. **Qualité de l'utilisateur demandeur et existence d'une demande valable**

2.1.1. Chaque partie déclare que, à sa connaissance, l'utilisateur demandeur est un utilisateur [au sens de l'article 2, point 12), du règlement sur les données] du produit et du ou des services connexes visés à la clause 1.2.1.

2.1.2. Chaque partie déclare que l'utilisateur demandeur a demandé au détenteur de données de mettre à la disposition du destinataire de données les données visées à la clause 3.1. La preuve de cette demande est jointe au présent contrat en **appendice 1**.

2.1.3. (*Le cas échéant*) Chaque Partie déclare qu'à sa connaissance, la partie agissant pour le compte de l'utilisateur demandeur a reçu l'autorisation nécessaire de sa part pour soumettre cette demande conformément au droit applicable. La preuve de l'autorisation est jointe au présent contrat en **appendice 1**.

En vertu du règlement sur les données, la demande peut être présentée par un tiers agissant pour le compte de l'utilisateur demandeur. Ce tiers peut, par exemple, être un courtier de données ou tout autre agent ou représentant, y compris le destinataire de données lui-même.

De toute évidence, si un tiers, y compris le destinataire de données, prétend avoir été autorisé par l'utilisateur demandeur, cette situation est une source potentielle d'abus par rapport à la situation habituelle de la demande. Par conséquent, les parties doivent prendre des mesures raisonnables pour vérifier qu'il n'y a pas eu de fraude ou de manipulation et que cette demande a été correctement présentée.

2.1.4. Chaque partie déclare qu'à sa connaissance, la demande est valable en vertu du droit applicable, n'a pas été retirée et n'a pas expiré.

S'il existe des éléments indiquant que la demande n'est pas valable ou a été retirée, les parties doivent prendre des mesures raisonnables pour vérifier qu'il existe toujours une demande valable. Si tel n'est pas le cas, le détenteur de données peut ne pas être autorisé à partager les données avec le destinataire de données et peut être tenu responsable d'un tel partage. Le destinataire de données peut également être responsable s'il demande des données qu'il n'est pas en droit de demander.

La validité de la demande peut dépendre de nombreux facteurs en vertu du droit applicable. Par exemple, pour qu'une demande soit juridiquement valable, il peut être nécessaire:

— qu'elle soit considérée comme une indication libre, suffisamment éclairée et explicite des souhaits de l'utilisateur demandeur;

— qu'elle soit présentée avec la capacité juridique nécessaire.

2.2. **Éligibilité du destinataire de données**

2.2.1. Le destinataire de données déclare qu'un contrat est en vigueur entre lui et l'utilisateur demandeur lui permettant d'utiliser les données et que, conformément au présent contrat, les données seront utilisées exclusivement pour (*indiquer la ou les finalités conformément au contrat conclu entre le destinataire de données et l'utilisateur demandeur*):

(*si les données peuvent divulguer des secrets d'affaires*) Le destinataire de données déclare que les données sont strictement nécessaires à cette fin.

Conformément à l'article 6, paragraphe 1, du règlement sur les données, le destinataire de données ne peut utiliser les données que sur la base d'un contrat conclu avec l'utilisateur et pour les finalités convenues avec celui-ci. Il convient que le destinataire de données fasse dans la présente clause des déclarations confirmant que tel est le cas. Si ces déclarations ne sont pas ou plus correctes, le détenteur de données peut avoir la possibilité de résilier le contrat conformément à la clause 2.4.3.

Les parties devraient s'efforcer de définir les finalités convenues de sorte qu'elles permettent au détenteur de données de déterminer si l'utilisation des données par le destinataire de données est autorisée, mais sans être suffisamment détaillées pour divulguer au détenteur de données des idées commerciales confidentielles appartenant au destinataire de données.

Lorsque les secrets d'affaires du détenteur de données sont en jeu, l'ensemble des finalités doit être divulgué afin de permettre au détenteur de données d'évaluer si la fourniture des données est strictement nécessaire pour atteindre la finalité déclarée.

2.2.2. Le destinataire de données déclare qu'il n'est pas désigné comme contrôleur d'accès, conformément à l'article 3 du règlement (UE) 2022/1925 (règlement sur les marchés numériques).

2.3. **Respect de la législation en matière de protection des données**

2.3.1. Dans la mesure où les données sont considérées comme des données à caractère personnel, chaque partie déclare se conformer au règlement (UE) 2016/679 et, le cas échéant, à la directive 2002/58/CE.

2.3.2. En particulier, lorsque l'utilisateur demandeur n'est pas la personne concernée, le détenteur de données ne peut mettre les données qui sont des données à caractère personnel à la disposition du destinataire de données que dans la mesure autorisée par le règlement (UE) 2016/679 et, le cas échéant, par la directive 2002/58/CE.

La notion de «données à caractère personnel» au sens du RGPD est très large. Elle couvre toute donnée se rapportant à une personne physique identifiée ou identifiable, c'est-à-dire une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Les données à caractère non personnel peuvent devenir des données à caractère personnel, par exemple lorsqu'elles font partie d'un ensemble de données mixte ou lorsqu'elles sont combinées à de nouvelles données et que le résultat de cette combinaison permet de relier les données à une personne identifiée ou identifiable. Cela peut également se produire lorsque de nouvelles capacités de traitement des données sont créées.

Les parties devraient commencer par examiner rigoureusement la présence de données à caractère personnel dans les données ainsi que leurs propres rôles, et celui de l'utilisateur, en vertu des définitions suivantes du RGPD:

— «personne concernée», la personne physique identifiée ou identifiable à laquelle les informations se rapportent;

— «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit, le responsable du traitement peut être désigné par ledit droit;

— «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

— «destinataire», la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers (à l'exclusion des autorités publiques, qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit applicable).

Les parties devraient tenir compte du fait qu'une partie peut jouer plusieurs rôles en fonction de la finalité du traitement et/ou qu'elle peut jouer un rôle conjointement avec une autre partie.

Une base juridique est nécessaire en vertu du RGPD pour permettre le partage des données avec le destinataire de données. Une base juridique possible pour le partage de données à caractère personnel lorsque l'utilisateur demandeur n'est pas la personne concernée pourrait être le consentement des personnes concernées au sens de l'article 6, paragraphe 1, point a), ou un intérêt légitime au sens de l'article 6, paragraphe 1, point f), du RGPD. Pour apprécier l'existence d'un tel intérêt légitime, l'obligation de mettre les données à disposition conformément à l'article 5 du règlement sur les données peut être prise en considération, bien que cette obligation ne constitue pas une base juridique suffisante en soi.

2.4. **Inexactitude des déclarations**

2.4.1. Toute partie qui s'aperçoit qu'une des déclarations visées aux clauses 2.1 à 2.3 n'est pas, ou n'est plus, exacte, ou ne le sera plus dans un avenir prévisible, doit en informer l'autre partie sans retard injustifié, sauf si l'autre partie le sait ou devrait déjà le savoir.

Si l'une des déclarations visées aux clauses 2.1 à 2.3 n'est pas ou plus exacte, la partie devrait prendre les mesures appropriées. En particulier, si l'utilisateur demandeur a vendu le produit et cesse d'être l'utilisateur et que le détenteur de données reçoit les informations appropriées, le détenteur de données doit résilier le contrat conclu avec le destinataire de données en ce qui concerne cet utilisateur. Il convient d'indiquer les motifs de résiliation dans l'avis de résiliation. Une simple notification ne serait pas suffisante en l'espèce, étant donné qu'il n'existe aucun moyen de remédier à la situation. Si le destinataire de données souhaite continuer à recevoir les données, il doit s'adresser au nouvel utilisateur. Toutefois, dans certains cas, les parties peuvent remédier à la violation de la représentation. Tel serait le cas, par exemple, lorsque la demande de l'utilisateur est émise par une personne non autorisée (par exemple, l'employé qui n'avait pas le pouvoir de représenter l'entreprise utilisatrice). Dans ce cas, le droit applicable peut permettre de valider cette action avec effet rétroactif.

2.4.2. Dès qu'elle a connaissance de cette situation, la partie concernée doit prendre les mesures appropriées et remédier, dans la mesure du possible, à l'inexactitude de la déclaration. Selon les circonstances, il peut s'agir d'informer l'utilisateur demandeur ou tout tiers protégé qui est concerné ou de suspendre temporairement la mise à disposition des données par le détenteur de données ou l'utilisation des données par le destinataire de données, si la mise à disposition des données ou l'utilisation des données est devenue illicite.

2.4.3. Si la situation n'est pas et ne peut pas être corrigée, le présent contrat doit prendre fin au moyen d'un avis de résiliation écrit mentionnant les motifs de résiliation donnés par l'une des parties à l'autre.

La résiliation a un effet immédiat. Lorsque l'inexactitude ne concerne qu'une partie des données couvertes par le présent contrat, la résiliation ne doit prendre effet que pour la partie concernée.

Les effets de la résiliation sont régis par la clause 7.3.

3. Mise à disposition des données

3.1. Données couvertes par le contrat

3.1.1. Les données couvertes par le présent contrat comprennent toutes les données relatives à un produit ou les données relatives à un ou des services connexes facilement accessibles au sens du règlement sur les données recensées dans la demande effectuée par l'utilisateur demandeur conformément à l'article 5 dudit règlement, et comprennent à la fois des données à caractère non personnel et des données à caractère personnel (ci-après les «données»).

Les données sont énumérées en détail à l'**appendice 2**.

Si, au cours du présent contrat, des données autres que celles spécifiées à l'**appendice 2** doivent être mises à la disposition du destinataire de données, l'**appendice 2** sera modifié en conséquence.

Les parties devraient, à l'appendice 2, préciser les données et métadonnées couvertes par le contrat, conformément à la demande formulée par l'utilisateur demandeur.

Conformément à l'article 2, points 15), 16) et 17) et à l'article 5 du règlement sur les données, ces données ne peuvent être que des données relatives au produit ou des données relatives au service connexe facilement accessibles:

— les données relatives au produit sont les données générées par l'utilisation du produit que le fabricant a conçu pour qu'elles puissent être extraites, au moyen d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré, par l'utilisateur, le détenteur de données ou un tiers, y compris, le cas échéant, le fabricant;

— les données relatives au service connexe sont les données représentant la numérisation des actions de l'utilisateur ou des événements liés au produit connecté, enregistrées intentionnellement par un utilisateur ou générées en tant que produit annexe de l'action d'un utilisateur lors de la fourniture d'un service connexe;

— les données facilement accessibles sont les données que le détenteur de données peut obtenir légalement à partir du produit ou du service connexe, sans effort disproportionné allant au-delà d'une simple opération.

Étant donné que le présent contrat fixe les modalités de mise à disposition des données au destinataire de données à la demande de l'utilisateur demandeur, ces données sont celles indiquées dans la demande.

La description des données doit être suffisante pour déterminer quelles données sont couvertes par un régime particulier, le cas échéant. En particulier, les parties devraient préciser quelles données peuvent être considérées comme des données à caractère personnel.

3.2. Caractéristiques des données et modalités d'accès

3.2.1. Le détenteur de données doit mettre les données à la disposition du destinataire de données, les données étant au moins de la même qualité que lorsqu'elles ont été mises à la disposition du détenteur de données et, en tout état de cause, dans un format complet, structuré, couramment utilisé et lisible par machine, de manière aisée et sécurisée, ainsi que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données.

On entend par «métadonnées» une description structurée du contenu ou de l'utilisation des données qui facilite la découverte ou l'utilisation de ces données. Conformément à l'article 5, paragraphe 1, du règlement sur les données, les métadonnées doivent être mises à disposition avec les données, dans la mesure où elles sont «*nécessaires à l'interprétation et à l'utilisation*» de ces données.

Bien que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données ne soient pas définies et doivent donc être déterminées au cas par cas, le règlement sur les données précise que «[l]*es données qui doivent être mises à disposition devraient inclure les métadonnées pertinentes, y compris leur contexte de base et leur horodatage, pour rendre les données utilisables, combinées à d'autres données, telles que les données triées et classifiées avec d'autres points de données les concernant, ou reformatées dans un format couramment utilisé*» (considérant 15 du règlement sur les données).

3.2.2. Le destinataire de données doit avoir accès aux données

a) de manière aisée et sécurisée;

b) sans retard injustifié;

(*le cas échéant*) c) en continu et en temps réel.

3.2.3. Afin de satisfaire aux exigences des clauses 3.2.1 et 3.2.2, les parties conviennent des spécifications énoncées à l'appendice 2.

Conformément à l'article 5, paragraphe 1, du règlement sur les données, les données doivent être mises à disposition sans retard injustifié et, lorsque cela est pertinent et techniquement réalisable, en continu et en temps réel.

Étant donné qu'il existe différents moyens de mettre en œuvre ces exigences légales, les parties devraient convenir de toutes les conditions dans lesquelles l'accès doit être fourni à l'**appendice 2**.

Ce faisant, elles devraient, dans un premier temps, décider si elles souhaitent:

— prévoir le **transfert complet** des données, c'est-à-dire qu'une copie des données est transférée sur un support placé sous le contrôle du destinataire de données:

  — par une transmission déclenchée par le détenteur de données («push»), telle qu'une transmission en ligne, un téléchargement dans l'espace en nuage du destinataire de données ou la livraison d'un support matériel sur lequel les données sont stockées; ou

  — par une récupération déclenchée par le destinataire de données («pull»), par exemple en lui fournissant une API, un accès à l'espace en nuage du détenteur de données ou à des outils similaires permettant au destinataire de données d'accéder aux données et de les extraire; ou

— **donner accès aux données là où elles sont stockées**, c'est-à-dire que les données sont consultées et traitées sur un support placé sous le contrôle du détenteur de données ou d'un tiers de confiance, par exemple en se connectant à un espace dédié sur les serveurs du détenteur de données ou du tiers de confiance, mais que les données ne sont pas transférées sur un support placé sous le contrôle du destinataire de données, sauf si des dispositions particulières sont prises.

Le transfert complet donne au destinataire de données une liberté maximale, mais réduit considérablement la capacité du détenteur de données à prévenir les abus.

L'accès à l'endroit où les données sont stockées augmente les risques de divulgation de leurs idées commerciales pour les destinataires de données, mais augmente considérablement la capacité du détenteur de données à prévenir les abus.

Outre le transfert complet et l'accès à l'endroit où les données sont stockées, il existe d'autres possibilités techniques, notamment l'accès sur l'appareil de l'utilisateur demandeur.

Si les parties optent pour l'accès à l'endroit où les données sont stockées, un certain nombre de détails doivent être réglés, notamment comment s'assurer que les idées commerciales du destinataire de données ne sont pas divulguées et quelles données le destinataire de données est autorisé à transférer sur un support sous son propre contrôle (par exemple, les données dérivées ou déduites résultant des activités de traitement du destinataire de données).

De manière générale, les conditions d'accès à l'endroit où les données sont stockées ne doivent pas porter atteinte aux droits accordés à l'utilisateur demandeur ou au destinataire de données en vertu du règlement sur les données ou d'une autre législation applicable.

L'accès à l'endroit où les données sont stockées sur un support contrôlé par un tiers de confiance sera souvent préférable à l'accès sur un support contrôlé par le détenteur de données. L'accès à l'endroit où les données sont stockées devrait normalement toujours signifier un accès à distance, et l'accès sur place devrait être limité aux situations extrêmes présentant le degré de sensibilité le plus élevé.

Les parties doivent également déterminer le calendrier de l'accès aux données. Conformément à l'article 5, paragraphe 1, du règlement sur les données, lorsque l'utilisateur le demande, les données doivent être mises à disposition sans retard injustifié et, lorsque cela est pertinent et techniquement réalisable, en continu et en temps réel.

Toutefois, cet accès n'est pas toujours nécessaire pour atteindre les finalités convenues entre le destinataire de données et l'utilisateur demandeur dans un cas spécifique. Par conséquent, les parties doivent se mettre d'accord sur des questions relatives au calendrier de l'accès aux données, telles que la question de savoir si, lorsque cela est pertinent et techniquement réalisable, l'accès est fourni en temps réel et, dans la négative, à quelle fréquence.

Les parties doivent également examiner toute une série d'autres questions, telles que les identifiants d'accès requis et le nombre d'employés du destinataire de données qui peuvent accéder aux données.

3.2.4. Si les données sont mises à disposition conformément aux spécifications de l'appendice concernant les caractéristiques des données et les modalités d'accès, et s'il apparaît que les spécifications convenues sont insuffisantes pour satisfaire aux exigences visées aux clauses 3.2.1 et 3.2.2, les parties s'engagent à entamer des négociations de bonne foi et à adapter les spécifications de manière à ce qu'elles répondent aux exigences convenues.

3.2.5. Le détenteur de données doit fournir au destinataire de données les informations nécessaires pour accéder aux données ou les recevoir, conformément à l'article 5 du règlement sur les données.

Cela inclut, en particulier, la fourniture d'informations facilement accessibles au détenteur de données concernant l'origine des données et tout droit que des tiers pourraient avoir à l'égard des données, tels que les droits des personnes concernées découlant du règlement (UE) 2016/679 (RGPD), ou les faits susceptibles de donner lieu à de tels droits.

Le détenteur de données précise ces informations à l'**appendice 2**.

Les parties restent libres de convenir de tout soutien supplémentaire, allant au-delà des exigences du règlement sur les données, gratuit ou payant.

3.2.6. Le détenteur de données s'engage à ne conserver aucune autre information sur l'accès du destinataire de données aux données demandées que celles qui sont nécessaires:

(a) à la bonne exécution i) de la demande d'accès de l'utilisateur demandeur et ii) du présent contrat;

(b) à la sécurité et à la maintenance de l'infrastructure de données; et

(c) au respect des obligations légales incombant au détenteur de données de conserver ces informations.

3.3. **Boucles de rétroaction**

3.3.1. Si le destinataire de données détecte un incident lié à la clause 3.1 sur les données couvertes par le contrat ou à la clause 3.2 sur les caractéristiques des données et les modalités d'accès et si le destinataire de données fournit au détenteur de données une description détaillée de l'incident, le détenteur de données et le destinataire de données doivent coopérer de bonne foi pour déterminer la raison de l'incident. Si l'incident a été causé par un manquement de la part du détenteur de données à ses obligations, il doit remédier à la violation dans les meilleurs délais. Si le détenteur de données ne le fait pas, cela est considéré comme une violation fondamentale et le destinataire de données peut invoquer la clause 8 du présent contrat relative aux voies de recours en cas de violation du contrat.

3.3.2. Si l'une des spécifications convenues conformément à la clause 3.2 est impossible ou excessivement onéreuse à respecter en raison d'un changement exceptionnel de circonstances survenu après la conclusion du contrat, le détenteur de données doit fournir au destinataire de données une description détaillée de cette situation et les parties entameront des négociations de bonne foi et adapteront les spécifications de manière à ce qu'elles satisfassent aux exigences énoncées dans les présentes clauses. En particulier, chaque partie doit fournir à l'autre des informations suffisantes pour évaluer, examiner et résoudre la situation particulière. La présente clause ne porte pas atteinte au droit du destinataire de données d'invoquer des voies de recours conformément à la clause 8.

3.4. **Modifications unilatérales apportées par le détenteur de données**

3.4.1. Le détenteur de données peut modifier unilatéralement les détails concernant les spécifications des caractéristiques des données et les modalités d'accès, si cela est objectivement justifié par la conduite normale des affaires du détenteur de données — par exemple par une modification technique due à une vulnérabilité immédiate en matière de sécurité dans la gamme de produits ou de services connexes proposés par le détenteur de données ou par une modification de l'infrastructure du détenteur de données. Toute modification doit répondre aux exigences des clauses 3.2.

3.4.2. Le détenteur de données doit notifier la modification au destinataire de données au moins (indiquer un délai raisonnable) avant qu'elle ne prenne effet.

Un délai de notification plus court peut suffire:

(a) lorsque la modification n'a pas d'incidence négative sur l'accès aux données et leur utilisation par le destinataire de données; ou

(b) lorsqu'une telle notification serait impossible ou déraisonnable compte tenu des circonstances, par exemple lorsque des changements immédiats sont nécessaires en raison d'une vulnérabilité en matière de sécurité qui vient d'être détectée.

3.4.3. Lorsque la modification a une incidence négative sur l'accès aux données et leur utilisation par le destinataire de données, ce dernier est en droit de résilier le contrat (ou la partie concernée du contrat) sans qu'aucune compensation ne soit due au détenteur de données, nonobstant tout autre droit ou voie de recours dont le destinataire de données pourrait disposer.

4. **(si les données doivent être protégées en tant que secrets d'affaires) Protection des secrets d'affaires**

1. **Transmission de secrets d'affaires** — Les détenteurs de données ne peuvent pas, en principe, refuser une demande d'accès aux données présentée au titre du règlement sur les données au seul motif que certaines données sont considérées comme étant des secrets d'affaires, car cela irait à l'encontre des effets attendus dudit règlement.

Voir les clauses 4.1.

2. **Secrets d'affaires** — Toutefois, si le détenteur de données constate que certaines données couvertes par le présent contrat sont protégées en tant que secrets d'affaires, tels que définis par la directive (UE) 2016/943 [8] (ci-après la «directive sur les secrets d'affaires»), il bénéficie de certains droits, principalement le droit de continuer à préserver la confidentialité des secrets en question.

Aux termes de l'article 2, point 1), de la directive sur les secrets d'affaires, on entend par «secret d'affaires» des informations qui répondent aux trois conditions suivantes: a) elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, elles ne sont pas généralement connues de personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles; b) elles ont une valeur commerciale parce qu'elles sont secrètes; et c) elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes.

On entend par «détenteur d'un secret d'affaires» toute personne physique ou morale qui a le contrôle d'un secret d'affaires de façon licite.

Les données ne peuvent être définies comme secrets d'affaires que si elles sont protégées en tant que telles par le détenteur de données ou le détenteur de secrets d'affaires lorsqu'une demande d'accès aux données est présentée conformément à l'article 5 du règlement sur les données.

Voir la clause 4.1.1.

3. **Définition initiale des secrets d'affaires** — Les droits des détenteurs de données en matière de secrets d'affaires ne sont, dans un premier temps, applicables que si et dans la mesure où les données protégées en tant que secrets d'affaires sont définies dans le contrat.

Voir la clause 4.1.2.

4. **Pendant la durée du contrat** — Les droits des détenteurs de données en matière de secrets d'affaires pourraient toutefois également s'appliquer pendant la durée du contrat, en ce qui concerne les nouvelles données qui seront mises à disposition dans le cadre de celui-ci.

Voir la clause 4.1.3.

5. **Droits d'audit** — Afin de préserver la confidentialité des données protégées en tant que secrets d'affaires, certains droits d'audit faisant intervenir des tiers indépendants doivent être pris en considération (sans interférer avec les activités du détenteur de données ou du destinataire de données), y compris les mécanismes en cas de désaccord sur les résultats du rapport d'audit.

Voir la clause 4.2.3.

6. **Droits du détenteur de secrets d'affaires (1/4)** — Le détenteur de données (ou le détenteur de secrets d'affaires tiers) peut convenir avec le destinataire de données des exigences visant à préserver la confidentialité des secrets d'affaires comme condition préalable à la transmission de ces secrets d'affaires définis, telles que la prise de certaines mesures techniques et organisationnelles proportionnées.

Voir les clauses 4.2 et 4.3.

7. **Droits du détenteur de secrets d'affaires (2/4)** — Si les mesures initiales ne suffisent pas, le détenteur de secrets d'affaires peut, au cas par cas, pour des données spécifiques constituant des secrets d'affaires et protégées en tant que telles, soit augmenter unilatéralement le niveau des mesures, soit demander que des mesures supplémentaires soient convenues avec le destinataire de données. En l'absence d'accord sur les mesures nécessaires, le détenteur de données peut suspendre le partage de données spécifiques protégées en tant que secrets d'affaires, dans les conditions énoncées dans le règlement sur les données.

Voir la clause 4.4.2.

8. **Droits du détenteur de secrets d'affaires (3/4)** — Le détenteur de secrets d'affaires peut également, au cas par cas, refuser de partager des secrets d'affaires définis spécifiques, uniquement dans des circonstances exceptionnelles et dans les conditions énoncées dans le règlement sur les données.

Voir la clause 4.4.3.

9. **Droits du détenteur de secrets d'affaires (4/4)** – Le détenteur de secrets d'affaires peut bloquer ou suspendre le partage de données si le destinataire de données manque à ses obligations en matière de protection des secrets d'affaires.

Voir la clause 4.4.4.

10. **Conservation de données contenant des secrets d'affaires définis** — Si le détenteur de données bloque ou suspend le partage de données conformément aux clauses 4.4.1, 4.4.2 ou 4.4.3, il sera toujours tenu de maintenir les données connexes contenant des secrets d'affaires définis facilement accessibles en les conservant jusqu'à ce qu'elles puissent être partagées dans le cadre du contrat.

Voir la clause 4.5.

11. **Détenteur de secrets d'affaires définis tiers** — Si le détenteur de secrets d'affaires est un tiers, le détenteur de données doit veiller à ce que la clause 4 protège également ses secrets d'affaires et obtenir toutes les autorisations pertinentes dudit détenteur de secrets d'affaires tiers.

Voir la clause 4.1.2.

4.1. **Applicabilité des accords relatifs aux secrets d'affaires**

4.1.1. Les mesures de protection convenues dans les clauses 4.2 et 4.3 du présent contrat, ainsi que les droits connexes convenus dans les clauses 4.4, s'appliquent exclusivement aux données ou métadonnées figurant dans les données que le détenteur de données doit mettre à la disposition du destinataire de données et qui sont protégées en tant que secrets d'affaires [tels que définis à l'article 2, point 1), de la directive sur les secrets d'affaires], détenus par le détenteur de données ou un autre détenteur de secrets d'affaires (tel que défini à l'article 2, point 2), de ladite directive)].

4.1.2. La définition des données protégées comme secrets d'affaires et l'identité du détenteur de secret d'affaires figurent à l'appendice 4.

Le détenteur de données déclare au destinataire de données qu'il dispose de tous les droits pertinents de la part de tout détenteur de secrets d'affaires tiers pour conclure le présent contrat en ce qui concerne les données protégées en tant que secrets d'affaires.

Conformément à l'article 5, paragraphe 9, du règlement sur les données, «*le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires, recense les données qui sont protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes*».
Par conséquent, le détenteur de données devrait recenser les données protégées en tant que secrets d'affaires à l'**appendice 4**. Toutefois, le détenteur de données ne devrait pas être tenu de décrire lui-même le secret d'affaires. Il suffit de déterminer les données qui doivent être protégées pour garantir la confidentialité du secret d'affaires, car l'analyse de ces données est susceptible de révéler le secret d'affaires.

4.1.3. Si, au cours du présent contrat, de nouvelles données protégées en tant que secrets d'affaires sont mises à la disposition du destinataire de données conformément à la clause 4.1.1, à la demande du détenteur de données, l'appendice 4 sera modifié en conséquence.

Tant que l'appendice 4 n'a pas été modifié et approuvé par les parties, le détenteur de données peut bloquer ou suspendre temporairement le partage des nouvelles données protégées en tant que secrets d'affaires. La décision du détenteur de données est dûment motivée et communiquée par écrit à l'utilisateur sans retard injustifié. Le détenteur de données notifie également à l'autorité compétente désignée en vertu de l'article 37 du règlement sur les données qu'il a bloqué ou suspendu le partage de données et indique quelles mesures n'ont pas été convenues ou mises en œuvre.

4.1.4. Les obligations énoncées aux clauses 4.2 et 4.3 restent en vigueur après toute résiliation du contrat, sauf si les parties en conviennent autrement.

4.2. **Mesures de protection prises par le destinataire de données**

4.2.1. Le destinataire de données doit appliquer les mesures de protection énoncées à l'**appendice 4** (ci-après les «mesures de protection du destinataire de données»).

Les parties devraient, dans un appendice distinct, exposer toutes les modalités de ces mesures, y compris pour les situations dans lesquelles le destinataire de données partage les données avec des tiers. Les mesures peuvent être à la fois techniques (par exemple, cryptage, pare-feu, stockage fractionné, etc.) et organisationnelles (par exemple, gouvernance interne, gestion appropriée de l'identité et contrôles d'accès, participation d'un tiers de confiance).

Étant donné que les mesures doivent être proportionnées, leur contenu variera en fonction de la nature du secret d'affaires. Les mesures dépendront également de la question de savoir si i) l'accès doit être fourni à l'endroit où les données sont stockées ou si ii) les données doivent être entièrement transférées au destinataire de données. Dans le premier cas, le détenteur de données a un degré de contrôle plus élevé et peut appliquer lui-même une partie des mesures de protection, tandis que le destinataire de données peut avoir un niveau d'utilisation des données moins élevé. Dans tous les cas, les deux parties devront s'attacher à produire les effets escomptés du règlement sur les données. Pour cette raison, les différents intérêts doivent être conciliés sans porter atteinte à ces effets recherchés.

4.2.2. Si le destinataire de données est autorisé dans le présent contrat et dans le contrat conclu par le destinataire de données avec l'utilisateur à mettre les données à la disposition d'un tiers, le destinataire de données peut partager les données protégées en tant que secrets d'affaires dans les conditions suivantes:

(a) s'il informe le détenteur de données, sans retard injustifié, du fait que les données protégées en tant que secrets d'affaires seront mises à la disposition d'un tiers, s'il précise les données en question et s'il indique au détenteur de données l'identité, le lieu d'établissement et les coordonnées du tiers.

(b) le tiers applique les mesures de protection prévues à l'appendice 4.

4.2.3. [OPTION] [Afin de vérifier si et dans quelle mesure le destinataire de données a mis en œuvre et maintient les mesures de protection du destinataire de données, celui-ci accepte soit i) d'obtenir chaque année un rapport d'évaluation de la conformité en matière de sécurité auprès d'un tiers indépendant qu'il a choisi, soit ii) d'autoriser chaque année un audit de l'évaluation de la conformité en matière de sécurité auprès d'un tiers indépendant choisi par le détenteur de données, sous réserve que ce tiers indépendant ait signé un accord de confidentialité tel que fourni par le destinataire de données. Ce rapport d'audit de sécurité doit démontrer la conformité du destinataire de données avec la clause 4 et l'appendice 4 applicables à ce moment-là. Les résultats des rapports d'audit seront communiqués aux deux parties dans les meilleurs délais.

Le destinataire de données peut choisir entre les options i) et ii). Si une partie estime que le rapport d'audit de sécurité est incorrect, elle conserve le droit d'obtenir un rapport d'audit de sécurité auprès d'un autre tiers indépendant. Si ce droit est exercé, les deux auditeurs tiers indépendants, conjointement avec les parties, examineront toute différence entre ces deux rapports et s'efforceront de résoudre toute question en suspens dans le respect de l'exigence de bonne foi.]

Les coûts de ces rapports d'audit seront supportés comme suit: (*préciser les modalités de paiement de ces coûts*).

La présente clause est indiquée comme une option, car les parties peuvent convenir d'autres mesures afin de vérifier le respect par l'utilisateur de ses obligations de mettre en œuvre et de maintenir les mesures de protection du destinataire de données.

4.3. **Mesures de protection prises par le détenteur de secrets d'affaires**

4.3.1. Le détenteur de données peut appliquer les mesures convenues à l'**appendice 4** pour préserver la confidentialité des données protégées en tant que secrets d'affaires (ci-après les «mesures de protection du détenteur de secret d'affaires»).

4.3.2. Le détenteur de données peut également mettre en œuvre unilatéralement des solutions de protection techniques et organisationnelles appropriées, telles que des mises à jour logicielles, si elles n'ont pas d'incidence négative sur le destinataire de données au titre du présent contrat.

4.3.3. Le destinataire de données s'engage à ne pas modifier ni supprimer les mesures de protection du détenteur de secrets d'affaires ni les mesures prises conformément à la clause 4.3.2, sauf si les parties en conviennent autrement.

4.4. **Obligation de partager et droit de refuser, de bloquer ou de résilier**

4.4.1. Lorsque les mesures de protection du destinataire de données et du détenteur de secrets d'affaires ne suffisent pas matériellement à protéger de manière appropriée des données spécifiques protégées en tant que secret d'affaires, le détenteur de données peut, en adressant au destinataire de données une notification décrivant en détail l'insuffisance des mesures, demander que des mesures techniques ou organisationnelles nécessaires supplémentaires soient convenues; en l'absence d'accord sur de telles mesures après un délai raisonnable et si la nécessité de telles mesures est dûment justifiée, par exemple dans un rapport d'audit de sécurité, le détenteur de données peut bloquer ou suspendre le partage des données spécifiques en question; dans ce cas, le détenteur de données doit adresser une notification au destinataire de données et à l'autorité compétente désignée en vertu de l'article 37 du règlement sur les données; la notification doit être dûment motivée, indiquer quelles mesures n'ont pas été convenues, le cas échéant, les secrets d'affaires concernés, et être faite par écrit sans retard injustifié; le détenteur de données doit continuer à partager toutes les données protégées en tant que secrets d'affaires autres que ces données spécifiques.

4.4.2. Si, dans des circonstances exceptionnelles, le détenteur de données peut démontrer qu'il risque fortement de subir un préjudice économique grave du fait de la divulgation au destinataire de données de certaines données protégées en tant que secret d'affaires malgré la mise en œuvre des mesures de protection du destinataire de données et, le cas échéant, des mesures de protection du détenteur de secrets d'affaires, le détenteur de données peut suspendre le partage des données spécifiques en question.

Il ne peut le faire que s'il adresse une notification dûment motivée au destinataire de données et à l'autorité compétente désignée en vertu de l'article 37 du règlement sur les données.

Toutefois, le détenteur de données doit continuer à partager toutes les données protégées en tant que secrets d'affaires autres que ces données spécifiques.

Le refus ou la suspension du partage de données au titre de l'article 5 du règlement sur les données est limité à des circonstances exceptionnelles. Par conséquent, la notification doit être dûment motivée. Les aspects à prendre en compte peuvent être, par exemple, l'absence d'applicabilité de la protection des secrets d'affaires dans les pays tiers, la nature et le niveau de confidentialité du secret d'affaires en question ou le caractère unique et novateur du produit connecté concerné.

4.4.3. Si le destinataire de données ne met pas en œuvre et ne maintient pas les mesures de protection du destinataire de données et si ce manquement est dûment justifié par le détenteur de données, par exemple dans un rapport d'audit de sécurité, le détenteur de données a le droit de bloquer ou de suspendre la transmission des secrets d'affaires définis spécifiques jusqu'à ce que le destinataire de données ait résolu l'incident.

Dans ce cas, le détenteur de données doit adresser, sans retard injustifié et par écrit, une notification dûment motivée au destinataire de données et à l'autorité compétente désignée en vertu de l'article 37 du règlement sur les données.

4.4.4. La clause 4.4.1 n'autorise pas le détenteur de données à résilier le contrat. Les clauses 4.4.2 ou 4.4.3 autorisent le détenteur de données à résilier le contrat uniquement en ce qui concerne les secrets d'affaires définis spécifiques, et si:

(a) toutes les conditions de la clause 4.4.2 ou de la clause 4.4.3 sont remplies;

(b) aucune solution n'a été trouvée par les parties après un délai raisonnable, malgré une tentative de trouver une solution à l'amiable, y compris après l'intervention de l'autorité compétente désignée en vertu de l'article 37 du règlement sur les données; et

(c) le destinataire de données n'a pas obtenu d'une juridiction compétente une décision de justice obligeant le détenteur de données à mettre les données à disposition et aucune procédure judiciaire n'est en cours pour une telle décision.

4.5. **Conservation de données protégées en tant que secrets d'affaires définis**

4.5.1. Lorsque le détenteur de données exerce le droit de bloquer ou de suspendre le partage de données conformément aux clauses 4.4.1, 4.4.2 et 4.4.3, il devra veiller à ce que les données en question soient conservées, de sorte que lesdites données soient mises à la disposition du destinataire de données:

(a) une fois que les protections appropriées ont été convenues et mises en œuvre; ou

(b) une fois qu'une décision contraignante est rendue par une autorité ou une juridiction compétente exigeant du détenteur de données qu'il fournisse les données au destinataire de données.

Cette obligation de conservation prend fin lorsqu'une autorité compétente ou une juridiction, dans une décision contraignante, autorise la suppression de ces données conservées ou lorsque le contrat prend fin conformément à la clause 4.4.4.

4.5.2. Le détenteur de données supportera les coûts nécessaires à la conservation des données en vertu de la clause 4.5.1. Toutefois, le destinataire de données couvrira ces coûts dans la mesure où le blocage ou la suspension du partage de données a lieu conformément à la clause 4.4.3.

5. **Utilisation des données et partage avec des tiers**

5.1. **Utilisation licite par le destinataire de données**

Le destinataire de données s'engage à traiter les données mises à sa disposition en vertu du présent contrat uniquement pour les finalités et dans les conditions convenues avec l'utilisateur demandeur.

Le destinataire de données doit effacer les données lorsqu'elles ne sont plus nécessaires à la finalité convenue, sauf accord contraire avec l'utilisateur demandeur en ce qui concerne les données qui sont des données à caractère non personnel.

5.2. **Partage de données avec des tiers**

5.2.1. Le destinataire de données ne doit pas mettre les données à la disposition d'un autre tiers, sauf si cela est contractuellement convenu avec l'utilisateur demandeur, compatible avec les éventuelles mesures de protection convenues avec le détenteur de données et compatible avec le droit de l'Union ou le droit national applicable.

Dans tous les cas, le destinataire de données ne doit pas mettre les données qu'il reçoit à la disposition d'une entreprise désignée comme contrôleur d'accès conformément à l'article 3 du règlement (UE) 2022/1925 (règlement sur les marchés numériques).

5.2.2. Lorsque le destinataire de données est autorisé à mettre des données à la disposition d'un tiers, il doit prendre les mesures contractuelles, techniques et organisationnelles appropriées pour s'assurer que:

(a) (*le cas échéant*) le tiers applique au moins les mêmes mesures de protection que celles que le destinataire de données doit appliquer en vertu de la clause 4.2 et respecte les mesures de protection prises par le détenteur de données en vertu de la clause 4.3;

(b) le tiers utilise les données exclusivement d'une manière compatible avec les clauses 5.1 et 5.3;

(c) le détenteur de données dispose au moins des mêmes voies de recours contre le tiers que contre le destinataire de données pour l'utilisation ou la divulgation de données interdite en vertu de la clause 5.3.

5.2.3. Nonobstant les clauses 5.2.1 et 5.2.2, le destinataire de données peut utiliser des services de traitement, par exemple des services d'informatique en nuage (y compris une infrastructure à la demande, une plateforme à la demande et un logiciel à la demande), des services d'hébergement ou des services similaires pour atteindre, pour son propre compte et sous sa propre responsabilité, les finalités convenues à la clause 5.1. Les tiers peuvent également utiliser ces services pour atteindre, pour leur propre compte et sous leur propre responsabilité, les finalités pour lesquelles les données sont partagées avec eux.

5.3. **Utilisation ou partage non autorisé de données**

5.3.1. Le destinataire de données ne peut pas:

(a) (aux fins de l'obtention de données) fournir de fausses informations au détenteur de données, avoir recours à des moyens trompeurs ou coercitifs ou tirer avantage de lacunes dans l'infrastructure technique du détenteur de données destinée à protéger les données; ou

(b) ne pas maintenir les mesures techniques ou organisationnelles contractuelles convenues en vertu des clauses 4.2 et 4.3; ou

(c) modifier ou supprimer, sans l'accord du détenteur de données, les mesures de protection techniques appliquées par le détenteur de données pour empêcher l'accès non autorisé aux données et garantir le respect du présent contrat; ou

(d) utiliser les données qu'il a reçues à des fins non autorisées, en violation de la clause 5.1; ou

(e) se servir des données pour mettre au point un produit concurrençant le produit, ni partager les données avec un tiers à cette fin;

(f) utiliser les données pour obtenir des informations sur la situation économique, les actifs et les méthodes de production du détenteur de données, ou sur son utilisation des données;

(g) utiliser les données d'une manière qui nuit à la sécurité du produit ou du service connexe;

(h) utiliser les données pour le profilage des personnes physiques, sauf si cela est nécessaire pour fournir le service demandé par l'utilisateur demandeur;

(i) divulguer les données à un autre tiers de manière illégale ou en violation des clauses 5.2.1 et 5.2.2.

Si le destinataire de données commet l'un de ces actes, cela constitue une inexécution essentielle telle que décrite à la clause 8.1.1 et a les conséquences supplémentaires décrites à la clause 5.3.2.

5.3.2. Dans les cas visés à la clause 5.3.1, le destinataire de données doit donner suite, sans retard injustifié, aux demandes du détenteur de données ou de l'utilisateur demandeur:

(a) informer l'utilisateur demandeur de l'utilisation ou de la divulgation non autorisée des données et des mesures prises pour y mettre fin;

(b) effacer les données mises à disposition par le détenteur de données en vertu du présent contrat, ou obtenues de manière non autorisée ou abusive, et les éventuelles copies de celles-ci;

(c) indemniser le détenteur de données, l'utilisateur demandeur ou un autre tiers protégé pour tout préjudice subi du fait de l'utilisation ou de la divulgation non autorisée;

(d) mettre fin à la production, à l'offre, à la mise sur le marché ou à l'utilisation de biens, de données dérivées ou de services produits sur la base des connaissances obtenues au moyen de ces données, ou à l'importation, à l'exportation ou au stockage de biens non conformes aux fins précitées; et

(e) détruire tout bien non conforme, i) s'il existe un risque grave que l'utilisation illicite des données cause un préjudice important au détenteur de données, au détenteur de secrets d'affaires ou à l'utilisateur, ou ii) si une telle mesure ne serait pas disproportionnée au regard des intérêts du détenteur de données, du détenteur de secrets d'affaires ou de l'utilisateur.

6. **Compensation pour la fourniture d'un accès aux données**

Les parties devraient, dans le contrat lui-même ou dans un appendice distinct, déterminer les modalités de la compensation.

Elles devraient se mettre d'accord, au minimum, sur les points suivants:

— le montant de la compensation due et la devise;

— la date d'échéance du paiement;

— les modalités de paiement.

Conformément au règlement sur les données, cette compensation peut toujours inclure une compensation pour les coûts occasionnés par la mise à disposition des données. Elle peut également inclure une marge, sauf lorsque le bénéficiaire de données est une PME ou une organisation à but non lucratif. Elle doit dans tous les cas être raisonnable.

Conformément à l'article 9, paragraphe 2, du règlement sur les données, «[l]es coûts occasionnés par la mise à disposition des données, dont, notamment, les coûts encourus pour le formatage des données, leur diffusion par voie électronique et leur stockage» ainsi que, si la compensation inclut une marge, «[l]es investissements dans la collecte et la production de données, le cas échéant, en prenant en compte le fait que d'autres parties ont contribué ou non à l'obtention, à la production ou à la collecte des données en question» doivent être pris en compte pour déterminer la compensation.

En vertu de l'article 9, paragraphe 3, du règlement sur les données, la compensation peut également dépendre du volume, du format et de la nature des données. En vertu de l'article 9, paragraphe 7, du règlement sur les données, le détenteur de données doit dans tous les cas fournir des informations exposant la base de calcul de la compensation de manière suffisamment détaillée pour permettre au destinataire de données d'évaluer si les exigences légales sont respectées.

6.1. **(Applicable si le détenteur de données est considéré comme une PME/un organisme de recherche à but non lucratif)**

6.1.1. Le destinataire de données déclare être une PME au sens de la recommandation 2003/361/CE *ou* un organisme de recherche à but non lucratif. Il déclare en outre qu'il n'a pas d'entreprises partenaires ou d'entreprises liées (ci-après les «entreprises») qui, au sens de l'article 3 de l'annexe de la recommandation 2003/361/CE, ne sont pas considérées comme des PME.

[OPTION] [La preuve de ce qui précède est fournie à l'**appendice 3**.]

6.1.2. Les parties conviennent que le destinataire de données indemnisera le détenteur de données [OPTION 1] [comme suit: (*veuillez préciser*)] [OPTION 2] [comme spécifié à l'**appendice 3**].

6.1.3. Le détenteur de données déclare que la compensation convenue n'excède pas les coûts directement liés à la mise à disposition des données au destinataire de données et qui sont imputables à la demande. Ces coûts comprennent les coûts encourus pour la reproduction des données ainsi que leur diffusion par voie électronique et leur stockage, mais pas pour la collecte ou la production de données.

Les informations exposant la base de calcul de la compensation, qui permettent au destinataire de données de vérifier que ces exigences sont respectées, sont fournies par le détenteur de données à l'**appendice 3**.

6.1.4. Le destinataire de données informera immédiatement le détenteur de données de tout changement remettant en cause sa qualification en tant que PME.

Lorsque le destinataire de données cesse d'être une PME, les parties s'engagent à entamer des négociations sur le montant de la compensation raisonnable. En l'absence d'accord après un délai raisonnable, le détenteur de données peut suspendre le partage des données en adressant une notification au destinataire de données.

Dans ce cas, le détenteur de données doit veiller à ce que les données soient conservées, de sorte que lesdites données soient mises à la disposition du destinataire de données une fois que la compensation est convenue ou qu'une décision contraignante est rendue par une autorité ou une juridiction compétente exigeant du détenteur de données qu'il fournisse les données au destinataire de données.

Le détenteur de données supportera les coûts nécessaires à la conservation des données. Toutefois, le destinataire de données doit indemniser le détenteur de données pour tout préjudice économique subi du fait qu'il n'a pas informé le détenteur de données.

6.2. **(Applicable si le destinataire de données n'est pas considéré comme une PME/un organisme de recherche à but non lucratif)**

6.2.1. Les parties conviennent que le destinataire de données indemnisera le détenteur de données [OPTION 1] [comme suit: *(veuillez préciser)*] [OPTION 2] [comme spécifié à l'**appendice 3**].

Les informations exposant la base de calcul de la compensation, qui permettent au destinataire de données de vérifier que ces exigences sont respectées, sont fournies par le détenteur de données à l'**appendice 3**.

6.2.2. (*applicable en cas de compensation monétaire*) En cas de retard dans le paiement de la compensation, le destinataire de données devrait verser au détenteur de données des intérêts sur la compensation exigible à compter de la date d'échéance du paiement jusqu'à la date du paiement, conformément au droit applicable.

6.2.3. Si le destinataire de données devient une PME et en informe le détenteur de données, les parties s'engagent à modifier le montant de la compensation raisonnable conformément à l'article 9, paragraphe 4, du règlement sur les données.

7. **Date d'application, durée du contrat et résiliation**

7.1. **Date d'application et durée**

7.1.1. Le présent contrat [OPTION 1] [prend effet immédiatement] [OPTION 2] [prend effet à compter du *(préciser la date)*].

7.1.2. [OPTION] [Le présent contrat est conclu pour [OPTION 1] [une durée indéterminée] [OPTION 2] [une durée déterminée de (*préciser)*], sous réserve de tout motif d'expiration ou de résiliation en vertu du présent contrat.]

Lors de l'examen de la durée du contrat, les parties devraient être guidées en premier lieu par la demande de l'utilisateur et le contrat conclu entre l'utilisateur et le destinataire de données. Si la demande porte sur une **fourniture ponctuelle** de données, il suffit de convenir de la date d'application.

Si la demande porte sur une **fourniture continue** de données, les parties devront convenir de la durée du contrat et choisir soit une période indéterminée, soit une période fixe, selon que l'utilisateur demandeur a précisé ou non une période particulière.

7.1.3. [OPTION] [Le détenteur de données doit commencer à mettre les données à la disposition du destinataire de données [OPTION 1] [sans retard injustifié après l'entrée en vigueur du contrat] [OPTION 2] [le (*préciser la date et, le cas échéant, donner de plus amples informations sur le calendrier*)].]

Généralement, les parties souhaitent que l'exécution commence juste après l'entrée en vigueur du contrat. Toutefois, ce n'est pas nécessairement le cas, par exemple si l'une des parties ou les deux doivent encore se préparer à l'exécution.

7.2. **Résiliation**

7.2.1. Indépendamment de la période contractuelle convenue en vertu de la clause 7.1.1, et sans préjudice de la clause 2.4.3, le présent contrat prend fin:

(a) lors de la destruction du produit ou de l'arrêt définitif du service connexe, ou lorsque le produit ou le service connexe perd sa capacité à générer les données de manière irréversible; ou

(b) lorsque les deux parties en conviennent.

7.2.2. Le destinataire de données peut résilier le contrat à tout moment au cours de la période contractuelle en donnant au détenteur de données un préavis de (*indiquer la durée*). Le destinataire de données doit notifier à l'utilisateur demandeur que le contrat a été résilié.

[OPTION] Lorsque le destinataire de données résilie le contrat en vertu de la présente clause avant (*indiquer la date ou la durée minimale du contrat*), il doit indemniser le détenteur de données pour les coûts supportés par celui-ci aux fins de la mise à disposition des données, comme suit: *(veuillez préciser)*.

Dans certains cas, le détenteur de données engage des dépenses pour mettre les données à la disposition du destinataire de données, par exemple en adaptant son infrastructure numérique, en étant convaincu que ces dépenses seront amorties au fil du temps.

Dans ce cas, le détenteur de données peut souhaiter s'assurer qu'il reçoit une compensation de la part du destinataire de données.

7.3. **Effets de l'expiration et de la résiliation**

7.3.1. L'expiration de la période contractuelle ou la résiliation du présent contrat libère les deux parties de leur obligation d'exécuter et de recevoir une exécution dans l'avenir, mais n'a pas d'incidence sur les droits et obligations acquis jusqu'au moment de l'expiration ou de la résiliation.

L'expiration ou la résiliation n'a pas d'incidence sur les dispositions qui restent applicables même après la fin du contrat, en particulier les éventuelles limitations de l'utilisation et du partage autorisés des données par le destinataire de données en vertu de la clause 5, de la clause 4 relative aux secrets d'affaires, de la clause 9.1 relative à la confidentialité, de la clause 9.5 relative au droit applicable et de la clause 9.7 relative au règlement des litiges.

7.3.2. [OPTION 1] [Le détenteur de données doit prendre des mesures de soutien à la sortie appropriées, comme le détenteur de données peut raisonnablement s'y attendre.] [OPTION 2] [Le détenteur de données doit prendre les mesures de soutien à la sortie suivantes: *(veuillez préciser)*]

Les parties peuvent examiner si le destinataire de données exige des mesures de soutien à la sortie.

Cela sera pertinent, par exemple, si le destinataire de données était autorisé à extraire des données d'un support contrôlé par le détenteur de données, mais qu'il n'avait pas encore extrait les données car il ne s'attendait pas à ce que le contrat soit résilié.

8. **Voies de recours en cas de violation du contrat**

Les parties peuvent souhaiter s'entendre non seulement sur les droits et obligations spécifiques aux données (dont beaucoup découlent déjà du règlement sur les données), mais aussi sur des questions de droit général des contrats, telles que les droits et voies de recours d'une partie contractante en cas d'inexécution de la part de l'autre partie contractante.

En ce qui concerne ces questions de droit général des contrats, les parties peuvent souhaiter se fonder sur des règles légales par défaut ou sur d'autres modèles de contrat.

Si elles souhaitent utiliser les présentes clauses contractuelles types, elles doivent s'assurer qu'elles sont compatibles avec toute autre loi nationale impérative susceptible d'être applicable au contrat.

8.1. **Cas d'inexécution**

8.1.1. L'inexécution d'une obligation par une partie est essentielle si:

(a) elle prive substantiellement l'autre partie de ce qu'elle était en droit d'attendre du présent contrat, à moins que la partie défaillante n'ait pas prévu et n'ait pas pu raisonnablement prévoir ce résultat; ou

(b) il ressort clairement des circonstances que l'on ne peut pas compter dans l'avenir sur une exécution par la partie défaillante.

8.1.2. Une partie est exonérée des conséquences de l'inexécution lorsque celle-ci est due à un empêchement qui lui échappe et si l'on ne pouvait raisonnablement attendre de cette partie qu'elle le prenne en considération au moment de la conclusion du présent contrat, ou qu'elle le prévienne ou le surmonte ou qu'elle en prévienne ou en surmonte les conséquences.

Lorsque l'empêchement exonératoire n'est que temporaire, l'exonération d'inexécution de la partie vaut pour la durée de l'empêchement. Cependant, si le retard équivaut à une inexécution essentielle, l'autre partie peut le traiter comme telle.

La partie défaillante doit faire en sorte que l'autre partie reçoive, sans retard excessif, notification de l'empêchement et de ses effets sur sa capacité de s'exécuter à partir du moment où la partie défaillante a eu, ou a pu avoir raisonnablement connaissance de ces circonstances. L'autre partie a droit à des dommages et intérêts en réparation du préjudice économique résultant de la non-réception de cette notification.

8.2. **Voies de recours en cas d'inexécution**

8.2.1. En cas d'inexécution par une partie, l'autre partie dispose des voies de recours énumérées dans les clauses suivantes, sans préjudice des voies de recours prévues par le droit applicable.

8.2.2. Les moyens d'action qui ne sont pas incompatibles peuvent être cumulés.

8.2.3. Une partie ne peut recourir à aucun moyen d'action dans la mesure où elle a provoqué l'inexécution de l'autre partie, par exemple lorsqu'une défaillance dans sa propre infrastructure de données n'a pas permis à l'autre partie de s'acquitter dûment de ses obligations. Une partie ne peut pas non plus introduire une demande de dommages et intérêts dans la mesure où elle aurait pu réduire son préjudice en prenant des mesures raisonnables.

8.2.4. La partie lésée peut:

(a) demander à la partie défaillante de se conformer, sans retard injustifié, aux obligations qui lui incombent en vertu du présent contrat, à moins que cela ne soit illicite ou impossible ou à moins qu'une exécution spécifique n'entraîne pour la partie défaillante des coûts disproportionnés par rapport au bénéfice que l'autre partie en retirerait;

(b) suspendre sa propre exécution au titre du présent contrat, à moins que cela ne cause vraisemblablement un préjudice à la partie défaillante qui soit manifestement disproportionné au regard de la gravité de l'inexécution (le cas échéant) [pour autant que toutes les conditions énoncées à la clause 4.4.4 soient remplies, si le destinataire de données ne met pas en œuvre ou ne maintient pas les mesures de protection du destinataire de données convenues à la clause 4.2.1];

(c) résilier le contrat avec effet immédiat et sans pénalité, en adressant une notification à l'autre partie, si:

i) l'inexécution de l'autre partie est essentielle; ou

ii) dans le cas d'une inexécution qui n'est pas essentielle, la partie lésée a, par notification, imparti un délai raisonnable pour remédier à l'inexécution et ce délai a expiré sans que l'autre partie ne se soit exécutée;

iii) (*le cas échéant*) [pour autant que toutes les autres conditions énoncées à la clause 4.4.5 soient remplies, dans les cas décrits à la clause 4.4.2 ou à la clause 4.4.3;]

(d) demander des dommages et intérêts pour le préjudice économique qui lui a été causé par l'inexécution de l'autre partie et qui ne bénéficie pas d'une exonération en vertu de la clause 8.1.2; la partie défaillante n'est responsable que des dommages qu'elle avait prévus ou qu'elle aurait raisonnablement dû prévoir au moment de la conclusion du présent contrat en raison de son inexécution, sauf si celle-ci était intentionnelle ou résultait d'une négligence grave.

8.2.5. [OPTION] Lorsqu'une partie n'exécute pas les obligations qui lui incombent en vertu du présent contrat, elle s'acquitte, en tout état de cause, des pénalités exposées en détail à l'**appendice 5**, que les parties considèrent comme des dommages et intérêts au sens de la clause 8.2.4, point d). La partie défaillante a le droit de demander que la pénalité soit réduite à un montant raisonnable si elle peut prouver que celle-ci est manifestement excessive par rapport au préjudice résultant de l'inexécution.

Les parties peuvent souhaiter établir des sanctions pour certains types d'inexécution, car il peut être trop onéreux pour la partie lésée de prouver le montant du préjudice réel causé, par exemple, par un défaut de fourniture de données. Les sanctions devraient être proportionnées.

9. Dispositions générales

9.1. Confidentialité

9.1.1. Les informations suivantes doivent être considérées comme confidentielles:

(a) les informations relatives aux secrets d'affaires, à la situation financière ou à tout autre aspect concernant les activités d'une partie, sauf si cette partie a rendu ces informations publiques;

(b) les informations exposant la base de calcul de la compensation raisonnable;

(c) les informations relatives à l'utilisateur demandeur et à tout tiers, sauf s'ils ont déjà rendu ces informations publiques.

9.1.2. Les deux parties conviennent de prendre toutes les mesures raisonnables pour conserver en toute sécurité les informations confidentielles et de ne pas mettre ces informations à la disposition d'un tiers, sauf dans les cas suivants:

(a) si l'une des parties a l'obligation légale de mettre à disposition les informations pertinentes, par exemple pour se conformer à l'obligation de fournir des informations attestant l'absence de discrimination conformément à l'article 8, paragraphe 3, du règlement sur les données; ou

(b) s'il est nécessaire que l'une des parties mette à disposition les informations pertinentes pour s'acquitter des obligations qui lui incombent en vertu du présent contrat; ou

(c) si l'une des parties a obtenu le consentement préalable de l'autre partie ou de la partie qui a fourni les informations confidentielles ou qui est concernée par leur divulgation.

9.1.3. Dans tous les cas, le détenteur de données peut divulguer ou mettre à la disposition [OPTION 1] [de l'utilisateur demandeur le contrat] [OPTION 2] [de l'utilisateur demandeur les informations nécessaires pour démontrer qu'il respecte les obligations qui lui incombent i) envers le destinataire de données en vertu de l'article 5 du règlement sur les données ou ii) découlant d'un contrat conclu avec l'utilisateur demandeur en vertu de l'article 4, paragraphe 6, du règlement sur les données].

9.1.4. Ces obligations de confidentialité restent applicables après la résiliation du contrat pendant une durée de (*préciser la durée*).

9.1.5. Ces obligations de confidentialité ne suppriment aucune des obligations plus strictes au titre i) du RGPD, ii) des dispositions mettant en œuvre la directive 2002/58/CE ou la directive (UE) 2016/943, ou iii) de toute autre disposition du droit de l'Union ou du droit d'un État membre.

9.2. **Non-discrimination**

Le détenteur de données déclare que les termes du présent contrat et toute pratique liée à son exécution ne donnent pas lieu à une discrimination entre des catégories comparables de destinataires de données, y compris l'une de leurs entreprises partenaires ou entreprises liées (ci-après les «entreprises»), telles que définies à l'article 3 de l'annexe de la recommandation 2003/361/CE, lors de la mise à disposition des données.

Si le destinataire de données considère que les conditions dans lesquelles des données ont été mises à sa disposition sont discriminatoires, le détenteur de données doit, à la demande du destinataire de données, fournir sans retard injustifié des informations attestant l'absence de discrimination.

9.3. **Moyens de communication**

Toute notification ou autre communication requise par le présent contrat doit être effectuée par écrit et peut être remise en main propre, envoyée par courrier prépayé ou transmise par voie électronique, y compris par courrier électronique, à condition que l'expéditeur conserve la preuve de l'envoi aux adresses énumérées ci-dessous:

Partie	Personne de contact	Adresse électronique	Numéro de téléphone	Adresse
Utilisateur	[Nom]/[Fonction]	[Adresse électronique]	[Numéro de téléphone]	[Adresse]
Destinataire de données	[Nom]/[Fonction]	[Adresse électronique]	[Numéro de téléphone]	[Adresse]

Toute notification ou communication de ce type est réputée reçue:

(a) en cas de remise en main propre, à la date de livraison;

(b) en cas d'envoi par courrier prépayé, le troisième jour ouvrable suivant l'envoi;

(c) en cas d'envoi par voie électronique, à la date de transmission, à condition qu'aucun message d'erreur indiquant un défaut de transmission n'ait été reçu par l'expéditeur.

9.4. **Contrat indivisible, modifications et caractère détachable**

9.4.1. Le présent contrat (ainsi que ses **appendices** mentionnés dans le contrat) constitue le contrat indivisible conclu entre les parties concernant l'objet du présent contrat et annule et remplace tous les accords ou contrats et protocoles antérieurs, oraux ou écrits, entre les parties concernant l'objet du présent contrat.

9.4.2. Toute modification du présent contrat ne sera valable que si les parties en conviennent par écrit, y compris sous une forme électronique.

9.4.3. Si une disposition du présent contrat est déclarée nulle, invalide, annulable ou inapplicable pour quelque raison que ce soit, et si cette disposition est détachable des autres clauses du contrat, ces autres dispositions resteront valables et exécutoires. Toute lacune ou ambiguïté qui en résulterait dans le présent contrat sera traitée conformément à la clause 9.6.

9.5. **Droit applicable**

Le présent contrat doit être régi par le droit de (*préciser l'État membre*).

9.6. **Interprétation**

9.6.1. Le présent contrat est conclu par les parties dans le cadre de leurs droits et obligations au titre du règlement sur les données. Les dispositions du présent contrat doivent être interprétées dans le sens de leur conformité avec le règlement sur les données et d'autres dispositions du droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union, ainsi qu'avec toute disposition du droit national applicable qui est compatible avec le droit de l'Union et auquel il ne peut être dérogé par accord.

9.6.2. Si une lacune ou une ambiguïté dans le présent contrat ne peut être résolue de la manière visée à la clause 9.6.1, le présent contrat doit être interprété à la lumière des règles d'interprétation prévues par le droit applicable (voir clause 9.5).

9.7. **Règlement des litiges**

9.7.1. Les parties conviennent de tout mettre en œuvre pour régler les litiges à l'amiable et, avant de porter une affaire devant une juridiction, de soumettre leur litige à (*insérer le nom et les coordonnées d'un organisme particulier de règlement des litiges ou, pour les litiges relevant de sa compétence, renvoyer à tout organisme de règlement des litiges d'un État membre qui remplit les conditions de l'article 10 du règlement sur les données*).

[OPTION] [Les tribunaux de (*préciser l'État membre*) seront seuls compétents pour connaître de l'affaire concernant le présent contrat.]

Appendice 1

(données probantes sur la demande et, le cas échéant, tout mandat)

[À rédiger par les parties]

Appendice 2

(présentation détaillée des données couvertes par le contrat et des modalités d'accès)

Dans le présent appendice, les parties doivent présenter de manière détaillée les données couvertes par le contrat, les modalités d'accès et les moyens et informations nécessaires pour accéder aux données et les utiliser, conformément aux clauses 3.1 et 3.2.

Le présent appendice contient simplement une liste d'éléments essentiels sur lesquels les parties devraient se mettre d'accord. Tant sa forme que son contenu doivent être adaptés par les parties de manière à répondre à leurs besoins. Les parties peuvent, en particulier, ajouter des éléments à cette liste.

A. **Spécification du contenu des données**

L'appendice devrait trier et énumérer les données relatives à un produit et les données relatives à un ou des services connexes couvertes par le contrat, en indiquant le contenu des données et la fréquence de collecte (liste structurée de points de données ou catégories précises de données).

B. **Durée de conservation**

L'appendice devrait indiquer la durée de conservation, afin que l'utilisateur soit informé de la durée de disponibilité des données. Cela peut se faire de manière détaillée pour chaque point de données ou groupe de points de données.

C. **Régime des données**

L'appendice devrait préciser ici si tout ou partie des données sont des données particulières régies par un régime particulier. L'appendice pourrait, par exemple, indiquer si les données peuvent être considérées comme des données à caractère personnel et, le cas échéant, lesquelles.

D. **Structure et format des données**

L'appendice devrait préciser ici dans quel format structuré, couramment utilisé et lisible par machine les données sont mises à disposition.

E. **Moyen de transfert/d'accès**

L'appendice devrait indiquer ici par quel moyen électronique sécurisé et pratique les données seront mises à la disposition du destinataire de données par le détenteur de données, soit par transfert, soit par accès.

F. **Calendrier de l'accès aux données**

L'appendice devrait préciser le taux, la fréquence et d'autres paramètres temporels de l'accès aux données, tels que, par exemple, en temps réel, en temps quasi réel, en continu, sans retard injustifié, à une certaine fréquence.

G. **Date de commencement**

L'appendice devrait préciser la date à laquelle le détenteur de données mettra les données à la disposition du destinataire de données.

H. **Informations nécessaires à l'exercice des droits d'accès du destinataire de données**

L'appendice peut préciser ici les informations nécessaires pour permettre au destinataire de données d'exercer ses droits d'accès. Il peut s'agir d'une personne de contact chargée de résoudre les problèmes techniques, tant du côté du détenteur de données que du côté du destinataire de données.

Appendice 3

(données probantes sur la taille du destinataire de données et précisions sur le calcul de la compensation)

[À rédiger par les parties]

Appendice 4

(secrets d'affaires)

[À rédiger par les parties]

ANNEXE V

CLAUSES CONTRACTUELLES TYPES

pour les contrats de partage volontaire de données entre les responsables du partage des données et les destinataires de données

Les présentes clauses contractuelles types sont destinées aux contrats dans lesquels le partage de données est volontaire entre un responsable du partage des données et un destinataire de données, c'est-à-dire que le responsable du partage des données n'est pas tenu de partager des données en vertu du règlement (UE) 2023/2854 (ci-après le «règlement sur les données») ou de toute autre obligation légale prévue par le droit de l'Union [telle que l'article 6, paragraphes 9 et 10, du règlement sur les marchés numériques] ou le droit national.

La principale nouveauté du règlement sur les données pour ce type de relations réside dans le fait qu'il prévoit, à son article 13, un contrôle des clauses contractuelles abusives. Les clauses contractuelles concernant l'accès aux données et l'utilisation des données ou la responsabilité et les voies de recours en cas de violation ou d'extinction d'obligations liées aux données qu'une entreprise a imposées unilatéralement à une autre entreprise ne sont pas contraignantes si elles sont abusives.

Bien que le présent contrat ne soit pas destiné à remplacer les contrats de partage volontaire de données qui existent déjà, il peut servir de référence pour évaluer l'équité des clauses des contrats existants.

En cas de partage obligatoire de données relatives au produit et de données relatives au service connexe en vertu du règlement sur les données, veuillez utiliser soit les «*clauses contractuelles types pour les contrats conclus entre les détenteurs de données et les destinataires de données concernant la mise à disposition de données à la demande des utilisateurs de produits connectés et de services connexes*» (article 5 du règlement sur les données), soit les «*clauses contractuelles types pour les contrats relatifs à l'accès aux données et à leur utilisation conclus entre les détenteurs de données et les utilisateurs de produits connectés et de services connexes*» (article 4 du règlement sur les données).

Les autres scénarios de partage obligatoire de données devraient être traités séparément par les parties, en veillant à ce que les obligations découlant à la fois de la règle de droit spécifique et du chapitre III du règlement sur les données soient respectées. Des ensembles de termes spécifiques élaborés par la Commission européenne ou un État membre peuvent s'appliquer à un tel scénario de partage obligatoire de données.

1. **Parties au contrat**

Le présent contrat relatif à l'accès aux données et à leur utilisation est conclu entre

(*insérer le nom, les coordonnées et d'autres références*) (ci-après le «responsable du partage des données»)

et

(*insérer le nom, les coordonnées et d'autres références*) (ci-après le «destinataire de données»)

dénommés collectivement dans le présent contrat «les parties» et individuellement «la partie».

Le responsable du partage des données peut être toute entreprise qui:

— détient des données,

— a le droit de mettre des données à disposition sur une base volontaire, et

— contrôle, selon le cas, les caractéristiques des données ou les moyens d'accès à celles-ci, de manière à pouvoir respecter les obligations prévues dans les présentes clauses contractuelles types (si tel n'est pas le cas, un autre contrat pourrait être plus approprié).

Veuillez noter que, pour le partage de données à caractère personnel, le respect de la législation applicable en matière de protection des données est requis (y compris la nécessité d'une base juridique et, lorsque les données sont partagées avec un destinataire de données dans un pays tiers, le respect des exigences applicables aux transferts internationaux de données).

Pour les cas d'utilisation liés au règlement sur les données, le responsable du partage des données pourrait être, par exemple:

— un détenteur de données au titre de l'article 2, point 13), du règlement (UE) 2023/2854 qui a le droit de partager des données relatives au produit et des données relatives au service connexe ou qui souhaite partager des données dérivées ou déduites;

— un utilisateur d'un produit connecté ou d'un service connexe auquel des données ont été transférées par un détenteur de données (y compris, par exemple, des données provenant d'un assistant virtuel interagissant avec le produit ou le service connexe);
— un ancien destinataire de données au titre de l'article 2, point 14), du règlement (UE) 2023/2854, qui a désormais le droit d'utiliser et de mettre les données à disposition conformément à ses accords avec l'utilisateur et le détenteur de données.

Dans d'autres cas d'utilisation, le responsable du partage des données pourrait être, par exemple:

— un agriculteur qui souhaite partager des données sur les sols afin d'améliorer ses modèles de culture avec son fournisseur d'IA ou en vue de la formation, de l'amélioration ou de la mise au point de nouveaux systèmes d'IA avec un autre fournisseur d'IA;

— une entreprise qui souhaite vendre une partie de ses données commerciales à une autre entreprise;

— une université qui souhaite vendre des données à un institut de recherche sociologique pour créer des statistiques;

— une entreprise informatique qui souhaite participer à un réseau de données sur les incidents de cybersécurité afin d'améliorer la rapidité de réaction en cas d'incident.

Le destinataire de données peut être toute entreprise à laquelle le responsable du partage des données met des données à disposition et qui reçoit et utilise les données pour ses propres finalités commerciales dans le cadre du présent contrat en tant que contrepartie du responsable du partage des données.

La définition du destinataire de données dans le présent contrat couvre toute partie destinataire de tout type de partage de données, et pas seulement les destinataires de données dans le cadre des scénarios de partage obligatoire de données prévus par le règlement sur les données.

2. **Données couvertes par le contrat**

Les données couvertes par le présent contrat sont les données indiquées à l'**appendice 1** (ci-après les «données»). Si tout ou partie des données fournies au titre du présent contrat sont couvertes par un régime particulier (à l'exception des données à caractère personnel spécifiquement visées à la clause 3.2), le responsable du partage des données s'engage à recenser ces données à l'**appendice 2**, ainsi qu'à prendre des mesures appropriées pour protéger ces données conformément au régime applicable.

Détermination des régimes particuliers

Étant donné que ces clauses concernent le partage de données purement volontaire, le responsable du partage des données n'a aucune obligation de partager des données qui seraient couvertes par un régime juridique spécial (en particulier et contrairement au partage obligatoire de données prévu par le règlement sur les données, il n'existe aucune obligation de partager des données protégées en tant que secrets d'affaires). Si les données relevant du régime particulier ne sont pas partagées, elles ne doivent pas être répertoriées à l'appendice 2; toutefois, si elles sont partagées, elles doivent être répertoriées et protégées en conséquence.

Les données recensées comme telles à l'appendice 2 peuvent être, par exemple:

— protégées en tant que secrets d'affaires par le responsable du partage des données, auquel cas elles seront couvertes par la clause relative aux «secrets d'affaires»;

— considérées comme confidentielles par le responsable du partage des données, auquel cas elles seront protégées par la clause relative à la «confidentialité»;

— protégées par les droits sui generis liés à la base de données ou tout autre droit de propriété intellectuelle, auquel cas la clause relative à la «propriété intellectuelle» s'applique;

— couvertes par un règlement sectoriel (par exemple, énergie, défense, sécurité, finance, études cliniques, etc.), y compris les règlements relatifs aux espaces européens communs des données;

— soumises à des restrictions en vertu du droit de la concurrence; ou

— protégées par tout autre régime juridique pertinent que les parties souhaiteraient mettre en évidence.

Il convient de compléter la description des données couvertes par le régime juridique applicable à l'aide des informations nécessaires à l'utilisation légale et sûre des données par le destinataire de données (par exemple, dans le cas de la protection de la propriété intellectuelle, les informations relatives aux licences et aux droits d'auteur de tiers).

Le cas spécifique des espaces européens communs des données

Dans certains cas, les données pourraient être partagées dans le cadre d'un espace européen commun des données spécifique à un domaine. Ce partage de données devrait être mis en œuvre conformément aux dispositions du règlement applicable à cet espace de données, lorsqu'il s'agit d'un partage obligatoire de données en vertu dudit règlement. En dehors du champ d'application du partage obligatoire de données au titre du règlement applicable à un espace de données, le partage volontaire de données reste possible. Dans ce cas, cet ensemble de conditions peut être utilisé.

3. **Base du contrat**

3.1. **Origine des données**

3.1.1. Le responsable du partage des données déclare par la présente que les données fournies dans le cadre du présent contrat proviennent des sources suivantes: *(Veuillez préciser toutes les sources de données et, si possible, les données fournies par chaque source)*

Les parties peuvent indiquer différents types de sources, par exemple:

— les données relatives au produit ou les données relatives au service connexe au titre du règlement sur les données;

— les autres données provenant d'un produit ou d'un service connexe qui ne sont pas considérées comme des données relatives à un produit ou à un service connexe au sens du règlement sur les données (par exemple, les données dérivées ou les données provenant d'un autre logiciel, telles que les données démographiques introduites dans une application par son utilisateur);

— les données provenant de sources externes, par exemple les données fournies au responsable du partage des données par un tiers en ce qui concerne les produits ou les utilisateurs de ce tiers;

— les données créées par le responsable du partage des données (de manière autonome), par exemple les dossiers clients créés par les employés du responsable du partage des données dans son système de gestion des relations avec la clientèle, les tableaux, les données traitées, les données déduites, les données dérivées, les données fusionnées, etc.

Des garanties sont généralement prévues lorsque le responsable du partage des données qui fournit les données et le destinataire de données ne sont pas en mesure de vérifier la légalité de ces données et leur origine. Dans de tels cas, le destinataire de données doit s'appuyer sur le responsable du partage des données et peut souhaiter obtenir certaines garanties à cet égard. Toutefois, les garanties peuvent ne pas être pertinentes dans les cas où le destinataire de données est mieux placé pour vérifier et/ou assumer le risque lié aux données, par exemple en raison du fait que le responsable du partage des données est une PME et/ou que les données sont extraites directement du produit.

3.1.2. Le responsable du partage des données déclare ce qui suit:

(a) (*le cas échéant*) étant donné que les données contiennent des données à caractère non personnel relatives au produit ou relatives au service connexe [telles que définies dans le règlement (UE) 2023/2854 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (ci-après le «règlement sur les données»)] et que le responsable du partage des données au titre du présent contrat a accès aux données en sa qualité de détenteur de données, le traitement et le partage de ces données font, conformément à l'article 4, paragraphe 13, du règlement sur les données, l'objet d'un contrat avec l'utilisateur concerné tel que défini à l'article 2, point 12), du règlement sur les données (ci-après l'«utilisateur»), et le présent contrat autorise le partage des données pour les finalités prises en compte dans le cadre du présent contrat;

(b) (*le cas échéant*) étant donné que les données contiennent des données relatives au produit ou au service connexe et que le responsable du partage des données au titre du présent contrat y a eu accès en sa qualité de destinataire de données en vertu de l'article 5 du règlement sur les données, le présent contrat ne constitue pas une violation des engagements contractuels avec l'utilisateur et le détenteur de données et des obligations au titre du règlement sur les données;

(c) il détient ou possède des droits juridiques et/ou contractuels suffisants sur les données sans qu'il y ait violation ou atteinte aux droits d'autrui et aucune action, poursuite ou procédure n'est en cours à son encontre qui, si elle aboutissait à une décision défavorable, aurait un effet négatif important sur sa capacité à accorder les droits concédés en vertu du présent accord;

(d) sauf disposition contraire de l'**appendice 2** et sans préjudice de la clause 3.2, il a obtenu et conservera, pour la durée et l'objet du contrat, à ses propres frais, toutes les licences et autorisations nécessaires au partage et à l'utilisation par le destinataire de données de toute donnée obtenue auprès d'un tiers ou fournie par celui-ci.

3.1.3. (*le cas échéant*) Étant donné que les données contiennent des données relatives au produit ou au service connexe (telles que définies dans le règlement sur les données) et que le responsable du partage des données dans le cadre du présent contrat y a eu accès conformément à l'article 4 du règlement sur les données en sa qualité d'utilisateur, le destinataire de données déclare qu'il n'est pas désigné comme contrôleur d'accès conformément à l'article 3 du règlement (UE) 2022/1925 (règlement sur les marchés numériques).

3.1.4. [OPTION] [Chaque partie veille à ce que toutes les données, tous les fichiers ou tous les logiciels transmis à l'autre partie dans le cadre du présent contrat soient exempts de tout virus, logiciel malveillant, rançongiciel ou autre code préjudiciable susceptible de compromettre l'intégrité, la sécurité ou la fonctionnalité des systèmes de l'autre partie.]

3.1.5. [OPTION] [Chaque partie veille à ce que toutes les données, tous les fichiers ou tous les logiciels transmis à l'autre partie dans le cadre du présent contrat résultent d'activités de collecte de données qui sont conformes aux normes en vigueur (*préciser: normes professionnelles, éthiques, industrielles, de cybersécurité, de recherche et/ou d'IA*.]

3.2. **Respect de la législation en matière de protection des données et de la vie privée**

3.2.1. Dans la mesure où les données sont considérées comme des données à caractère personnel, chaque partie déclare qu'elles sont conformes au règlement (UE) 2016/679 (ci-après le «RGPD») et, le cas échéant, à la directive 2002/58/CE, ainsi qu'à toute autre législation applicable en matière de protection des données.

3.2.2. Les parties doivent préciser à l'**appendice 3** les informations permettant de déterminer quelles données sont considérées comme des données à caractère personnel, ainsi que les obligations respectives des parties concernant le traitement de ces données à caractère personnel dans le cadre du présent contrat.

Rôles des parties et accords en vertu du RGPD

La notion de «données à caractère personnel» au sens du RGPD est très large. Elle couvre toute donnée se rapportant à une personne physique identifiée ou identifiable. Les données à caractère non personnel peuvent devenir des données à caractère personnel, par exemple lorsqu'elles font partie d'un ensemble de données mixte ou lorsqu'elles sont combinées à de nouvelles données et que le résultat de cette combinaison permet de relier les données à une personne identifiée ou identifiable. Cela peut également se produire lorsque de nouvelles capacités de traitement des données sont créées. Les parties devraient évaluer leurs propres rôles au titre du RGPD.

Notions clés du RGPD:

— «personne concernée», la personne physique identifiée ou identifiable à laquelle les informations se rapportent;

— on entend par «responsable du traitement» la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement;

— on entend par «sous-traitant» la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Les présentes clauses s'appliquent lorsque le responsable du partage des données est un responsable du traitement ou un responsable conjoint du traitement avec une autre partie au titre du RGPD. Pour déterminer leur rôle au titre du RGPD, les parties doivent examiner si elles décident pourquoi (finalité) et comment (moyens à utiliser) les données à caractère personnel sont traitées.

— Si le responsable du partage des données partage des données avec le destinataire de données qui utilise les données à ses propres fins, les deux parties sont des responsables du traitement distincts et assument leur propre responsabilité en ce qui concerne le respect du RGPD.

— Si le responsable du partage des données partage des données avec le destinataire de données afin de poursuivre une finalité commune, le responsable du partage des données et le destinataire de données sont des responsables conjoints du traitement au sens de l'article 26 du RGPD. Ils doivent organiser conjointement la manière dont ils se conforment au RGPD.

— Lorsque des clauses contractuelles supplémentaires sont nécessaires pour garantir le respect du RGPD (par exemple, en vertu de l'article 26 ou de l'article 46), ces clauses peuvent (et devraient) être utilisées en même temps que les présentes clauses contractuelles types. Les parties peuvent les consulter à l'**appendice 3**, qui devrait généralement préciser la manière dont les exigences énoncées dans le RGPD sont respectées, y compris en ce qui concerne les rôles et responsabilités respectifs des parties au titre du RGPD.

Base juridique valable

Il devrait exister une base juridique valable au titre de l'article 6, paragraphe 1, du RGPD pour partager les données et la personne concernée doit être informée de ce traitement (ultérieur) au titre de l'article 13 ou 14 du RGPD.

— Une base juridique valable pour que le responsable du partage des données et le destinataire de données agissent en tant que deux responsables distincts ou conjoints du traitement pourrait être le consentement de la personne concernée, un contrat avec la personne concernée ou dans son intérêt ou l'intérêt légitime du ou des responsables du traitement ou d'un tiers (pour autant que les intérêts ou les droits de la personne concernée ne l'emportent pas).

— Les données ne peuvent être partagées que pour une finalité déterminée, explicite et légitime. Il pourrait s'agir, par exemple, du partage de données dans le but d'améliorer le produit, lorsque les parties ont convenu d'utiliser les données pour mettre au point conjointement une nouvelle fonctionnalité.

— Un responsable du partage des données agissant en tant que responsable du traitement pourrait également partager — sur la base de son intérêt légitime à mieux fidéliser ses clients à l'avenir — les données avec sa société mère agissant également en tant que responsable indépendant du traitement des données et utilisant les données pour créer des statistiques mondiales — sur la base de son intérêt légitime à améliorer les services fournis à l'échelle mondiale par le groupe.

Le destinataire de données devrait recevoir suffisamment d'informations de la part du responsable du partage des données pour être en mesure de démontrer qu'il respecte le RGPD. Par exemple, les parties peuvent convenir de mentionner à l'**appendice 3** la finalité initiale de la collecte des données. Cela peut être nécessaire afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées en vertu de l'article 6, paragraphe 4, du RGPD en cas de responsabilité conjointe du traitement. Toutes les informations nécessaires relatives aux obligations respectives des parties concernant le traitement de ces données à caractère personnel au titre du présent contrat doivent être précisées à l'**appendice 3**.

Pour en savoir plus sur le RGPD:

— Explication des notions clés du RGPD:

https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

— Guide sur la protection des données pour les petites entreprises:

https://www.edpb.europa.eu/sme-data-protection-guide/home_fr

— Lignes directrices, recommandations et bonnes pratiques du comité européen de la protection des données:

https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_fr

— Vous trouverez des orientations supplémentaires fournies par les autorités nationales chargées de la protection des données dans chaque État membre. Liste des autorités chargées de la protection des données:

https://www.edpb.europa.eu/about-edpb/about-edpb/members_fr

— Clauses contractuelles types au titre de l'article 28 du RGPD:
https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_fr

— Informations lors du transfert de données à caractère personnel en dehors de l'UE/EEE:
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en

3.3. **Inexactitude des déclarations**

3.3.1. Toute partie qui s'aperçoit qu'une des déclarations visées à la présente clause n'est pas, ou n'est plus, exacte, ou ne le sera plus dans un avenir prévisible, doit en informer l'autre partie sans retard injustifié, sauf si l'autre partie le sait ou devrait déjà le savoir.

3.3.2. Dès qu'elle a connaissance de cette situation, la partie concernée doit prendre les mesures appropriées et remédier, dans la mesure du possible, à l'inexactitude de la déclaration. Si la situation n'est pas et ne peut pas être corrigée, le présent contrat doit prendre fin au moyen d'un avis de résiliation écrit mentionnant les motifs de résiliation donnés par l'une des parties à l'autre. La résiliation a un effet immédiat. Lorsque l'inexactitude ne concerne qu'une partie des données couvertes par le présent contrat, la résiliation ne doit prendre effet que pour la partie concernée.

3.3.3. Les autres effets de la résiliation sont régis par la clause 9.3.

4. Mise à disposition des données

4.1. Caractéristiques des données

Le responsable du partage des données peut prendre différents engagements concernant les données fournies, allant de l'engagement le plus élémentaire, à savoir qu'elles seront fournies avec les métadonnées, ce qui les rendra intelligibles, à l'engagement le plus strict, à savoir qu'elles seront adaptées aux finalités envisagées par le destinataire de données et/ou qu'elles seront exhaustives et exactes. Les parties pourraient choisir parmi les options suivantes.

Il est en outre possible pour les parties d'ajouter toute exigence supplémentaire qui se justifie au regard de la situation spécifique en matière de partage des données: par exemple, lorsque les données sont partagées à des fins de recherche, l'objectif de reproductibilité de la recherche peut exiger que la fréquence et la période de conservation de chaque version actualisée de l'ensemble de données soient précisées, auquel cas ces éléments peuvent être ajoutés dans la section «Exigences de qualité spécifiques» ci-dessous.

Le responsable du partage des données met les données à la disposition du destinataire de données:

(a) à un niveau de qualité identique à celui dont bénéficie le responsable du partage des données; et

(b) avec les métadonnées pertinentes, les tables de domaine, la sémantique, les informations relatives aux licences ainsi que les autres informations nécessaires pour rendre les données intelligibles pour le destinataire de données.

[OPTION] (c) [et *(veuillez sélectionner, le cas échéant, une ou plusieurs options selon le cas*)

i) Les données sont mises à disposition dans un format complet, structuré, couramment utilisé et lisible par machine. Les parties considèrent que cette exigence est satisfaite par les spécifications suivantes concernant les données: *(veuillez préciser)*

ii) Les données sont mises à disposition conformément aux principes FAIR (faciles à trouver, accessibles, interopérables et réutilisables) décrits plus en détail à l'adresse suivante: www.go-fair.org/fair-principles: [OPTION] *[(Veuillez décrire comment respecter les critères FAIR)]*

Le respect des principes FAIR est assuré lorsque plusieurs exigences mesurables sont satisfaites. Le modèle de maturité FAIR de la Research Data Alliance (RDA) (https://publications.jrc.ec.europa.eu/repository/handle/JRC140764) propose un cadre permettant d'évaluer dans quelle mesure ces indicateurs sont remplis. Un responsable du partage des données devrait aligner ses pratiques en la matière sur un niveau de maturité adapté à ses besoins spécifiques.

Au minimum, le responsable du partage des données doit veiller à ce que les métadonnées soient disponibles et répondent à tous les indicateurs signalés comme «essentiels» par le modèle de maturité. En outre, un responsable du partage des données peut utiliser des outils, des bonnes pratiques et des lignes directrices propres au contexte, tels que ceux disponibles à l'adresse https://doi.org/10.2760/5646214, afin de simplifier et de concrétiser la mise en œuvre des principes FAIR.

iii) Les données sont adaptées au contexte suivant de traitement par le responsable du partage des données conformément aux attentes habituelles: (*veuillez ajouter une brève description*)

iv) Les données sont adaptées aux objectifs poursuivis par le destinataire de données: (*veuillez ajouter une brève description*)

v) Le responsable du partage des données met les éléments suivants à la disposition du destinataire de données: (*veuillez ajouter/supprimer/compléter les exigences de qualité spécifiques*)

— un ensemble de données exhaustif, c'est-à-dire que les données contiennent toutes les données en la possession du responsable du partage des données dans le cadre du présent contrat; et/ou

— un ensemble de données à jour, c'est-à-dire que les données correspondent aux données en possession du responsable du partage des données à la date de signature du présent contrat; et/ou

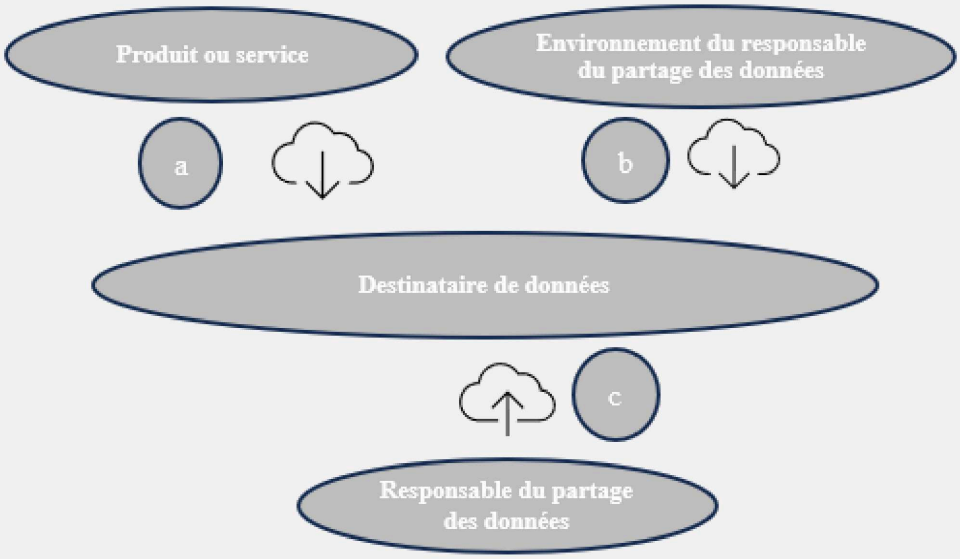
— un ensemble de données exact, c'est-à-dire que les données ont été sélectionnées par le responsable du partage des données et sont, à sa connaissance, exemptes d'erreur, correctes et fiables; et/ou

— un ensemble de données qui est conforme aux normes suivantes: *(veuillez préciser, par exemple, l'interopérabilité, l'accessibilité, la sécurité, etc.)*

— un ensemble de données disponible dans un format ouvert, c'est-à-dire un format qui n'est pas propriétaire et qui peut être utilisé par tout le monde, à savoir: *(veuillez préciser)*].

4.2. **Obligations du responsable du partage des données en ce qui concerne l'accès aux données**

Le responsable du partage des données peut mettre les données à disposition de différentes manières, en conférant ou en conservant le contrôle technique des données (sans préjudice des droits de propriété intellectuelle accordés ou conservés). Les parties peuvent, par exemple, convenir que le destinataire de données extrait les données du produit ou du service [option a)] ou de l'environnement du responsable du partage des données [option b)], ou que le responsable du partage des données transfère les données vers l'environnement du destinataire de données [option c)].



Les parties peuvent également convenir que les données ne seront pas transférées au destinataire de données, mais qu'elles seront mises à disposition pour traitement dans l'environnement du responsable du partage des données. Cela serait particulièrement pertinent dans une situation impliquant des données à caractère personnel (option d).



Lors de la mise à disposition de données dans le cadre d'une ou de plusieurs de ces options, différentes mesures de sécurité des données doivent être mises en œuvre par les parties afin de garantir la confidentialité, l'intégrité et la disponibilité initiales et continues des données. Outre les garanties juridiques relatives aux données à caractère personnel décrites à la clause 3.2 (respectivement à l'appendice 3), les mesures de sécurité (décrites plus en détail à l'appendice 4) devraient également couvrir les aspects techniques et organisationnels concernant, par exemple:

— la confidentialité des données par le contrôle d'accès et la sécurité du flux de données;

— les dispositions relatives à la conservation et à la suppression des données;

— les mesures d'intégrité des données et les mesures de suivi;

— les dispositions relatives aux violations de données.

4.2.1. Le responsable du partage des données met les données à la disposition du destinataire de données comme suit:

(a) [OPTION: récupération par le destinataire de données à partir de produits ou de services] [en permettant la récupération directement à partir des produits et/ou services suivants non hébergés par le responsable du partage des données, y compris en mettant à disposition toutes les spécifications techniques requises (par exemple, le protocole de communication) dans les conditions techniques suivantes: (*indiquer la méthode et les produits/services non hébergés par le responsable du partage des données*);]

(b) [OPTION: récupération par le destinataire de données à partir de l'environnement du responsable du partage des données] [en permettant la récupération à partir de l'environnement du responsable du partage des données, y compris en mettant à disposition toutes les spécifications techniques requises, dans les conditions techniques suivantes: [*indiquer la méthode, par exemple le téléchargement de fichiers ou l'utilisation de l'API (interface de programmation) pour interagir avec les services du responsable du partage des données*);]

(*Applicable si les options a ou b sont choisies*) [Le responsable du partage des données autorise par la présente le destinataire de données à utiliser les spécifications aux fins de l'extraction des données uniquement comme défini dans le présent contrat. À l'exception du droit susmentionné, le destinataire de données accepte et reconnaît par la présente qu'il n'a aucun autre droit, intérêt ou licence pour les spécifications.]

(c) [OPTION: transfert par le responsable du partage des données vers l'environnement du destinataire de données] [en garantissant le transfert complet des données depuis l'environnement du responsable du partage des données vers l'environnement du destinataire de données, dans les conditions techniques suivantes: *(indiquer la méthode, par exemple le transfert ponctuel ou régulier de fichiers zip au destinataire de données);*]

(d) [OPTION: accès du destinataire de données à l'environnement du responsable du partage des données] [en donnant accès aux données dans l'environnement du responsable du partage des données dans les conditions techniques suivantes: *(indiquer la méthode, par exemple connexion à une plateforme, fonctions autorisées, y compris les fonctions d'exportation, selon le cas);*]

Le responsable du partage des données accorde par la présente au destinataire de données le droit d'accéder aux données dans l'environnement décrit ci-dessus, qui n'est pas transférable et ne peut pas faire l'objet d'une sous-licence, uniquement pour l'objet et la durée spécifiés dans le présent contrat. Le responsable du partage des données se réserve le droit de suspendre l'accès à l'environnement en cas de détection d'une utilisation non conforme.

4.2.2. Aux fins de la clause 4.2.1, l'environnement du responsable du partage des données et l'environnement du destinataire de données sont réputés inclure:

(a) l'environnement de tout tiers désigné par la partie concernée pour détenir ou recevoir les données pour son compte [y compris, le cas échéant, tout environnement de traitement sécurisé au sens de l'article 2, point 20), du règlement (UE) 2022/868];

(b) toute application ou tout logiciel hébergé par la partie concernée directement ou par l'intermédiaire de fournisseurs de services.

Dans les cas où des applications d'apprentissage automatique ou d'IA doivent être mises au point, de nouvelles technologies telles que l'apprentissage fédéré et la confidentialité différentielle, qui sont décrites plus en détail dans la publication du JRC https://publications.jrc.ec.europa.eu/repository/handle/JRC141298, peuvent être utilisées pour garantir que le destinataire de données accède aux données dans le respect de la vie privée.

Dans le cas de l'apprentissage fédéré, les données sont «visitées» par l'algorithme du destinataire de données, qui est exécuté dans l'environnement de traitement sécurisé du responsable du partage des données ou d'un tiers. Cette approche empêche le destinataire de données d'avoir un accès direct aux données et de les voir. Dans le cas de la confidentialité différentielle, du bruit est ajouté aux données d'origine afin de protéger certaines caractéristiques sensibles.

4.2.3. Le responsable du partage des données met les données à la disposition du destinataire de données conformément aux délais / au calendrier suivants: (*indiquer les délais, par exemple quotidiennement, à une heure précise, fréquence, en temps réel et/ou le calendrier détaillé ou la date limite*)

[OPTION] [Si, pendant la durée du présent contrat, le responsable du partage des données entre en possession d'une version actualisée ou corrigée des données, il s'engage à mettre cette version actualisée ou corrigée à la disposition du destinataire de données sans retard injustifié après sa mise à disposition du responsable du partage des données. Lorsque les données sont actualisées et corrigées en permanence, elles sont mises à la disposition du destinataire de données (*préciser: quotidiennement / hebdomadairement / mensuellement).*]

[OPTION] Le responsable du partage des données veillera à ce que chaque nouvelle version de l'ensemble de données soit correctement indiquée et à ce que les versions précédentes restent à la disposition du destinataire pendant toute la durée du contrat et pendant une période de (*veuillez préciser*) après celui-ci.

[OPTION] Les données sont conservées par le responsable du partage des données pendant une durée de *(veuillez préciser)*, après quoi elles ne seront plus accessibles au destinataire de données.

4.2.4. Le responsable du partage des données doit fournir au destinataire de données les moyens et informations nécessaires pour accéder aux données ou les recevoir conformément au présent contrat. Cela inclut notamment:

(a) [OPTION lorsque les données ne sont pas fournies dans un format standard] [la fourniture d'un logiciel et d'une licence d'accompagnement nécessaires à l'utilisation des données pour les finalités convenues, qui ne sont pas facilement disponibles sur le marché, mais pourraient être fournis par le responsable du partage des données et/ou la conversion du format disponible en une spécification/un vocabulaire ouvert et couramment utilisé;]

(b) la fourniture d'informations facilement accessibles au responsable du partage des données concernant l'origine des données et tout droit que des tiers pourraient avoir à l'égard des données, ou les faits susceptibles de donner lieu à de tels droits.

[OPTION] Les parties conviennent par la présente que ces moyens et informations comprennent les éléments suivants: *(veuillez préciser)*.

4.3. **Obligations du destinataire de données en ce qui concerne l'accès aux données**

4.3.1. Le destinataire de données fournit au responsable du partage des données les informations techniques et les données pertinentes nécessaires au respect, par le responsable du partage des données, des exigences énoncées ci-dessus.

4.3.2. (Le cas échéant, en cas d'accès aux données dans l'environnement du responsable du partage des données) Le destinataire de données:

(a) s'engage à faire en sorte que seuls les employés qui travaillent pour ou avec le destinataire de données et dont les tâches nécessitent un accès pour l'exécution du présent contrat (principe du «besoin d'en connaître») puissent accéder à l'environnement du responsable du partage des données et que ces employés respectent les dispositions du présent contrat, ses appendices et la législation applicable;

(b) s'engage à ne pas faire ce qui suit:

i) autoriser ou permettre à tout tiers d'accéder à l'environnement du responsable du partage des données;

ii) créer des œuvres dérivées ou accéder à l'environnement du responsable du partage des données afin de mettre au point tout produit ou service concurrent ou de copier tout élément, fonction ou graphique dans l'environnement du responsable du partage des données;

iii) copier, reproduire, faire de la rétro-ingénierie, décompiler, désassembler ou tenter d'extraire tout code source, algorithme, méthode ou technique utilisé dans l'environnement du responsable du partage des données [OPTION] [sauf dans la mesure strictement requise pour les essais de compatibilité ou l'optimisation en vue de l'intégration];

iv) contourner tout mécanisme de sécurité de l'environnement du responsable du partage des données; ou

v) utiliser l'environnement technique du responsable du partage des données pour obtenir l'accès à des données autres que les données couvertes par le présent contrat ou dans des conditions différentes de celles prévues par le présent contrat.

4.4. **Mesures de sécurité**

4.4.1. Chaque partie garantit la confidentialité, l'intégrité et la disponibilité des données en mettant en œuvre les mesures de sécurité appropriées décrites à l'**appendice 4** lors de la mise à disposition des données dans le cadre des modalités d'accès visées à la clause 4.2.1.

4.4.2. Si des modifications des données ou de leur environnement sont susceptibles d'avoir une incidence sur la sécurité des données, le responsable du partage des données et le destinataire de données conviennent d'évaluer les mesures de sécurité (préciser: régulièrement/à la demande de l'autre partie/lors d'événements spéciaux), et de négocier de bonne foi toute adaptation nécessaire.

4.4.3. Chaque partie fournit, sur demande, à l'autre partie des informations détaillées sur les mesures de mise en œuvre prises conformément à la présente clause 4.4 et à l'appendice 4.

4.4.4. Chaque partie signale à l'autre partie toute atteinte à la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée des données ou l'accès non autorisé à celles-ci dans les 24 heures suivant leur découverte.

4.4.5. [OPTION] [Le responsable du partage des données se réserve le droit de procéder à des audits périodiques ou de demander des documents afin de vérifier le respect des exigences de sécurité imposées au destinataire de données.]

4.4.6. (le cas échéant) Le responsable du partage des données s'engage à ne conserver aucune autre information sur l'accès du destinataire de données aux données demandées que celles qui sont nécessaires:

(a) à l'accès aux données;

(b) (le cas échéant) à la sécurité et à la maintenance de l'infrastructure de données; et

(c) au respect des obligations légales auxquelles le responsable du partage des données est soumis.

Le responsable du partage des données informe le destinataire de données des informations qu'il conserve conformément à la législation applicable ou si le destinataire de données en fait la demande.

4.5. **Devoir de renégociation, boucles de rétroaction et modifications unilatérales**

4.5.1. Si les données sont mises à disposition conformément aux dispositions contractuelles relatives aux caractéristiques des données, aux procédures d'accès ou aux moyens et informations nécessaires pour accéder aux données et les utiliser, et s'il apparaît que les dispositions contractuelles convenues sont insuffisantes pour accéder aux données et les utiliser conformément aux termes du présent contrat, les parties s'engagent à entamer des négociations de bonne foi et à adapter les dispositions contractuelles.

4.5.2. Si le destinataire de données détecte un incident lié à la clause 2 sur les données couvertes par le contrat ou aux clauses 4.1 et 4.2 sur les caractéristiques des données et les modalités d'accès, et si le destinataire de données en informe le responsable du partage des données en lui fournissant une description détaillée de l'incident, le responsable du partage des données et le destinataire de données doivent coopérer de bonne foi pour déterminer la raison de l'incident. Si l'incident a été causé par un manquement du responsable du partage des données à ses obligations, celui-ci doit remédier à la violation sans retard injustifié. Si le responsable du partage des données ne le fait pas, cela est considéré comme une violation fondamentale et le destinataire de données peut invoquer la clause 10 du présent contrat relative aux voies de recours en cas de violation du contrat.

4.5.3. Si l'une des dispositions contractuelles convenues conformément aux clauses 4.1 et 4.2 est impossible ou excessivement onéreuse en raison d'un changement exceptionnel de circonstances survenu après la conclusion du contrat, le responsable du partage des données doit fournir au destinataire de données une description détaillée de cette situation et les parties entameront des négociations de bonne foi et adapteront les dispositions contractuelles. En particulier, chaque partie doit fournir à l'autre des informations suffisantes pour évaluer, examiner et résoudre la situation particulière. La présente clause ne porte pas atteinte au droit du destinataire de données d'invoquer des voies de recours conformément à la clause 10.

4.5.4. Le responsable du partage des données peut, de bonne foi, modifier unilatéralement les détails concernant les dispositions contractuelles relatives aux données et les modalités d'accès, si cela est objectivement justifié par la conduite normale des affaires du responsable du partage des données, par exemple par une modification technique due à une vulnérabilité immédiate en matière de sécurité dans la gamme de produits ou de services connexes proposés par le responsable du partage des données ou par une modification de l'infrastructure du responsable du partage des données. Toute modification doit répondre aux exigences fondamentales des clauses 4.1 et 4.2.

4.5.5. Le responsable du partage des données doit notifier la modification au destinataire de données au moins (*indiquer un délai raisonnable*) avant qu'elle ne prenne effet.

Un délai de notification plus court peut suffire:

(a) lorsque la modification n'a pas d'incidence négative sur l'accès aux données et leur utilisation par le destinataire de données; ou

(b) lorsqu'une telle notification serait impossible ou déraisonnable compte tenu des circonstances, par exemple lorsque des changements immédiats sont nécessaires en raison d'une vulnérabilité en matière de sécurité qui vient d'être détectée.

Lorsque le changement a une incidence négative sur l'accès aux données et leur utilisation par le destinataire de données, les parties s'engagent à coopérer pour atténuer cette incidence. Le destinataire de données peut dans tous les cas résilier le contrat (ou la partie concernée du contrat) sans qu'aucune compensation ne soit due au responsable du partage des données, nonobstant tout autre droit ou voie de recours dont le bénéficiaire de données pourrait disposer.

5. **Utilisation des données et partage avec des tiers**

5.1. **Utilisation des données**

5.1.1. Finalités autorisées (*veuillez ne sélectionner qu'une seule option*)

[OPTION RESTRICTIVE] [Le destinataire de données ne peut traiter les données que pour les finalités suivantes: *(préciser les finalités autorisées)* (ci-après les «finalités autorisées»)].

ou

[OPTION LARGE pour les données à caractère non personnel uniquement] [Le destinataire de données peut traiter les données à toute fin licite (ci-après les «finalités autorisées») [OPTION] [autre que (*préciser, par exemple, utiliser les données qu'il reçoit pour obtenir des informations sur la situation économique, les actifs et les méthodes de production du responsable du partage des données ou son utilisation des données*)].]

(*Le cas échéant, lorsque les données contiennent des données relatives au produit ou au service connexe et que le responsable du partage des données au titre du présent contrat y a eu accès conformément à l'article 4 ou 5 du règlement sur les données en sa qualité d'utilisateur ou de destinataire de données*). Dans tous les cas, le destinataire de données ne doit pas utiliser les données qu'il reçoit pour mettre au point un produit concurrençant le produit dont proviennent les données.

Lorsqu'elles conviennent des finalités autorisées, les parties devraient tenir compte de toute restriction découlant du droit applicable ou de leur engagement contractuel envers des tiers. Par exemple, si les données sont des données relatives au produit, telles que définies dans le règlement sur les données et si le responsable du partage des données est un utilisateur du produit ou un destinataire de données au sens dudit règlement, il devrait respecter l'interdiction de mettre au point un produit concurrent prévue à l'article 4, paragraphe 10, et à l'article 6, paragraphe 2, point e), du règlement sur les données. Si le responsable du partage des données est un utilisateur de ce type et s'il a convenu avec le détenteur de données de restrictions spécifiques à ses droits légaux en vertu du règlement sur les données, le présent contrat doit respecter ces restrictions.

5.1.2. Opérations autorisées sur les données (*veuillez ne sélectionner qu'une seule option*)

[OPTION RESTRICTIVE] [Le destinataire de données ne peut mettre en œuvre que les opérations suivantes sur les données: (*préciser les opérations autorisées, par exemple l'accès aux données et la copie des données pour créer des statistiques agrégées en rapport avec les finalités autorisées*) (ci-après les «opérations autorisées»).]

ou

[OPTION LARGE pour les données à caractère non personnel uniquement] [Le destinataire de données peut mettre en œuvre toute opération licite sur les données (ci-après les «opérations autorisées») [OPTION] [autre que (*préciser, par exemple, héberger ou transférer ou rendre accessibles d'une autre manière des données en dehors de l'Union européenne, ou tenter d'identifier des personnes concernées*)]

[*Le cas échéant, lorsque les données contiennent des données relatives au produit ou au service connexe et que le responsable du partage des données au titre du présent contrat y a eu accès conformément à l'article 4 ou 5 du règlement (UE) 2023/2854 en sa qualité d'utilisateur ou de destinataire de données*] Dans tous les cas, le destinataire de données ne doit pas utiliser les données qu'il reçoit d'une manière qui nuit à la sécurité du produit ou du service connexe.]

5.1.3. En outre, le destinataire de données s'engage à ne pas adopter le comportement suivant aux fins de l'obtention des données:

(a) fournir de fausses informations au responsable du partage des données;

(b) déployer des moyens trompeurs ou coercitifs;

(c) abuser des lacunes ou exploiter toute vulnérabilité de l'infrastructure technique du responsable du partage des données conçue pour protéger les données.

5.1.4. Le droit d'utiliser les données conformément à la présente clause est accordé au destinataire de données [*préciser: à perpétuité/pour la durée du contrat/pour une durée de (préciser)*].

5.1.5. (Le cas échéant, en cas de récupération des données par le destinataire de données/de transfert des données au destinataire de données et si les parties conviennent d'une limitation dans le temps de l'utilisation des données) À la fin ou à l'expiration de son droit d'utiliser les données, le destinataire de données s'engage à supprimer définitivement les données (y compris toute copie ou sauvegarde) et à veiller à ce que tout tiers auquel les données ont été communiquées efface définitivement ces données. Le destinataire de données produit, sans retard injustifié, une attestation écrite de cet effacement à la demande du responsable du partage des données.

5.2. **Partage de données avec des tiers**

5.2.1. Le destinataire de données ne partage ni ne transfère aucune donnée à un tiers, que ce soit sous une forme identifiée, anonymisée, pseudonymisée ou agrégée [OPTION] [sauf si le destinataire de données partage les données uniquement pour l'utilisation suivante des données: *(veuillez préciser)*. Le tiers ne partage ni ne transfère aucune donnée ultérieurement, [OPTION] [sauf pour l'utilisation suivante des données: (veuillez *préciser*)]].

5.2.2. (le cas échéant, lorsque les données contiennent des données relatives au produit ou au service connexe et que le responsable du partage des données au titre du présent contrat a obtenu l'accès à ces données conformément à l'article 4 ou 5 du règlement sur les données en sa qualité d'utilisateur ou de destinataire de données) Le détenteur de données ne doit pas mettre les données qu'il reçoit à la disposition d'une entreprise désignée comme contrôleur d'accès conformément à l'article 3 du règlement (UE) 2022/1925 (règlement sur les marchés numériques).

5.2.3. Lorsque le destinataire de données est autorisé à mettre des données à la disposition d'un tiers sur la base du présent contrat, il doit:

(a) [OPTION] [informer le responsable du partage des données du fait que les données seront mises à la disposition d'un tiers, préciser les données en question et indiquer au responsable du partage des données l'identité et les coordonnées du tiers;]

(b) prendre les mesures contractuelles, techniques et organisationnelles appropriées pour s'assurer que le tiers respecte les mêmes obligations que celles qui découlent du présent contrat pour le destinataire de données ou des obligations substantiellement équivalentes à celles-ci. Il s'agit en particulier des obligations suivantes du destinataire de données:

i) veiller à ce que le tiers applique au moins les mêmes mesures de sécurité et obligations que celles convenues par le destinataire de données en vertu de la clause relative aux «Mesures de sécurité»;

ii) s'assurer que le tiers utilise les données exclusivement d'une manière compatible avec la clause 5.1 relative à l'utilisation des données;

iii) [OPTION] [veiller à ce que le responsable du partage des données dispose au moins des mêmes voies de recours contre le tiers en cas d'utilisation ou de divulgation non autorisée de données que contre le destinataire de données en vertu du présent contrat; et]

iv) (*applicable si le tiers est autorisé à mettre les données à la disposition d'autres parties conformément à la clause 5.2.1*) [exiger du tiers qu'il veille à ce que tous les tiers ultérieurs qui reçoivent les données respectent les obligations énoncées dans le présent contrat].

5.2.4. Nonobstant les clauses 5.2.1 et 5.2.3, le destinataire de données peut utiliser des services de traitement, par exemple des services d'informatique en nuage (y compris une infrastructure à la demande, une plateforme à la demande et un logiciel à la demande), des services d'hébergement ou des services similaires pour utiliser les données conformément aux clauses 5.1.1 et 5.2.1, pour son propre compte et sous sa propre responsabilité. Les tiers peuvent également utiliser ces services pour utiliser les données conformément à la clause 5.2.1, pour leur propre compte et sous leur propre responsabilité.

6. **(si les données sont protégées en tant que secrets d'affaires) Secrets d'affaires**

À propos des secrets d'affaires:

Les secrets d'affaires sont des informations confidentielles qui confèrent un avantage concurrentiel à une entreprise.

Aux termes de l'article 2, point 1), de la directive (UE) 2016/943, on entend par «secret d'affaires» des informations qui répondent aux trois conditions suivantes: a) elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, elles ne sont pas généralement connues de personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles; b) elles ont une valeur commerciale parce qu'elles sont secrètes; et c) elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes.

On entend par «détenteur d'un secret d'affaires» toute personne physique ou morale qui a le contrôle d'un secret d'affaires de façon licite.

En ce qui concerne les données, le responsable du partage des données peut bénéficier de la protection des secrets d'affaires, en particulier lorsque les informations numériques couvrent:

— des informations techniques (technologie des produits, données de R&D, savoir-faire en matière de processus, technologies non brevetées, etc.);

— des informations commerciales (stratégies de marché, informations financières, etc.).

Ainsi, en ce qui concerne les informations numériques, le responsable du partage des données doit détecter un secret d'affaires potentiel. Pour de plus amples informations sur les secrets d'affaires dans le secteur numérique, voir le guide de l'OMPI sur les secrets d'affaires et l'innovation:

https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/fr/part-vii-trade-secrets-and-digital-objects.html.

Un accès limité pour les autres, le cryptage ou les accords de confidentialité seraient des méthodes permettant de garder les données secrètes, et donc d'assurer la protection des secrets d'affaires.

Comment gérer les secrets d'affaires?

Si le responsable du partage des données établit que certains secrets d'affaires font partie du partage de données dans le cadre du présent contrat, il n'est pas tenu de partager ces données, contrairement à ce qui est prévu à l'article 4, paragraphe 6, et à l'article 5, paragraphe 9, du règlement sur les données.

Si le responsable du partage des données décide de partager ces données, il peut fixer des conditions au partage de données protégées en tant que secrets d'affaires, telles que la prise de certaines mesures techniques et organisationnelles supplémentaires afin de préserver la confidentialité, et convenir de ces exigences avec le destinataire de données. Le responsable du partage des données et le destinataire de données doivent, dans l'**appendice 2** du contrat, recenser en détail les données qui sont protégées en tant que secrets d'affaires.

6.1. **Applicabilité des accords relatifs aux secrets d'affaires**

6.1.1. Les mesures de protection ainsi que les droits connexes convenus ci-dessous s'appliquent exclusivement aux données ou métadonnées figurant dans les données que le responsable du partage des données doit mettre à la disposition du destinataire de données et qui sont protégées en tant que secrets d'affaires [tels que définis à l'article 2, point 1), de la directive sur les secrets d'affaires (UE) 2016/943], détenus par le détenteur de données ou un autre détenteur de secrets d'affaires (tel que défini à l'article 2, point 2), de ladite directive)].

6.1.2. Les données protégées en tant que secrets d'affaires et l'identité du détenteur de secrets d'affaires figurent à l'**appendice 2**.

6.1.3. Les obligations énoncées aux clauses 6.2 et 6.3 restent en vigueur après toute résiliation du contrat, sauf si les parties en conviennent autrement.

6.2. **Mesures de protection à prendre par le destinataire de données**

Le destinataire de données applique les mesures de protection énoncées à l'**appendice 4** (ci-après les «mesures de protection du destinataire de données»).

Les parties devraient, à l'**appendice 4**, inclure toutes les modalités des mesures de protection. Les mesures peuvent être à la fois de nature technique (par exemple, cryptage, pare-feu, stockage fractionné, etc.) et organisationnelle (par exemple, gouvernance interne, gestion appropriée de l'identité et contrôles d'accès, participation d'un tiers de confiance).

Étant donné que les mesures doivent être proportionnées, leur contenu variera en fonction de la nature du secret d'affaires. Les mesures dépendront également de la question de savoir si i) l'accès doit être fourni à l'endroit où les données sont stockées ou si ii) les données doivent être entièrement transférées au destinataire de données. Dans le premier cas, le détenteur de données a un degré de contrôle plus élevé et peut appliquer lui-même une partie des mesures de protection, tandis que le destinataire de données peut avoir un niveau d'utilisation des données moins élevé. Dans tous les cas, les deux parties devront s'attacher à produire les effets escomptés du présent contrat.

6.3. **Mesures de protection prises par le responsable du partage des données**

6.3.1. Le responsable du partage des données peut appliquer les mesures convenues à l'appendice 4 afin de préserver la confidentialité des données protégées en tant que secrets d'affaires (ci-après les «mesures de protection du responsable du partage des données»).

6.3.2. Le responsable du partage des données peut également ajouter unilatéralement des mesures de protection techniques et organisationnelles appropriées, si elles n'ont pas d'incidence négative sur l'accès aux données et leur utilisation par le destinataire de données dans le cadre du présent contrat.

6.3.3. Le destinataire de données s'engage à ne pas modifier ni supprimer les mesures de protection du responsable du partage des données ni les mesures prises conformément à la clause 6.3.2, sauf si les parties en conviennent autrement.

6.4. **Détenteurs tiers de secrets d'affaires définis**

6.4.1. Le responsable du partage des données déclare au destinataire de données qu'il dispose de tous les droits pertinents de la part de tout détenteur tiers de secrets d'affaires pour conclure le présent contrat en ce qui concerne les données protégées en tant que secrets d'affaires.

6.4.2. Les mesures de protection du destinataire de données et les mesures de protection du responsable du partage des données tiennent compte des engagements contractuels du responsable du partage des données envers le détenteur de données initial. Si les engagements du responsable du partage des données envers le détenteur de données initial devaient évoluer, le destinataire de données s'engage à se conformer à toute nouvelle mesure convenue entre le responsable du partage des données et le détenteur de données initial.

7. **Droits de propriété intellectuelle**

On entend par «droits de propriété intellectuelle» le droit d'auteur (y compris les droits sur les logiciels informatiques et autres droits voisins), les droits sur les dessins ou modèles (y compris les dessins ou modèles enregistrés et les droits sur ces dessins ou modèles), les marques, les marques de service, les noms commerciaux ou les appellations commerciales, les marques de commerce, les noms de domaine et les URL, les droits sur les secrets d'affaires, le savoir-faire et les informations confidentielles et non divulguées (telles que les inventions, brevetables ou non), les droits sur les logos et les brevets, les droits sui generis liés à la base de données et tout droit similaire reconnu par le droit applicable.

Les données relevant du champ d'application du présent contrat et l'utilisation autorisée par le détenteur de données doivent être régies par le présent contrat afin de protéger les droits de propriété intellectuelle du responsable du partage des données, des tiers ou les nouveaux droits de propriété intellectuelle émergents du destinataire de données. En ce qui concerne le partage de données, les principaux droits de propriété intellectuelle qui doivent être pris en compte lors de la conclusion d'un contrat sont le droit sui generis prévu par la directive sur les bases de données et le droit d'auteur.

Droit sui generis:

conformément à l'article 43 du règlement sur les données, «[l]*e droit sui generis prévu par l'article 7 de la directive 96/9/CE ne s'applique pas lorsque des données sont obtenues à partir d'un produit connecté ou d'un service connexe relevant du champ d'application du présent règlement ou générées par un tel produit ou service, en particulier en ce qui concerne ses articles 4 et 5*». Toutefois, «[c]*ela ne porte pas atteinte à la potentielle application du droit sui generis prévu par l'article 7 de la directive 96/9/CE aux bases de données contenant des données ne relevant pas du champ d'application du présent règlement, à condition que les conditions de la protection en application du paragraphe 1 dudit article soient remplies*» (considérant 112).

Le droit sui generis de la directive sur les bases de données protège le fabricant de la base de données, étant donné qu'il s'agit de la personne qui a réalisé des investissements substantiels du point de vue qualitatif et quantitatif pour l'acquisition, la vérification ou la présentation de son contenu. Le fabricant peut interdire l'extraction et la réutilisation de la totalité ou d'une partie substantielle, évaluée de façon qualitative et/ou quantitative, du contenu de cette base de données. Les œuvres individuelles ou les éléments de données de la base de données, s'ils sont originaux, peuvent être protégés séparément par le droit d'auteur, bien que cette protection soit distincte de celle prévue par la directive sur les bases de données.

Droit d'auteur:

le droit d'auteur est une forme de protection de la propriété intellectuelle qu'assure le droit aux créateurs d'œuvres originales d'auteur. Cette protection couvre un large éventail d'œuvres, y compris éventuellement l'architecture d'une base de données. N.B.: la protection du droit d'auteur n'a pas été totalement harmonisée et peut donc varier d'un État membre à l'autre.

Brevets:

le partage et l'utilisation des données peuvent donner lieu à des inventions car elles inspirent de nouvelles idées, optimisent les technologies existantes et accélèrent la mise au point de solutions innovantes. Les inventions à caractère technique qui sont nouvelles et impliquent une activité inventive pouvant être utilisées dans une industrie sont brevetables. Les parties devraient donc réglementer les inventions et déterminer qui est habilité à utiliser ces résultats brevetables.

7.1. **Droits de propriété intellectuelle antérieurs**

7.1.1. Sauf disposition contraire expresse du contrat, chaque partie conserve la propriété de tout droit de propriété intellectuelle détenu par les parties ou concédé sous licence à celles-ci par des tiers, avant l'exécution du contrat ou en toute indépendance par rapport à celle-ci, y compris toute modification et/ou amélioration de celui-ci (ci-après les «éléments préexistants»). Le contrat ne peut en aucun cas être considéré comme accordant à l'une ou l'autre des parties un droit de propriété intellectuelle sur les éléments préexistants de l'autre partie, sauf disposition contraire expresse du contrat.

7.1.2. (*applicable si les données sont couvertes par des droits de propriété intellectuelle*) Sous réserve du paiement de la rémunération (par exemple, les redevances de licence) au titre du présent contrat, le responsable du partage des données accorde par la présente au destinataire de données, pour la durée du contrat, une licence couvrant les caractéristiques suivantes: *(veuillez préciser, par exemple mondiale, non exclusive, non transférable* y compris le droit (*veuillez préciser, par exemple, d'utiliser, de copier, de modifier, d'améliorer, de conserver*) les données qui seraient couvertes par un droit de propriété intellectuelle uniquement dans la mesure nécessaire au titre du contrat. Une sous-licence aux sous-traitants du destinataire de données n'est autorisée qu'aux fins de la sous-traitance et dans la mesure où elle n'est pas incompatible avec les dispositions du présent contrat.

7.2. **Droits de propriété intellectuelle sur les résultats**

7.2.1. Si l'utilisation des données par le destinataire de données dans le cadre du présent contrat génère des produits tangibles susceptibles d'être protégés par des droits de propriété intellectuelle (ci-après les «résultats»), il est convenu que:

7.2.2. [OPTION 1] [le destinataire de données devient le seul propriétaire de tous les droits de propriété intellectuelle relatifs aux résultats; seul le destinataire de données peut, à sa discrétion, s'enregistrer ou obtenir un tel titre de propriété intellectuelle;

7.2.3. [OPTION 2] [les parties seront conjointement et à parts égales titulaires des droits de propriété intellectuelle sur les résultats et concluront un contrat distinct décrivant les modalités d'exercice de ces droits;

7.2.4. [OPTION 3] [le destinataire de données accepte de céder, dans la mesure nécessaire, au responsable du partage des données la pleine propriété juridique et effective des résultats, ainsi que tous les droits de propriété intellectuelle y afférents, à titre exclusif, moyennant une contrepartie à convenir entre les parties, dans le monde entier, pour toute la durée des droits de propriété intellectuelle.

7.2.5. En outre, les parties conviennent que d'autres licences sur les résultats seront accordées comme suit:

[OPTION] [(*préciser la partie qui ne détient pas les droits de propriété intellectuelle (DPI) sur les résultats*) accorde par la présente à (*préciser le titulaire des DPI sur les résultats*), pour la durée de protection des droits de propriété intellectuelle, une licence mondiale, non exclusive, non transférable et entièrement libérée permettant d'utiliser, de copier, de modifier, d'améliorer et de conserver ses éléments préexistants uniquement dans la mesure nécessaire à l'exercice de ses droits sur les résultats en vertu de la présente clause.]

[OPTION] [(*préciser le titulaire des DPI sur les résultats*) accorde par la présente à (*préciser la partie qui ne détient pas les DPI sur les résultats*), pour la durée de protection des droits de propriété intellectuelle, une licence mondiale, non exclusive et non transférable et entièrement libérée permettant d'utiliser, de copier, de modifier, d'améliorer et de conserver les résultats aux seules fins suivantes: (*à compléter le cas échéant*).]

8. **Rémunération pour la fourniture de l'accès aux données**

Les parties peuvent, dans le contrat lui-même ou dans un appendice distinct, déterminer les modalités de la rémunération, y compris les coûts de mise en place de l'API (utilisée pour le partage des données) ou d'autres coûts liés à la facilitation du partage des données, y compris les redevances ou droits de licence, selon le cas. Les parties devraient se mettre d'accord, au minimum, sur les points suivants: le montant de la rémunération due et la devise concernée; la date d'échéance de la rémunération; et les procédures de paiement.

Elles peuvent convenir d'une rémunération supplémentaire, le cas échéant, pour des services supplémentaires, qui feront l'objet d'une redevance supplémentaire.

Les parties conviennent que le destinataire de données rémunérera le responsable du partage des données comme suit: *(à compléter le cas échéant)*

Les parties devraient se mettre d'accord, au minimum, sur les points suivants: le montant de la rémunération due et la devise concernée; la date d'échéance du paiement; et les procédures de paiement.

9. **Date d'application, durée du contrat et résiliation**

9.1. **Date d'application et durée**

9.1.1. Le présent contrat [OPTION 1] [prend effet immédiatement] [OPTION 2] [prend effet à compter du *(préciser la date)*].

9.1.2. [OPTION] [Le présent contrat est conclu pour [OPTION 1] [une durée indéterminée] [OPTION 2] [une durée déterminée de (*préciser*)], sous réserve de tout motif d'expiration ou de résiliation en vertu du présent contrat.]

9.1.3. [OPTION] [Le responsable du partage des données doit commencer à mettre les données à la disposition du destinataire de données [OPTION 1] sans retard injustifié après l'entrée en vigueur du contrat. [OPTION 2] le (*indiquer la date et, le cas échéant, donner de plus amples informations sur le calendrier*).]

Si la demande porte sur une fourniture ponctuelle de données, il suffit de convenir de la date d'application dans la clause 9.1.1. Si la demande porte sur une fourniture continue de données, les parties devront convenir de la durée du contrat et choisir la première ou la deuxième option dans la clause 9.1.2.

9.2. **Résiliation pour raisons de commodité**

9.2.1. Le destinataire de données peut résilier le contrat à tout moment au cours de la période contractuelle en donnant au responsable du partage des données un préavis de *(indiquer la durée)*.

9.2.2. [OPTION] Lorsque le destinataire de données résilie le contrat en vertu de la clause 9.3.1 avant (*indiquer la date ou la durée minimale du contrat*), il doit indemniser le responsable du partage des données pour les coûts supportés par celui-ci pour la mise à disposition des données, y compris, le cas échéant, pour la fourniture de tout soutien supplémentaire, comme suit: *(veuillez préciser)*

Dans certains cas, le responsable du partage des données engage des dépenses lorsqu'il met les données à la disposition du destinataire de données, par exemple en adaptant son infrastructure numérique, en étant convaincu que ces dépenses seront amorties au fil du temps.

Dans ce cas, le responsable du partage des données peut souhaiter s'assurer qu'il reçoit une compensation de la part du destinataire de données.

9.3. **Effets de l'expiration ou de la résiliation**

9.3.1. L'expiration de la période contractuelle ou la résiliation du présent contrat libère les deux parties de leur obligation d'exécuter et de recevoir une exécution dans l'avenir, mais n'a pas d'incidence sur les droits et obligations acquis jusqu'au moment de la résiliation.

L'expiration ou la résiliation n'a pas d'incidence sur les dispositions du présent contrat relatives au règlement des litiges en vertu de la clause 11.6 ou toute autre disposition qui restent applicables même après la fin du contrat.

9.3.2. [OPTION 1] [Le responsable du partage des données doit prendre des mesures de soutien à la sortie appropriées, comme le destinataire de données de données peut raisonnablement s'y attendre.] [OPTION 2] [Le responsable du partage des données doit prendre les mesures de soutien à la sortie suivantes: (veuillez préciser).]

Les parties peuvent examiner si le destinataire de données exige des mesures de soutien à la sortie.

Cela sera pertinent, par exemple, si le destinataire de données était autorisé à extraire des données d'un support contrôlé par le responsable du partage des données, mais qu'il n'avait pas encore extrait les données car il ne s'attendait pas à ce que le contrat soit résilié.

10. **Voies de recours en cas de violation du contrat**

10.1. **Cas d'inexécution**

10.1.1. L'inexécution d'une obligation est essentielle si:

(a) elle prive substantiellement l'autre partie de ce qu'elle était en droit d'attendre du présent contrat, à moins que la partie défaillante n'ait pas prévu et n'ait pas pu raisonnablement prévoir ce résultat; ou

(b) il ressort clairement des circonstances que l'on ne peut pas compter dans l'avenir sur une exécution par la partie défaillante.

10.1.2. Une partie est exonérée des conséquences de l'inexécution lorsque celle-ci est due à un empêchement qui lui échappe et si l'on ne pouvait raisonnablement attendre de cette partie qu'elle le prenne en considération au moment de la conclusion du présent contrat, ou qu'elle le prévienne ou le surmonte ou qu'elle en prévienne ou en surmonte les conséquences.

Lorsque l'empêchement exonératoire n'est que temporaire, l'exonération d'inexécution de la partie vaut pour la durée de l'empêchement. Cependant, si le retard équivaut à une inexécution essentielle, l'autre partie peut le traiter comme telle.

La partie défaillante doit faire en sorte que l'autre partie reçoive, sans retard excessif, notification de l'empêchement et de ses effets sur sa capacité de s'exécuter à partir du moment où la partie défaillante a eu, ou a pu avoir raisonnablement connaissance de ces circonstances. L'autre partie a droit à des dommages et intérêts en réparation du préjudice économique résultant de la non-réception de cette notification.

10.2. **Voies de recours en cas de violation**

10.2.1. En cas d'inexécution par une partie, l'autre partie dispose des voies de recours énumérées dans les clauses suivantes, sans préjudice des voies de recours prévues par le droit applicable.

10.2.2. Les moyens d'action qui ne sont pas incompatibles peuvent être cumulés.

10.2.3. Une partie ne peut recourir à aucun moyen d'action dans la mesure où elle a provoqué l'inexécution de l'autre partie, par exemple lorsqu'une défaillance dans sa propre infrastructure de données n'a pas permis à l'autre partie de s'acquitter dûment de ses obligations. Une partie ne peut pas non plus introduire une demande de dommages et intérêts dans la mesure où elle aurait pu réduire son préjudice en prenant des mesures raisonnables.

10.2.4. La partie lésée peut:

(a) résilier le présent contrat avec effet immédiat et sans pénalité, en adressant une notification à l'autre partie, si:

i) l'inexécution de l'autre partie est une inexécution essentielle; ou

ii) dans le cas d'une inexécution qui n'est pas essentielle, la partie lésée a, par notification, exigé qu'il soit remédié à l'inexécution sans retard injustifié et l'autre partie ne s'est pas exécutée.

(b) demander des dommages et intérêts pour le préjudice économique qui lui a été causé par l'inexécution de l'autre partie et qui ne bénéficie pas d'une exonération en vertu de la clause 10.1.2; la partie défaillante n'est responsable que des dommages qu'elle avait prévus ou qu'elle aurait raisonnablement dû prévoir au moment de la conclusion du présent contrat comme pouvant résulter de son inexécution, sauf si celle-ci était intentionnelle ou résultait d'une négligence grave;

(c) demander à la partie défaillante de se conformer, sans retard injustifié, aux obligations qui lui incombent en vertu du présent contrat, à moins que cela ne soit illicite ou impossible ou qu'une exécution spécifique n'entraîne pour la partie défaillante des coûts disproportionnés par rapport au bénéfice que l'autre partie en retirerait.

10.2.5. [OPTION] [Lorsqu'une partie n'exécute pas les obligations qui lui incombent en vertu du présent contrat, elle s'acquitte, en tout état de cause, des pénalités exposées en détail à l'appendice 5, que les parties considèrent comme des dommages et intérêts au sens de la clause 10.2.4, point b). La partie défaillante a le droit de demander que la pénalité soit réduite à un montant raisonnable lorsqu'elle peut prouver que celle-ci est manifestement excessive par rapport au préjudice résultant de l'inexécution.]

11. **Dispositions générales**

11.1. **Confidentialité**

11.1.1. Les informations suivantes doivent être considérées comme confidentielles:

(a) les informations relatives aux secrets d'affaires, à la situation financière ou à tout autre aspect des activités d'une partie, sauf si l'autre partie a rendu ces informations publiques;

(b) les informations exposant la base de calcul de la compensation raisonnable;

(c) les informations relatives à tout tiers, sauf s'il a déjà rendu ces informations publiques.

11.1.2. Les deux parties conviennent de prendre toutes les mesures raisonnables pour conserver en toute sécurité et en toute confidentialité les informations visées à la clause 11.1.1 et de ne pas les divulguer ou les mettre à la disposition d'un tiers, sauf dans les cas suivants:

(a) si l'une des parties a l'obligation légale de divulguer ou de mettre à disposition les informations pertinentes; ou

(b) s'il est nécessaire que l'une des parties divulgue ou mette à disposition les informations pertinentes pour s'acquitter des obligations qui lui incombent en vertu du présent contrat; ou

(c) si l'une des parties a obtenu le consentement préalable de l'autre partie ou de la partie qui a fourni les informations confidentielles ou qui est concernée par leur divulgation.

11.1.3. Ces obligations de confidentialité restent applicables après la résiliation du contrat pendant une durée de (*préciser la durée*).

11.1.4. Ces obligations de confidentialité ne suppriment aucune des obligations plus strictes au titre i) du règlement (UE) 2016/679 (RGPD), ii) des dispositions mettant en œuvre la directive 2002/58/CE ou la directive (UE) 2016/943, ou iii) de toute autre disposition du droit de l'Union ou du droit d'un État membre.

11.2. **Moyens de communication**

Toute notification ou autre communication requise ou autorisée par le présent contrat doit être effectuée par écrit et peut être remise en main propre, envoyée par courrier prépayé ou transmise par voie électronique, y compris par courrier électronique, à condition que l'expéditeur conserve la preuve de l'envoi aux adresses énumérées ci-dessous:

Partie	Personne de contact	Adresse électronique	Numéro de téléphone	Adresse
Utilisateur	[Nom]/[Fonction]	[Adresse électronique]	[Numéro de téléphone]	[Adresse]
Destinataire de données	[Nom]/[Fonction]	[Adresse électronique]	[Numéro de téléphone]	[Adresse]

Toute notification ou communication de ce type est réputée reçue:

(a) en cas de remise en main propre, à la date de livraison;

(b) en cas d'envoi par courrier prépayé, le troisième jour ouvrable suivant l'envoi;

(c) en cas d'envoi par voie électronique, à la date de transmission, à condition qu'aucun message d'erreur indiquant un défaut de transmission n'ait été reçu par l'expéditeur.

11.3. **Contrat indivisible, modifications et caractère détachable**

11.3.1. Le présent contrat (ainsi que ses appendices mentionnés dans le contrat) constitue le contrat indivisible conclu entre les parties concernant l'objet du présent contrat et annule et remplace tous les accords ou contrats et protocoles antérieurs, oraux ou écrits, entre les parties concernant l'objet du présent contrat.

11.3.2. Toute modification du présent contrat ne sera valable que si les parties en conviennent par écrit, y compris sous une forme électronique.

11.3.3. Si une disposition du présent contrat est déclarée nulle, invalide, annulable ou inapplicable pour quelque raison que ce soit, et si cette disposition est détachable des autres clauses du contrat, ces autres dispositions n'en seront pas affectées et resteront valables et applicables, sauf si la disposition n'est pas détachable des autres dispositions du présent contrat. Toute lacune ou ambiguïté qui en résulterait dans le présent contrat sera traitée conformément à la clause 11.5.

11.4. **Droit applicable**

Le présent contrat est régi par le droit de (*préciser l'État membre*).

11.5. **Interprétation**

11.5.1. Les dispositions du présent contrat doivent être interprétées dans le sens de leur conformité avec le droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union, ainsi qu'avec toute disposition du droit national applicable qui est compatible avec le droit de l'Union et auquel il ne peut être dérogé par accord.

11.5.2. Si une lacune ou une ambiguïté dans le présent contrat ne peut être résolue de la manière visée à la clause 11.5.1, le présent contrat doit être interprété à la lumière des règles d'interprétation prévues par le droit applicable (voir clause 11.4).

11.6. **Règlement des litiges**

11.6.1. Les parties conviennent de tout mettre en œuvre pour régler les litiges à l'amiable et, avant de porter une affaire devant une juridiction, de soumettre leur litige à (insérer le nom et les coordonnées d'un organisme particulier de règlement des litiges].

11.6.2. [OPTION] [Les tribunaux de (*préciser l'État membre*) seront seuls compétents pour connaître de l'affaire concernant le présent contrat.]

Appendice 1 (contient une description des données)

[à rédiger par les parties]

Appendice 2 (contient de plus amples informations concernant les données couvertes par un régime nécessitant des mesures spécifiques)

[à rédiger par les parties]

Appendice 3 (contient des informations détaillées sur les données à caractère personnel et les obligations respectives des parties)

[à rédiger par les parties]

Appendice 4 (contient les mesures de sécurité applicables au partage des données)

[à rédiger par les parties]

[OPTION] Appendice 5 (contient des précisions sur les sanctions)

[à rédiger par les parties]

ANNEXE VI

CLAUSES CONTRACTUELLES STANDARDS

relatives au changement de fournisseur et à la sortie

Les principaux objectifs du règlement (UE) 2023/2854 (ci-après le «règlement sur les données») sur le changement de fournisseur de services en nuage consistent notamment à permettre aux clients de services de traitement de données (informatique en nuage et services en périphérie) de: i) passer d'un fournisseur à un autre fournisseur proposant le même type de service, ii) se tourner vers une infrastructure TIC sur site, ou iii) recourir simultanément à plusieurs services fournis par différents fournisseurs. Par conséquent, le règlement sur les données précise les droits et obligations des fournisseurs et des clients dans le cadre de ce processus. Dans ce contexte, les clients devraient également évaluer leurs objectifs concernant le changement de fournisseur et, en particulier, leurs besoins spécifiques, les dépenses supplémentaires ou le calendrier. Tant le fournisseur d'origine que le client et le fournisseur de destination doivent coopérer de bonne foi pour rendre le processus de changement de fournisseur effectif, permettre le transfert en temps utile des données et maintenir la continuité des services de traitement de données (article 27 du règlement sur les données).

Les présentes CCS traduisent en clauses contractuelles les nouveaux droits et obligations introduits par le règlement sur les données en ce qui concerne le processus de changement de fournisseur et de sortie. Le règlement sur les données impose aux fournisseurs de fournir aux clients un contrat écrit précisant les modalités du processus de changement de fournisseur. Le contrat doit également préciser les délais applicables aux fins du changement de fournisseur (période transitoire maximale de 30 jours) ainsi que les coûts éventuels engagés [y compris les pénalités liées à la résiliation anticipée, les frais de service standards (article 29, paragraphe 4, du règlement sur les données) et les frais de transfert de données]. Il existe également des obligations relatives au processus de changement de fournisseur lui-même qu'il convient de préciser dans le contrat: la garantie d'une assistance raisonnable au client (et à tout tiers autorisé par le client), le maintien de la continuité des activités et l'assurance d'un niveau élevé de sécurité tout au long du processus de changement de fournisseur.

Frais de changement de fournisseur

Conformément à l'article 29 du règlement sur les données, un fournisseur peut continuer d'appliquer des frais de changement de fournisseur jusqu'au 12 janvier 2027, mais ceux-ci ne peuvent dépasser les coûts supportés par le fournisseur qui sont directement liés au processus de changement de fournisseur. À compter du 12 janvier 2027, le fournisseur n'est pas autorisé à imposer des frais de changement de fournisseur. Les frais de changement de fournisseur comprennent les frais de transfert de données ainsi que d'autres coûts liés aux actions que le fournisseur est tenu de réaliser dans le cadre du processus de changement de fournisseur. Il s'agit notamment des frais liés à l'utilisation d'outils de changement de fournisseur ou d'outils de test automatisés, lorsque ceux-ci sont utilisés par le fournisseur pour se conformer aux obligations qui lui incombent en vertu du règlement sur les données.

Lorsqu'un service de traitement de données est utilisé parallèlement à un autre service de traitement de données, les fournisseurs peuvent — même après le 12 janvier 2027 — continuer à répercuter sur le client les coûts supportés pour le transfert des données (article 34 du règlement sur les données).

Si le règlement sur les données définit les «frais de changement de fournisseur» comme des frais «*imposés par un fournisseur de services de traitement de données à un client pour les actions requises par le présent règlement pour changer de fournisseur en passant au système d'un fournisseur différent ou à une infrastructure TIC sur site* [...]», l'article 25, paragraphe 2, point a) i), du règlement sur les données précise également que le fournisseur doit «*fourni[r] une assistance raisonnable au client et aux tiers autorisés par le client dans le cadre du processus de changement de fournisseur*». Tous les frais liés à la fourniture de cette «assistance raisonnable» devraient être supprimés au fil du temps, comme indiqué à l'article 29.

Le règlement sur les données précise les cas dans lesquels une approche standard n'est pas possible:

— l'article 29, paragraphe 5, dispose que «*[l]e cas échéant, les fournisseurs de services de traitement de données communiquent à un client des informations sur les services de traitement de données pour lesquels un changement de fournisseur est très complexe ou coûteux ou pour lesquels il est impossible de changer de fournisseur sans qu'il y ait une interférence significative portant sur les données, les actifs numériques ou l'architecture des services*»,

— tandis que l'article 29, paragraphe 6, dispose que «*[l]e cas échéant, les fournisseurs ... mettent les informations ... à la disposition des clients publiquement*».

D'autres clauses contractuelles standards recommandées par la Commission figurent en annexe et portent sur des sujets spécifiques autres que le changement de fournisseur et la sortie. Les parties sont encouragées à envisager également l'utilisation de ces autres clauses, étant donné qu'elles ont été élaborées de façon à être cohérentes et à se renforcer mutuellement.

Régime spécifique

Il convient de noter que l'article 31 du règlement sur les données prévoit des exceptions à certaines obligations liées aux CCS relatives au changement de fournisseur et à la sortie. Par exemple, un régime spécifique s'applique au changement de services de traitement de données lorsque:

(a) la majorité des caractéristiques principales du service de traitement de données ont été conçues sur mesure pour les besoins spécifiques d'un client particulier OU que tous les composants ont été développés pour les besoins d'un client particulier; que

(b) ces services de traitement de données ne sont pas proposés à grande échelle sur le plan commercial par l'intermédiaire du catalogue de services du fournisseur; et que
(c) le fournisseur a dûment informé le client que les obligations en matière de changement de fournisseur ne s'appliquent pas à ce service particulier.

En fonction de l'exception considérée, certaines obligations légales peuvent ne pas s'appliquer. Toutefois, il appartient au client et au fournisseur de convenir de les inclure ou non dans leur accord. Bien que les présentes clauses contractuelles standards n'aient pas été rédigées pour couvrir de telles situations, elles peuvent néanmoins servir de base aux parties à un accord/contrat en ce qui concerne ce type de services.

Le fournisseur devrait informer les clients potentiels, bien avant la conclusion d'un accord, des services particuliers auxquels s'applique le régime spécifique prévu à l'article 31 du règlement sur les données.

Rien n'empêche le fournisseur de déployer à terme ces services à grande échelle, auquel cas ce fournisseur devrait se conformer à toutes les obligations en matière de changement de fournisseur prévues par le règlement sur les données.

Approches en matière de changement de fournisseur

Un nombre croissant de fournisseurs proposent des outils de changement de fournisseur en libre-service tant pour l'entrée des données, lorsque les clients commencent à utiliser un service, que pour le transfert des données, lorsque les clients cessent d'utiliser un service et se tournent soit vers un système sur site, soit vers un nouveau fournisseur (de destination). Dans le cas de certains services de traitement de données, il se peut que de tels outils ne soient pas disponibles ou qu'ils ne permettent pas un changement de fournisseur complet.

Deux approches en matière de planification et d'exécution du processus de changement de fournisseur sont prévues dans les présentes CCS:
(a) le changement de fournisseur fondé sur le plan de changement et de sortie (option A); et
(b) le changement de fournisseur à l'aide d'outils automatisés (option B).

Ces options peuvent être combinées. Par exemple, à l'**appendice 1** intitulé «Plan de changement de fournisseur et de sortie», les parties peuvent également envisager l'utilisation d'outils automatisés qui peuvent s'appliquer à certains types de services ou à certaines données.

Dans le cadre de ces deux approches, les fournisseurs sont tenus de supprimer les obstacles au changement effectif de fournisseur, ainsi que le prévoit le règlement (UE) 2023/2854, en vertu duquel les fournisseurs doivent «*fourni[r] au client: des informations sur les procédures disponibles pour le changement de fournisseur et le portage vers le service de traitement de données, y compris des informations sur les méthodes et formats de changement de fournisseur et de portage disponibles, ainsi que sur les restrictions et les limitations techniques connues du fournisseur de services de traitement de données*» [article 26, point a)]; et selon lequel «*[l]e fournisseur d'origine de services de traitement de données facilite le processus de changement de fournisseur en fournissant des capacités, les informations adéquates, de la documentation, une assistance technique et, le cas échéant, les outils nécessaires*» (article 30).

Il est également important de noter que le fournisseur n'est pas censé partager ou détailler des données spécifiques au fonctionnement interne de son service de traitement de données lorsqu'il existe un risque de violation des secrets d'affaires du fournisseur. Conformément aux obligations contractuelles énoncées à l'article 25, paragraphe 2, point f), le fournisseur est uniquement tenu de fournir une spécification exhaustive des catégories de ces données.

Les CCS s'appliquent-elles à tous les modèles de services en nuage (par exemple, aux contrats IaaS, PaaS ou SaaS)?

Les présentes CCS s'appliquent à tous les types de modèles de contrats de services en nuage, lorsque le service en nuage en question répond à la définition d'un service de traitement de données énoncée à l'article 2, point 8). Selon ledit article, on entend par «service de traitement de données» «un service numérique qui est fourni à un client et qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services». Les dispositions du règlement sur les données s'appliquent donc aux types de services qui présentent les caractéristiques énumérées dans la définition des services de traitement de données:

— ils permettent l'accès à des ressources informatiques, telles que des réseaux, des serveurs, des dispositifs de stockage, des applications et des services;

— ils permettent un accès par réseau à la demande, ce qui signifie qu'un client peut mobiliser unilatéralement les ressources informatiques disponibles sur le réseau et au moyen de mécanismes standards, par exemple par l'intermédiaire de téléphones portables, d'ordinateurs portables ou de postes de travail;

— ils peuvent être rapidement mobilisés et libérés avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services, de sorte que la mobilisation unilatérale peut être effectuée sans intervention significative du fournisseur de services et peut être déployée rapidement, ce qui permet aux organisations de commencer à utiliser les ressources presque immédiatement;

— ils sont variables et peuvent être rapidement mobilisés, ce qui signifie que les solutions peuvent être facilement modulées pour répondre à l'évolution des besoins et que les utilisateurs peuvent augmenter ou réduire la demande en fonction de leurs besoins.

Un fournisseur dont l'offre de services présente ces caractéristiques doit se conformer aux dispositions du règlement sur les données afin de permettre le passage d'un service de traitement de données à un autre. Il s'agit, par exemple, de mettre les contrats de services en conformité avec l'article 25, de réduire et de supprimer les frais de changement de fournisseur et de transfert de données conformément à l'article 29, et de se conformer aux aspects techniques du changement de fournisseur définis à l'article 30. Toutefois, les exigences imposées aux services de traitement de données au titre du chapitre VI du règlement sur les données ne s'appliquent pas toutes aux SaaS. En particulier, la notion d'équivalence fonctionnelle énoncée à l'article 30, paragraphe 1, ne s'applique qu'aux fournisseurs d'IaaS, tandis que l'article 30, paragraphes 2 et 3, s'applique aux fournisseurs de PaaS et de SaaS. Ces deux dernières dispositions imposent aux fournisseurs de PaaS et de SaaS de mettre à disposition des interfaces ouvertes et de se conformer aux spécifications d'interopérabilité ouvertes et aux normes harmonisées publiées dans un répertoire de l'UE.

L'article 30 du règlement sur les données établit une distinction entre:

1. les IaaS, définis comme des «*services de traitement de données qui concernent des ressources informatiques modulables et variables limitées à des éléments d'infrastructure tels que les serveurs, les réseaux et les ressources virtuelles nécessaires à l'exploitation de l'infrastructure, sans donner accès aux services, logiciels et applications d'exploitation qui sont stockés, autrement traités ou déployés sur ces éléments d'infrastructure*»;

et

2. d'autres types de services en nuage.

En outre, le considérant 81 du règlement sur les données précise que la notion générique de «services de traitement de données» couvre un nombre important de services ayant un très large éventail de finalités, de fonctionnalités et de configurations techniques différentes et qu'ils sont généralement compris comme relevant d'un ou de plusieurs des trois modèles de fourniture de services de traitement de données que sont les IaaS, les PaaS et les SaaS.

Capacités des parties

L'article 24 du règlement sur les données précise que «*[l]es responsabilités des fournisseurs de services de traitement de données définies aux articles 23, 25, 29, 30 et 34 ne s'appliquent qu'aux services, contrats ou pratiques commerciales du fournisseur d'origine de services de traitement de données*».

Entre autres éléments, la connaissance de la structure des données et de la relation entre les données est requise pour définir la séquence des opérations d'exportation des données exportables. La liste ci-dessous fournit donc des orientations générales aux parties afin de les aider à comprendre les capacités respectives qui sous-tendent les différents éléments du processus de changement de fournisseur. Toutefois, la liste n'est qu'indicative et il peut y avoir des nuances importantes entre les catégories de modèles de services ci-dessous et au sein de celles-ci, en fonction du service de traitement de données concerné. Les parties devraient accorder une attention particulière à ces différences.

Infrastructure à la demande (IaaS)

— Le client connaît la structure de la base de données qu'il a définie. Le fournisseur d'IaaS ne connaît pas la structure de la base de données. Le fournisseur d'IaaS est en mesure de fournir des précisions sur les méthodes de portage et, le cas échéant, les outils nécessaires.

— Le client est en mesure de définir la séquence des opérations, une fenêtre temporelle ainsi que les ressources informatiques requises.

— Le fournisseur est en mesure de confirmer la disponibilité des ressources informatiques requises pendant la fenêtre temporelle définie.

— Le client est en mesure de déclencher le changement de fournisseur au moment convenu.

— Le client est responsable de l'importation et de la mise en œuvre des données dans l'environnement de destination.

Plateforme à la demande (PaaS)

— Le client connaît la structure de la base de données qu'il a définie.

— Le fournisseur de PaaS connaît également les caractéristiques de la base de données parce que le client lui a demandé de fournir des services tels que l'attribution d'espaces, l'optimisation, la réorganisation et les sauvegardes.

— Le fournisseur de PaaS possède une expérience pratique des procédures applicables aux opérations telles que les sauvegardes. Il connaît les ressources qui sont nécessaires et le temps qui s'est écoulé. Le fournisseur de PaaS est en mesure de fournir des précisions sur les méthodes de portage et, le cas échéant, les outils et informations nécessaires concernant le calendrier et les ressources informatiques requises.

— Le client est en mesure de définir la séquence des opérations, une fenêtre temporelle (une période, telle qu'un week-end, au cours de laquelle le client envisage de rendre ses systèmes indisponibles pour les utilisateurs, pendant laquelle aucune mise à jour n'a lieu afin que les données soient gelées, et durant laquelle le client peut effectuer le changement de fournisseur), ainsi que les ressources informatiques nécessaires.

— Le fournisseur est en mesure de confirmer la disponibilité des ressources informatiques requises pendant la fenêtre temporelle définie.

— Le client déclenche le changement de fournisseur au moment convenu.

Logiciel à la demande (SaaS)

— Le client ne connaît pas la structure de la base de données.

— Le fournisseur de SaaS connaît la structure de la base de données qu'il a définie.

— Le fournisseur de SaaS connaît les procédures et le temps nécessaires pour des opérations telles que les sauvegardes, les optimisations et les réorganisations.

— Lorsqu'une nouvelle version du logiciel à la demande est installée avec une nouvelle version de la structure de la base de données, il n'est pas inhabituel de procéder à une exportation complète de l'ancienne structure suivie d'une importation complète dans la nouvelle structure. Cette procédure donne au fournisseur de SaaS une vue concrète de la procédure, des ressources et du temps nécessaires pour l'exportation des données.

— Le fournisseur de SaaS est en mesure de fournir des précisions sur les méthodes de portage et, le cas échéant, les outils nécessaires,

— ainsi que des informations sur le calendrier et les ressources informatiques nécessaires,

— et il peut proposer les méthodes et formats d'exportation ainsi que la séquence des opérations.

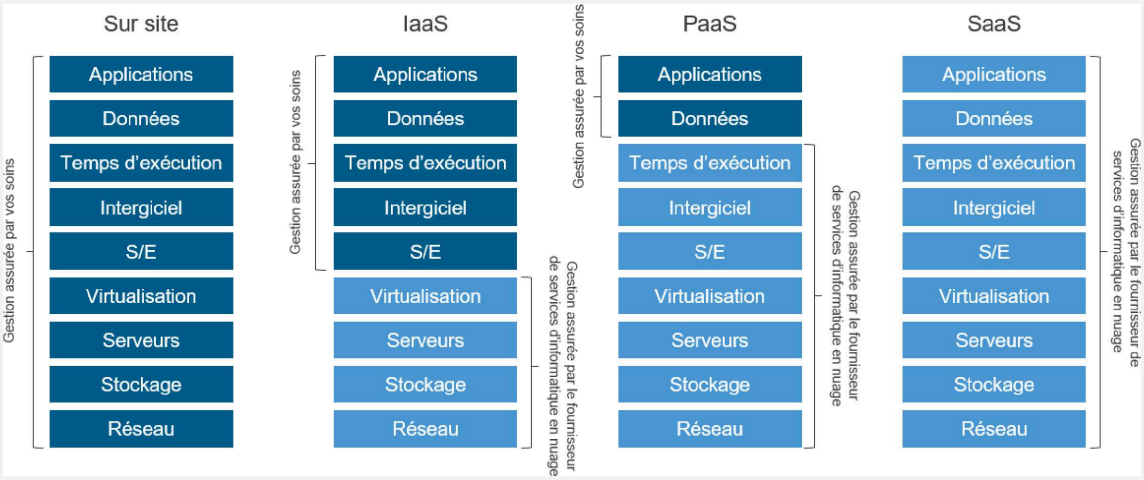
— Le client est responsable de l'importation des données dans l'environnement de destination et peut formuler des exigences et des remarques sur la séquence proposée.

— Le fournisseur de SaaS et le client sont en mesure de convenir de la séquence des opérations, de la fenêtre temporelle et des ressources informatiques nécessaires.

— Le fournisseur est en mesure de confirmer la disponibilité des ressources informatiques requises pendant la fenêtre temporelle.

— En fonction de la séquence et de l'outil convenus, le fournisseur ou le client déclenche le changement de fournisseur au moment convenu.

— Le client est responsable de l'importation des données dans l'environnement de destination.



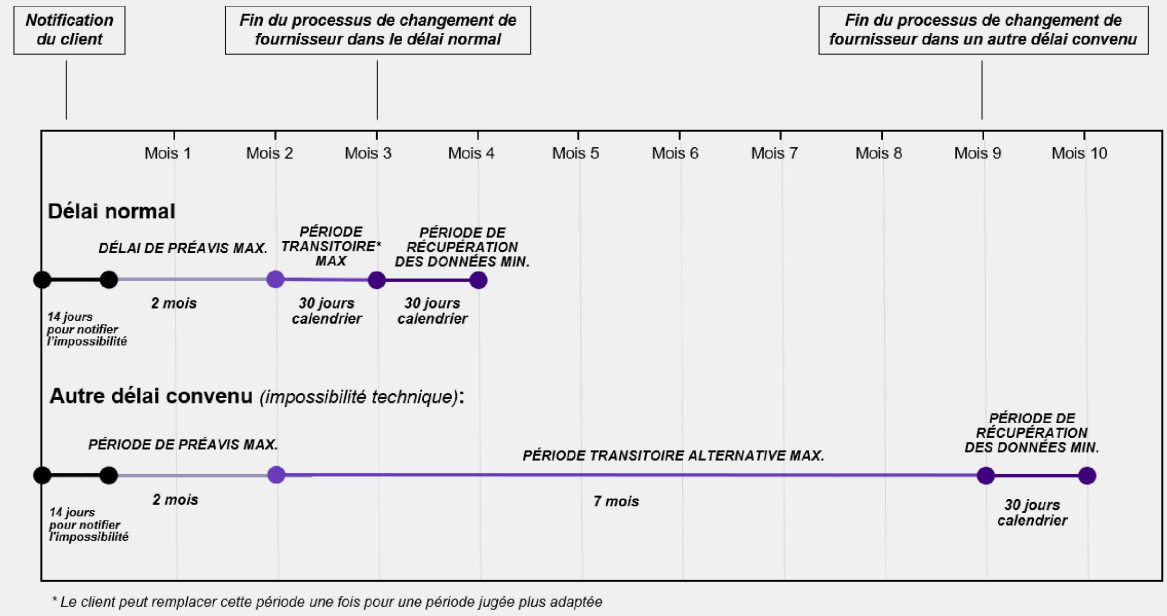
Actions exécutées au cours du délai de préavis maximal et de la période transitoire

Lancement du processus de changement de fournisseur: l'article 25, paragraphe 2, point d), du règlement sur les données exige que les contrats prévoient un délai de préavis maximal pour le lancement du processus de changement de fournisseur, qui ne doit pas dépasser deux mois. Cette clause définit les informations que le fournisseur doit communiquer au client au cours de cette période, ainsi que les actions qu'il exécutera après le lancement du processus de changement de fournisseur.

Période transitoire: l'article 25, paragraphe 2, point a), du règlement sur les données exige que les contrats contiennent des clauses permettant au client, sur demande, de passer à un autre service de traitement de données ou de transférer toutes les données exportables vers une infrastructure TIC sur site, sans retard injustifié et, en tout état de cause, dans un délai ne dépassant pas la période transitoire maximale obligatoire de 30 jours calendaires prenant effet au terme du délai de préavis maximal.

L'article 25, paragraphe 2, point g), du règlement sur les données exige également que le contrat comporte une période minimale d'au moins 30 jours calendaires pour la récupération des données, débutant après la fin de la période transitoire convenue entre les parties.

Lorsque la période transitoire maximale obligatoire de 30 jours pour le changement de fournisseur est techniquement impossible, le fournisseur doit en informer le client dans un délai de 14 jours ouvrables à compter de la demande de changement de fournisseur, expliquer l'impossibilité technique et indiquer une période transitoire alternative, qui ne peut excéder sept mois (article 25, paragraphe 4, du règlement sur les données). Le client a le droit de prolonger la période transitoire maximale obligatoire une fois pour une durée qu'il juge plus appropriée (article 25, paragraphe 5, du règlement sur les données).



L'accord de traitement de données est considéré comme résilié après l'achèvement avec succès du processus de changement de fournisseur ou à l'issue du délai de préavis maximal, lorsque le client ne souhaite pas changer de fournisseur mais souhaite effacer ses données exportables et actifs numériques lors de la résiliation du service. Aucun préavis de résiliation de la part du client n'est nécessaire, étant donné que l'accord prendra fin automatiquement. Toutefois, dans un souci de sécurité juridique et afin de garantir la protection des intérêts des parties, le fournisseur est tenu d'informer le client de la résiliation du contrat [article 25, paragraphe 2, point c), du règlement sur les données].

Option A: plan de changement de fournisseur et de sortie joint en tant qu'annexe à l'accord

Avant de conclure le contrat, les parties pourraient envisager d'élaborer un plan détaillé pour le changement de fournisseur et la sortie. Cela peut être utile, en particulier dans le cas de services complexes de traitement de données. Le plan de changement de fournisseur et de sortie inclus ici donne aux parties, dès le début de la relation contractuelle, une vision claire du processus de changement de fournisseur, y compris en ce qui concerne les types d'informations, de données et de processus qui devront être partagés entre les parties afin de changer de fournisseur sans retard ni incidence sur les services ou les activités du client.

Le modèle de «plan de changement de fournisseur et de sortie» figurant à l'**appendice 1** n'est qu'un exemple de plan de ce type, dont l'objectif est de donner au client une idée des questions qu'il devra poser à son fournisseur ainsi qu'une idée de la structure de ces échanges.

La répartition des responsabilités au cours de l'exécution du processus de changement de fournisseur est un exemple qui respecte, le cas échéant, les droits et obligations consacrés dans le règlement sur les données. Tout en respectant ces droits et obligations, les parties peuvent convenir d'une répartition différente ou de l'inclusion d'informations supplémentaires.

C'est pour cette raison que le plan n'est pas identique à une clause contractuelle standard. Une option consisterait à conserver ce plan en tant qu'annexe technique distincte du contrat susceptible d'être modifiée/mise à jour séparément par les parties. Les parties pourraient également vouloir inclure l'annexe dans le contrat lui-même.

Cette annexe pourrait constituer un plan de changement de fournisseur et de sortie standard proposé par le fournisseur et approuvé par le client, ou bien un plan personnalisé de changement de fournisseur et de sortie proposé par le fournisseur pour son client.

Les parties pourraient mettre à jour le plan de changement de fournisseur et de sortie pendant la durée de l'accord, en fonction de l'évolution des services de traitement de données et des données couvertes par l'accord, aux périodes convenues par les parties. Cette mise à jour pourrait également avoir une incidence sur la période transitoire convenue, par exemple, dans les limites fixées par le règlement sur les données.

Le plan de changement de fournisseur et de sortie s'applique uniquement lorsque le client change de fournisseur ou se tourne vers une infrastructure TIC sur site, et non si le client a l'intention de faire supprimer ses données à la fin du délai de préavis.

Option B: outils de changement de fournisseur automatisés en libre-service

Bien que l'utilisation d'outils de changement de fournisseur automatisés en libre-service soit répandue, elle peut se heurter à certaines difficultés. Ainsi, une préoccupation particulière provient du fait que, dans le cas de SaaS, certaines bases de données et leurs configurations peuvent ne pas être migrées correctement et/ou complètement, nécessitant ainsi une intervention manuelle de la part du fournisseur. Si le fournisseur recourt à ce type de solution en libre-service, les clauses figurant dans l'option B permettent au client de faire en sorte que l'accord contienne suffisamment d'informations sur le processus et l'outil. Les éléments inclus dans l'option A (plan de changement de fournisseur et de sortie en tant qu'annexe à l'accord) peuvent servir de base.

Si un fournisseur utilise des outils de changement de fournisseur pour exécuter les actions prescrites par le règlement sur les données afin de passer au système d'un autre fournisseur ou à une infrastructure TIC sur site, les frais facturés au client pour l'utilisation de ces outils de changement de fournisseur seraient considérés comme des frais de changement de fournisseur.

Qu'en est-il si le changement de fournisseur n'est pas achevé avec succès? La clause 1.7 de l'option A ainsi que la clause 2.6 de l'option B couvrent les situations dans lesquelles le changement de fournisseur n'aboutit pas en précisant les mesures que le client (et son fournisseur de destination) et le fournisseur d'origine devront prendre, de bonne foi, pour achever avec succès le changement de fournisseur et/ou pour déclencher l'option relative à l'effacement des données prévue par le règlement sur les données.

Exemple: le fournisseur d'origine propose une solution de SaaS A tandis que le fournisseur de destination propose une solution de SaaS B. Le client demande au fournisseur d'origine de l'aider à passer au fournisseur de destination en exportant et en transférant ses données exportables vers un serveur spécifique. Les scénarios suivants peuvent se produire:

1. le fournisseur d'origine ne propose pas d'outils ou de procédures efficaces pour l'exportation et le transfert de toutes les données exportables vers le serveur spécifique;
2. les données ont été transmises au serveur spécifique, mais le client ou le fournisseur de destination ne sont pas en mesure de les télécharger correctement.

1. Option A: changement de fournisseur et sortie dans le cadre d'un plan annexé à l'accord

1.1. Informations

1.1.1. Les parties confirment que le fournisseur a mis à la disposition du client, dans une annexe à l'accord ou sur son site web, des informations claires sur:

(a) leurs frais de service standards et, le cas échéant, les pénalités liées à la résiliation anticipée;

(b) les frais de changement de fournisseur;

(c) le cas échéant, les services pour lesquels un changement de fournisseur est très complexe ou coûteux ou pour lesquels il est impossible de changer de fournisseur sans qu'il y ait une interférence significative portant sur les données, les actifs numériques ou l'architecture des services;

(d) le cas échéant, les services spécifiques pour lesquels les obligations en matière de changement de fournisseur et de sortie ne s'appliquent pas.

L'article 31 du règlement sur les données établit un régime spécifique pour certains services de traitement de données. Pour les services conçus sur mesure ou fortement personnalisés, certaines obligations en matière de changement de fournisseur ne s'appliquent pas. Les parties doivent convenir de la manière dont ce changement pourrait avoir lieu (y compris en ce qui concerne le coût). Dans le cas de services de traitement de données fournis en tant que version non destinée à la production à des fins d'essai et d'évaluation et pour une durée limitée, les obligations en matière de changement de fournisseur ne s'appliquent pas. Bien que les présentes clauses contractuelles standards n'aient pas été rédigées pour couvrir de telles situations, elles peuvent néanmoins servir de base aux parties à un accord en ce qui concerne ce type de services.

En vertu de l'article 30, paragraphe 6, du règlement sur les données, les fournisseurs ne seront pas tenus de développer de nouvelles technologies ou de nouveaux services. Ils ne seront pas non plus tenus de divulguer ou de transférer à un client ou à un autre fournisseur de services de traitement de données des actifs numériques qui: i) sont protégés par des droits de propriété intellectuelle; ii) constituent un secret d'affaires; ou iii) compromettent la sécurité et l'intégrité du service du client ou du fournisseur.

1.2. **Changement de fournisseur et sortie**

1.2.1. Les parties conviennent d'un «plan de changement de fournisseur et de sortie» (ci-après le «plan»), en utilisant le formulaire figurant à l'appendice 1, lequel fait partie intégrante de l'accord et sera mis en œuvre par les parties. Le plan comporte:

(a) une spécification exhaustive de toutes les catégories de données et d'actifs numériques qui peuvent être transférés, y compris, au minimum, toutes les données exportables [article 25, paragraphe 2, point e), du règlement sur les données];

(b) une spécification exhaustive des catégories de données spécifiques au fonctionnement interne du service de traitement de données du fournisseur qui seront exclues des données exportables lorsqu'il existe un risque de violation des secrets d'affaires du fournisseur [article 25, paragraphe 2, point f), du règlement sur les données];

(c) des informations claires sur les risques connus, qui relèvent du fournisseur d'origine, pour la continuité de la fourniture des fonctions ou services [article 25, paragraphe 2, point a) iii), du règlement sur les données];

(d) des précisions concernant l'assistance fournie dans le cadre du changement de fournisseur et de la sortie, y compris les méthodes et formats de portage, ainsi que les étapes nécessaires pour effectuer le processus de changement de fournisseur;

(e) le nom et les coordonnées du représentant désigné par le client et le fournisseur pour exécuter le plan;

(f) une estimation du temps nécessaire pour exporter et transférer les données et les actifs numériques depuis l'environnement du fournisseur d'origine;

Le fournisseur d'origine peut faciliter le processus de changement de fournisseur du client en donnant une estimation du temps nécessaire pour exporter et transférer les données exportables en dehors de son environnement, sur la base du temps nécessaire pour importer les données, du volume estimé, de la capacité du réseau, de l'expérience acquise ou d'essais antérieurs. De même, le client peut estimer le temps nécessaire pour importer et mettre en œuvre les données dans l'environnement de destination. Les deux parties devraient tenir compte de ces informations pour déterminer si une période transitoire alternative est nécessaire.

(g) les restrictions et les limitations techniques, y compris celles découlant du stockage de données en dehors de l'Union européenne;

(h) une description de la séquence des opérations de changement de fournisseur proposées par le fournisseur;

(i) une description de la méthode d'essai proposée par le fournisseur si des essais sont effectués.

1.2.2. Le fournisseur communique au client une référence au registre en ligne, avec des informations sur les structures et formats de données, les normes pertinentes et les spécifications d'interopérabilité ouvertes, dans lequel les données exportables sont disponibles à l'adresse [*préciser le lien vers l'emplacement*] [article 26, point b), du règlement sur les données].

1.2.3. À la demande du client, le fournisseur doit mettre à la disposition du personnel désigné par le client (ou par des tiers autorisés), à l'aide de moyens électroniques appropriés, des informations expliquant les procédures pertinentes.

1.2.4. À la demande du client, le fournisseur organisera un essai ou aidera le client à réaliser un essai, comme convenu à l'appendice 1, afin de vérifier que le plan fonctionne dans la pratique en ce qui concerne les données exportables et les actifs numériques. Si des problèmes apparaissent au cours de l'essai, les parties analyseront les causes de bonne foi et conviendront de solutions.

1.2.5. Le fournisseur et le client devraient mettre à jour le plan chaque fois que cela est nécessaire ou lorsque le client en fait la demande, sur la base d'éléments justifiant les changements requis.

1.3. **Lancement du processus de changement de fournisseur**

1.3.1. Le client lance le changement de fournisseur en adressant au fournisseur un avis de changement de fournisseur comme indiqué à la clause 1.10, en respectant le délai de préavis de [*délai de préavis convenu ne pouvant excéder deux mois, à indiquer par les parties*]. Si le client souhaite changer de fournisseur uniquement pour certains services et pour les données ou actifs numériques correspondants, cela doit être précisé dans l'avis de changement de fournisseur. [Option] [Le client adresse l'avis de changement de fournisseur au moyen du formulaire figurant à l'**appendice 3**].

Sous réserve des termes de l'accord, le client peut choisir de ne demander le changement que pour un certain sous-ensemble de services hébergés par le fournisseur d'origine. Dans ce cas, les obligations de changement de fournisseur ne concernent que ces services ainsi que les données et actifs numériques correspondants; pour le reste, les conditions contractuelles convenues précédemment restent applicables.

1.3.2. Dans l'avis de changement de fournisseur, le client indique au fournisseur s'il a l'intention:

(a) de passer à un fournisseur de services de traitement de données différent. Dans ce cas, le client fournit les renseignements nécessaires sur le fournisseur de destination [article 25, paragraphe 3, point a), du règlement sur les données];

(b) de passer à une infrastructure TIC sur site du client [article 25, paragraphe 3, point b), du règlement sur les données]; ou

(c) de ne pas changer de fournisseur mais seulement d'effacer ses données exportables et ses actifs numériques [article 25, paragraphe 3, point c), du règlement sur les données].

(d) [OPTION] [Le client adresse son avis de changement de fournisseur en utilisant le formulaire figurant à l'**appendice 4**]

1.3.3. Le fournisseur confirme au client la réception de l'avis de changement de fournisseur au plus tard dans un délai de [trois jours ouvrables] en utilisant le même moyen de communication que celui utilisé par le client.

1.4. **Période transitoire**

1.4.1. Le client a le droit de changer de fournisseur sans retard injustifié au cours de la période transitoire maximale de 30 jours. Le client peut convenir avec le fournisseur de la période transitoire de [*période transitoire convenue, qui ne peut excéder 30 jours calendaires, à indiquer par les parties*] [article 25, paragraphe 2, point a), du règlement sur les données].

1.4.2. Si le fournisseur n'est pas en mesure de respecter la période transitoire [maximale obligatoire] parce que cela est techniquement impossible, il doit [article 25, paragraphe 4, du règlement sur les données]:

(a) informer le client dans un délai de 14 jours ouvrables à compter du [date de l'avis de changement de fournisseur];

(b) indiquer une période transitoire alternative, qui ne peut excéder sept (7) mois à compter de la date de l'avis de changement de fournisseur adressé par le client; et

(c) motiver dûment l'impossibilité technique.

1.4.3. Le client confirme la réception de la notification d'une période transitoire alternative [dans un délai de trois jours ouvrables].

1.4.4. Le client peut prolonger la période transitoire une fois pour une période qu'il juge plus appropriée à ses propres fins, pour une durée n'excédant pas [*préciser le nombre de mois*] (article 25, paragraphe 5, du règlement sur les données). Dans ce cas, le client fait part de ses intentions au fournisseur, comme convenu à la clause 1.11, avant la fin de la période transitoire initiale et indique la période transitoire alternative proposée. Le fournisseur confirme la réception de cet avis de prolongation [dans un délai de trois jours ouvrables].

1.4.5. [OPTION] Le client notifie la période transitoire alternative en utilisant le formulaire figurant à l'appendice 5.

1.5. **Obligations du fournisseur pendant le processus de changement de fournisseur**

1.5.1. Le fournisseur s'engage à fournir une assistance raisonnable au client et aux tiers autorisés par ce dernier dans le cadre du processus de changement de fournisseur dès le début du processus et tout au long de celui-ci, afin que le client puisse changer de fournisseur au cours de la période transitoire. À cet effet, le fournisseur doit plus particulièrement:

(a) fournir des capacités, des informations adéquates (y compris la documentation nécessaire pour effectuer le changement de fournisseur) et une assistance technique; si des problèmes sont relevés, le fournisseur et le client analyseront de bonne foi les causes et conviendront de solutions;

(b) agir avec la diligence requise pour maintenir la continuité des activités et poursuivre la fourniture des fonctions ou services au titre de l'accord [article 25, paragraphe 2, point a) ii), du règlement sur les données];

(c) maintenir un niveau élevé de sécurité tout au long du processus de changement de fournisseur, en particulier en ce qui concerne la sécurité des données pendant leur transfert [article 25, paragraphe 2, point a) iv), du règlement sur les données].

1.6. **Obligations du client pendant le processus de changement de fournisseur**

1.6.1. Le client s'engage à prendre toutes les mesures raisonnables pour parvenir à un changement effectif de fournisseur. Le client est responsable de l'importation des données et des actifs numériques dans ses propres systèmes ou dans les systèmes du fournisseur de destination, ainsi que de la mise en œuvre de ces données et de ces actifs numérique s au sein de ces systèmes, y compris lorsque le client utilise les services d'un tiers pour ces actions.

1.6.2. Le cas échéant et sans préjudice de l'article 30, paragraphe 6, du règlement sur les données, le client et le fournisseur, ou les tiers mandatés par ces derniers, s'engagent à respecter les droits de propriété intellectuelle de tout matériel fourni par le fournisseur dans le cadre du processus de changement de fournisseur, ainsi que les secrets d'affaires du fournisseur. Le client s'engage à fournir aux tiers qu'il a mandatés l'accès à ce matériel et à permettre son utilisation uniquement dans la mesure où cela est nécessaire pour mener à bien le processus de changement de fournisseur et uniquement avec l'autorisation explicite du fournisseur. L'accès au matériel des fournisseurs ayant trait au processus de changement de fournisseur ainsi que l'utilisation du matériel protégé par des droits de propriété intellectuelle et/ou des secrets d'affaires liés au processus de changement de fournisseur seront supprimés au plus tard à la fin de la période transitoire convenue, y compris la période transitoire alternative, dans le plein respect des engagements de confidentialité et des droits de propriété intellectuelle accordés par le fournisseur.

1.6.3. Le client agit de bonne foi pour mettre en œuvre toute orientation relative au processus de changement de fournisseur partagée par le fournisseur.

1.6.4. Le client peut convenir avec le fournisseur d'origine de paramètres attestant du succès du changement, ainsi que de jalons au cours du processus de changement de fournisseur. Il informe le fournisseur d'origine de la mesure dans laquelle ces jalons ont été atteints au cours du processus de changement de fournisseur. En tout état de cause, le client doit informer le fournisseur qu'il a achevé avec succès le processus de changement de fournisseur.

Outre les obligations prévues dans cet accord, toutes les parties concernées, y compris les fournisseurs de destination de services de traitement de données, ont l'obligation légale, énoncée à l'article 27 du règlement sur les données, de coopérer de bonne foi afin de rendre effectif le processus de changement de fournisseur, de permettre le transfert en temps utile des données, et de maintenir la continuité des services de traitement de données.

1.7. **Échec du changement de fournisseur**

1.7.1. Si le processus de changement de fournisseur n'a pas abouti, les parties doivent coopérer de bonne foi pour déterminer la cause de l'échec et achever le processus avec succès, permettre le transfert en temps utile des données et maintenir la continuité des services. En particulier, à la demande du client, le fournisseur aide ce dernier à déterminer les raisons de l'échec du changement de fournisseur et, dans la mesure où les raisons identifiées sont liées à l'environnement ou aux processus de changement du fournisseur, donne des conseils sur la manière de résoudre les problèmes techniques recensés. Les règles régissant les frais de changement de fournisseur s'appliquent au soutien fourni par le fournisseur et aux autres services du fournisseur visés dans la présente section.

1.7.2. Le client peut autoriser le fournisseur de destination à agir en son nom.

1.8. **Récupération et effacement des données**

1.8.1. Le client peut récupérer ou effacer ses données pendant la période convenue pour la récupération des données, qui est de […] jours.

1.8.2. À la fin de la période convenue pour la récupération des données, et pour autant que le processus de changement de fournisseur ait été achevé avec succès, le fournisseur efface toutes les données exportables et tous les actifs numériques générés par le client ou directement liés au client. Le fournisseur confirme [dans un délai de x jours ouvrables] que cet effacement a été effectué, à l'exception des données à caractère personnel exportables qu'il est tenu de stocker en vertu de la législation de l'UE ou de la législation nationale.

Le délai fixé pour la récupération des données commence au terme de la période transitoire convenue et doit être d'au moins 30 jours calendaires à compter de la fin de la période transitoire convenue entre le client et le fournisseur. Le client peut décider de ne pas faire usage de son droit de récupération des données. Dans ce cas, soit il efface lui-même les données [et peut en informer le fournisseur conformément à l'article 25, paragraphe 3, point c), du règlement sur les données], soit le fournisseur efface les données non récupérées conformément à la clause 1.8.2 de l'option A et à la clause 2.7.2 de l'option B.

1.9. **Frais de changement de fournisseur**

1.9.1. Les frais à payer par le client pour le changement de fournisseur sont les suivants […]

En cas d'utilisation simultanée de plusieurs services de traitement de données (scénario de déploiement multi-nuage), les frais de transfert des données ne sont pas considérés comme des frais de changement de fournisseur et, en tant que tels, peuvent être imposés au client à titre de récupération des coûts supportés par le fournisseur, sans pour autant excéder les coûts réels. Dans tous les autres cas, aucun frais de changement de fournisseur ne peut être imposé au client après le 12 janvier 2027 (voir les explications sur les frais de changement de fournisseur figurant dans les informations introductives des présentes CCS).

1.10. **Résiliation du processus de changement de fournisseur**

[Voir les CCS relatives à la résiliation]

1.11. **Notifications**

Les parties conviennent de toute notification à effectuer entre elles concernant le changement de fournisseur et la sortie [*les parties indiquent les moyens de communication retenus, y compris par des moyens électroniques adéquats*].

1.12. **Ordre de priorité**

En cas de conflit ou d'incohérence entre les présentes clauses relatives au changement de fournisseur et à la sortie et toutes autres dispositions contractuelles, modalités ou conditions applicables ou tout autre accord applicable relatifs au changement de fournisseur d'un service de traitement de données, les présentes clauses prévaudront.

2. **Option B: changement de fournisseur et sortie à l'aide outils de changement de fournisseur automatisés en libre-service**

2.1. **Informations**

2.1.1. Avant la passation de toute commande pour des services de traitement de données, le fournisseur aura fourni au client des informations claires sur:

(a) les outils de changement automatisés en libre-service disponibles pour ces services (ci-après les «outils de changement de fournisseur») et les conditions de leur utilisation;

(b) leurs frais de service standards et, le cas échéant, les pénalités liées à la résiliation anticipée;

(c) les frais de changement de fournisseur, y compris les frais d'utilisation des outils de changement de fournisseur.

L'article 31 du règlement sur les données établit un régime spécifique pour certains services de traitement de données. Pour les services conçus sur mesure ou fortement personnalisés, certaines obligations en matière de changement de fournisseur ne s'appliquent pas. Les parties doivent convenir de la manière dont ce changement pourrait avoir lieu (y compris en ce qui concerne le coût). Dans le cas de services de traitement de données fournis en tant que version non destinée à la production à des fins d'essai et d'évaluation et pour une durée limitée, les obligations en matière de changement de fournisseur ne s'appliquent pas. Bien que les présentes clauses contractuelles standards n'aient pas été rédigées pour couvrir de telles situations, elles peuvent néanmoins servir de base aux parties à un accord en ce qui concerne ce type de services.

Conformément à l'article 30, paragraphe 6, du règlement sur les données, les fournisseurs ne seront pas tenus de développer de nouvelles technologies ou de nouveaux services. Ils ne seront pas non plus tenus de divulguer ou de transférer à un client ou à un autre fournisseur de services de traitement de données des actifs numériques qui: i) sont protégés par des droits de propriété intellectuelle; ii) constituent un secret d'affaires; ou iii) compromettent la sécurité et l'intégrité du service du client ou du fournisseur.

2.1.2. La liste de contrôle relative au changement de fournisseur figurant à l'**appendice 2**, qui fait partie intégrante de l'accord, comprend:

(a) une spécification exhaustive de toutes les catégories de données et d'actifs numériques qui peuvent être transférés à l'aide d'outils de changement de fournisseur, y compris, au minimum, toutes les données exportables [article 25, paragraphe 2, point e), du règlement sur les données];

(b) une spécification exhaustive des catégories de données spécifiques au fonctionnement interne du service de traitement de données du fournisseur qui seront exclues des données exportables lorsqu'il existe un risque de violation des secrets d'affaires du fournisseur [article 25, paragraphe 2, point f), du règlement sur les données];

(c) des informations sur les procédures de changement de fournisseur et de portage à l'aide des outils de changement de fournisseur, y compris les méthodes et formats, les restrictions et les limitations techniques (y compris celles découlant du stockage de données en dehors de l'UE), les procédures, la documentation, ainsi que, le cas échéant, les bonnes pratiques, les capacités, l'assistance technique que le fournisseur mettra à la disposition du client (en particulier pendant les essais, lors de la préparation du changement de fournisseur et au cours de ce changement), y compris des lignes d'appel directes disponibles pour les clients pendant le changement de fournisseur ou d'autres canaux de communication, ainsi que des scénarios d'essai; ces informations doivent expliquer comment changer toutes les données exportables et tous les actifs numériques d'une manière cohérente et uniforme, suffisamment rapidement pour permettre un changement effectif;

(d) une estimation du temps nécessaire pour exporter et transférer les données et les actifs numériques depuis l'environnement du fournisseur d'origine, lorsque les outils de changement de fournisseur sont utilisés conformément à la documentation du fournisseur;

(e) des informations claires sur les risques connus, qui relèvent du fournisseur d'origine, pour la continuité de la fourniture des fonctions ou services [article 25, paragraphe 2, point a) iii), du règlement sur les données];

(f) les ressources, y compris les ressources informatiques (telles que serveurs, CPU, mémoire, I/O, bande passante), qui seront mises à disposition par le fournisseur pour assurer un changement de fournisseur effectif, ainsi que la procédure applicable pour l'obtention de ressources informatiques supplémentaires.

2.1.3. Le fournisseur communique au client une référence au registre en ligne, avec des informations sur les structures de données et les formats de données, les normes pertinentes et les spécifications d'interopérabilité ouvertes, dans lequel les données exportables sont disponibles à l'adresse [*préciser le lien vers l'emplacement*] [article 26, point b), du règlement sur les données].

2.2. **Lancement du processus de changement de fournisseur**

2.2.1. Le client lance le changement de fournisseur en adressant au fournisseur un avis de changement de fournisseur comme convenu à la clause 2.10, en respectant le délai de préavis de [*délai de préavis convenu ne pouvant excéder deux mois, à indiquer par les parties*]. Si le client souhaite changer de fournisseur uniquement pour certains services et pour les données ou actifs numériques correspondants, cela doit être précisé dans l'avis de changement de fournisseur. [OPTION] [Le client adresse son avis de changement de fournisseur en utilisant le formulaire figurant à l'**appendice 3**]

L'avis de changement de fournisseur est un instrument différent de l'avis de résiliation de contrat. Sous réserve des termes de l'accord, le client peut choisir de ne demander le changement que pour un certain sous-ensemble de services fournis par le fournisseur d'origine. Dans ce cas, les obligations de changement de fournisseur ne concernent que ces services ainsi que les données et actifs numériques correspondants; pour le reste, les conditions contractuelles convenues précédemment restent applicables.

2.2.2. Dans l'avis de changement de fournisseur, le client indique au fournisseur s'il a l'intention:

(a) de passer à un fournisseur de services de traitement de données différent; dans ce cas, le client doit fournir les informations nécessaires concernant le fournisseur de destination;

(b) de passer à une infrastructure TIC sur site du client; ou

(c) de ne pas changer de fournisseur, mais seulement d'effacer ses données exportables et ses actifs numériques.

(d) [OPTION] [Le client adresse son avis de changement de fournisseur en utilisant le formulaire figurant à l'**appendice 4**]

2.2.3. Le client peut également indiquer dans l'avis de changement de fournisseur la ou les fenêtres temporelles prévues pour le changement de fournisseur ainsi que les ressources informatiques supplémentaires dont il a besoin pendant ce laps de temps. Si le fournisseur n'est pas en mesure de garantir ces ressources informatiques dans les fenêtres temporelles indiquées, il doit s'y opposer dans un délai maximal de [trois jours ouvrables] à compter de la réception de l'avis de changement de fournisseur, en fournissant une justification appropriée et en proposant au client plusieurs autres «fenêtres temporelles» dans le respect de la période transitoire maximale.

La ou les fenêtres temporelles prévues pour le changement de fournisseur sont une période, par exemple un week-end, au cours de laquelle le client envisage de rendre ses systèmes indisponibles pour les utilisateurs, pendant laquelle aucune mise à jour n'a lieu afin que les données soient gelées, et durant laquelle le client peut procéder au changement de fournisseur.

2.2.4. Le fournisseur confirme au client la réception de l'avis de changement de fournisseur [dans un délai de trois jours ouvrables] en utilisant le même moyen de communication que celui utilisé par le client.

Il se peut que le client doive effectuer le changement de fournisseur dans un délai spécifique afin de réduire au minimum la perturbation de ses activités. En outre, le changement de fournisseur peut exiger des ressources supplémentaires de la part du fournisseur d'origine. Par conséquent, le client doit préciser, au besoin, les fenêtres temporelles pendant lesquelles il a l'intention de procéder au changement de fournisseur, ainsi que les ressources supplémentaires (conformément aux informations fournies par le fournisseur d'origine). Si le fournisseur d'origine n'est pas en mesure de fournir ces ressources durant ces fenêtres temporelles pour des raisons justifiées (par exemple, la maintenance programmée de services qui nuirait gravement à la disponibilité des ressources au cours de cette période), il doit proposer au client des solutions de remplacement à même de garantir un changement de fournisseur effectif avant la fin de la période transitoire maximale.

2.3. **Période transitoire**

2.3.1. Si le fournisseur n'est pas en mesure de respecter la période transitoire [maximale obligatoire] parce que cela est techniquement impossible, il doit s'engager à:

(a) informer le client par écrit, y compris par des moyens électroniques adéquats, dans un délai de 14 jours ouvrables à compter du [date de l'avis de changement de fournisseur];

(b) indiquer une période transitoire alternative, qui ne peut excéder sept (7) mois à compter de la date de l'avis de changement de fournisseur adressé par le client; et

(c) motiver dûment l'impossibilité technique.

Le client confirme la réception de cet avis de prolongation [dans un délai de trois jours ouvrables].

2.3.2. Le client peut prolonger la période transitoire une fois pour une période qu'il juge plus appropriée à ses propres fins, pour une durée n'excédant pas [*préciser le nombre de mois*]. Dans ce cas, le client fait part de son intention au fournisseur par écrit, y compris par des moyens électroniques adéquats, avant la fin de la période transitoire initiale et indique la période transitoire alternative proposée. Le fournisseur confirme la réception de cet avis de prolongation [dans un délai de trois jours ouvrables].

[OPTION] [Le client adresse son avis de prolongation en utilisant le formulaire figurant à l'**appendice 5**]

2.4. **Obligations du fournisseur pendant le processus de changement de fournisseur**

2.4.1. Le fournisseur s'engage à fournir une assistance raisonnable au client et aux tiers autorisés par ce dernier dans le cadre du processus de changement de fournisseur dès le début du processus et tout au long de celui-ci, afin que le client puisse changer de fournisseur au cours de la période transitoire. À cet effet, le fournisseur doit plus particulièrement:

(a) agir avec la diligence requise pour maintenir la continuité des activités et poursuivre la fourniture des fonctions ou services au titre de l'accord;

(b) maintenir un niveau élevé de sécurité tout au long du processus de changement de fournisseur, en particulier en ce qui concerne la sécurité des données pendant leur transfert; et

(c) si des problèmes sont détectés lors du changement de fournisseur et ne peuvent être résolus par une assistance technique, en collaboration avec le client, analyser les causes et convenir des solutions à mettre en œuvre.

Même dans l'option B intitulée «Outils de changement de fournisseur automatisés en libre-service», le fournisseur partage la responsabilité en ce qui concerne le calendrier du changement de fournisseur, par exemple si les outils sont trop lents pour garantir le succès du changement de fournisseur ou si le fournisseur réagit avec un retard injustifié lorsque le client détecte un problème qui nécessite son assistance.

2.5. **Obligations du client pendant le processus de changement de fournisseur**

2.5.1. Le client s'engage à prendre toutes les mesures raisonnables pour parvenir à un changement effectif de fournisseur. Le client s'engage à être responsable de l'importation des données et des actifs numériques dans ses propres systèmes ou dans les systèmes du fournisseur de destination, ainsi que de la mise en œuvre de ces données et de ces actifs numériques, y compris lorsque le client recourt aux services d'un tiers pour ces actions.

2.5.2. Le cas échéant et sans préjudice de l'article 30, paragraphe 6, du règlement sur les données, le client et le fournisseur, ou les tiers mandatés par ces derniers, s'engagent à respecter les droits de propriété intellectuelle de tout matériel fourni par le fournisseur dans le cadre du processus de changement de fournisseur, ainsi que les secrets d'affaires du fournisseur. Le client s'engage à fournir aux tiers qu'il a mandatés l'accès à ce matériel et à permettre son utilisation uniquement dans la mesure où cela est nécessaire pour mener à bien le processus de changement de fournisseur et uniquement avec l'autorisation explicite du fournisseur. L'accès au matériel des fournisseurs ayant trait au processus de changement de fournisseur ainsi que l'utilisation du matériel protégé par des droits de propriété intellectuelle et/ou des secrets d'affaires liés au processus de changement de fournisseur seront supprimés au plus tard à la fin de la période transitoire convenue, y compris la période transitoire alternative, dans le plein respect des engagements de confidentialité et des droits de propriété intellectuelle accordés par le fournisseur.

2.5.3. Le client peut convenir avec le fournisseur d'origine de paramètres attestant du succès du changement, ainsi que de jalons au cours du processus de changement de fournisseur. Il informe le fournisseur d'origine de la mesure dans laquelle ces jalons ont été atteints au cours du processus de changement de fournisseur. En tout état de cause, le client doit informer le fournisseur qu'il a achevé avec succès le changement de fournisseur.

2.5.4. Le client agit de bonne foi pour mettre en œuvre toute orientation relative au processus de changement de fournisseur partagée par le fournisseur.

Outre les obligations prévues dans cet accord, toutes les parties concernées, y compris les fournisseurs de destination de services de traitement de données, ont l'obligation légale, énoncée à l'article 27 du règlement sur les données, de coopérer de bonne foi afin de rendre effectif le processus de changement de fournisseur, de permettre le transfert en temps utile des données, et de maintenir la continuité des services de traitement de données.

Les mesures raisonnables que le client peut prendre pour garantir un changement de fournisseur effectif comprennent notamment:

— la préparation en interne du processus de changement de fournisseur (par exemple, l'arrêt de tout accès aux données et l'information des utilisateurs quant à l'indisponibilité du système; si un tiers est chargé du processus de changement de fournisseur, la communication d'instructions appropriées à ce tiers afin qu'il respecte l'accord conclu entre le client et le fournisseur);

— le suivi du processus de changement de fournisseur (par exemple, la vérification des données et des actifs numériques exportés lors du changement de fournisseur afin de détecter immédiatement tout problème);

— l'élaboration de modalités contractuelles appropriées avec le fournisseur de destination ou la mise à disposition de ressources adéquates pour le changement de fournisseur sur site.

2.6. **Échec du changement de fournisseur**

2.6.1. Si le processus de changement de fournisseur n'a pas abouti, les parties doivent coopérer de bonne foi pour déterminer la cause de l'échec et achever le processus avec succès, permettre le transfert en temps utile des données et maintenir la continuité des services. En particulier, à la demande du client, le fournisseur aide ce dernier à déterminer les raisons de l'échec du changement de fournisseur et, dans la mesure où les raisons identifiées sont liées à l'environnement ou aux processus de changement du fournisseur, donne des conseils sur la manière de résoudre les problèmes techniques recensés. Les règles régissant les frais de changement de fournisseur s'appliquent au soutien fourni par le fournisseur et aux autres services du fournisseur visés dans la présente section.

2.6.2. Le client peut autoriser le fournisseur de destination à agir en son nom.

2.7. **Récupération et effacement des données**

2.7.1. Les parties conviennent que le client récupère ou efface ses données pendant la période convenue pour la récupération des données, qui est de […] jours.

2.7.2. Au terme fin de la période convenue pour la récupération des données, et si le processus de changement de fournisseur a été achevé avec succès, le fournisseur s'engage à effacer toutes les données exportables et tous les actifs numériques générés directement par le client ou liés au client et à confirmer au client la bonne exécution de l'effacement, à l'exception des données exportables que le fournisseur est tenu de stocker en vertu de la législation obligatoire de l'UE ou des États membres de l'UE, pour autant que le fournisseur ait indiqué au client, si la législation l'y autorise, les données exportables qu'il conservera, pendant combien de temps et pour quels motifs.

Le délai fixé pour la récupération des données commence au terme de la période transitoire convenue et doit être d'au moins 30 jours calendaires à compter de la fin de la période transitoire convenue entre le client et le fournisseur. Le client peut décider de ne pas faire usage de son droit de récupération des données. Dans ce cas, soit il efface lui-même les données [et peut en informer le fournisseur conformément à l'article 25, paragraphe 3, point c), du règlement sur les données], soit le fournisseur efface les données non récupérées conformément à la clause 1.8 de l'option A et à la clause 2.7 de l'option B.

2.8. **Frais de changement de fournisseur**

Les frais à payer par le client pour le changement de fournisseur sont les suivants […]

En cas d'utilisation simultanée de plusieurs services de traitement de données (scénario de déploiement multi-nuage), les frais de transfert des données ne sont pas considérés comme des frais de changement de fournisseur et, en tant que tels, peuvent être imposés au client à titre de récupération des coûts supportés par le fournisseur, sans pour autant excéder les coûts réels. Les outils de test prévus pour le changement de fournisseur ainsi que le soutien raisonnable que le fournisseur apporte au client pendant les tests, tel que convenu dans le plan, devraient être considérés comme faisant partie du processus de changement de fournisseur et, par conséquent, les frais pour ces services devraient être progressivement supprimés conformément à l'article 29 du règlement sur les données.

2.9. **Interruption du processus de changement de fournisseur**

Voir la clause 1 des CCS relatives à la résiliation.

2.10. **Notifications**

Les parties conviennent de toute notification à effectuer entre elles concernant le changement de fournisseur et la sortie [*les parties complètent les moyens de communication retenus, y compris par des moyens électroniques adéquats*].

2.11. **Ordre de priorité**

En cas de conflit ou d'incohérence entre les présentes clauses relatives au changement de fournisseur et à la sortie et toutes autres dispositions contractuelles, modalités ou conditions applicables ou tout autre accord applicable relatifs au changement de fournisseur d'un service de traitement de données, les présentes clauses prévaudront.

Appendice 1

Plan de changement de fournisseur et de sortie

1. **Coordonnées**

(a) Informations de contact du fournisseur pour le changement de fournisseur et la sortie: …

(b) Informations de contact du client pour le changement de fournisseur et la sortie: …

2. **Le client est tenu de fournir les informations suivantes dans la notification écrite:**

(a) les données concernées par la notification, conformément à l'identification convenue à l'**appendice 2**;

(b) la destination des données: l'infrastructure TIC du client sur site ou un fournisseur de destination des données, en incluant les spécifications techniques pertinentes concernant le site de destination;

(c) l'emplacement où les données devraient être exportées et transportées.

3. **Obligations du fournisseur de réagir à la notification écrite**

Dans un délai de …. jours, le fournisseur répondra par écrit au client en lui communiquant les informations suivantes:

(a) les spécifications exhaustives de toutes les catégories de données à transférer pendant le processus de changement de fournisseur

i) Données exportables

— Toutes les données importées par le client au début du contrat de service, y compris les métadonnées (*données d'entrée*)

— A, avec métadonnées: ….. au format ….

— B, avec métadonnées: ….. au format ….

— C, avec métadonnées: ….. au format ….

— Toutes les données cogénérées directement ou indirectement du fait de l'utilisation par le client du service de traitement de données:

— D, avec métadonnées: ….. au format ….

— E, avec métadonnées: ….. au format ….

— F, avec métadonnées: ….. au format ….

ii) Actifs numériques:

— L, au format …

— M, au format ...

(b) les spécifications exhaustives des catégories de données spécifiques au fonctionnement interne du service de traitement de données du fournisseur qui doivent être exclues des données exportables lorsqu'il existe un risque de violation des secrets d'affaires du fournisseur: ...

4. **Confirmation des données concernées par le changement de fournisseur**

Le client indiquera les données et les actifs numériques qu'il souhaite recevoir au cours de la période transitoire (ou de la période alternative) convenue.

5. **Ordre, calendrier et essais**

Pendant la période transitoire:

(a) l'ordre et le calendrier convenus pour l'exportation et le transfert des données et des actifs numériques choisis sont les suivants: …

(b) description de la méthode d'essai proposée par le fournisseur: ...

(c) le fournisseur ou le client utilisant les outils et processus du fournisseur testera l'exportation et le transfert vers l'emplacement convenu avec une partie des données et actifs numériques convenus, afin de confirmer ou d'adapter l'ordre et le calendrier;

(d) le client testera l'importation et la mise en œuvre des données et des actifs numériques convenus dans ses propres systèmes ou dans les systèmes du fournisseur de destination;

(e) en cas de problèmes avec les essais ou les résultats des essais, le fournisseur d'origine et le client détermineront si ces problèmes découlent de l'exportation des données et actifs numériques convenus et des processus de transfert relevant de la responsabilité du fournisseur, ou des processus d'importation et de mise en œuvre relevant de la responsabilité du client.

6. **Exécution du processus de changement de fournisseur**

(a) Le fournisseur est tenu d'exporter et de transférer par voie électronique ou physique les données ou les actifs numériques vers l'emplacement spécifié par le client tandis que le client (ou tout tiers autorisé par celui-ci) est tenu d'importer les données ou les actifs numériques dans ses propres systèmes ou dans les systèmes du fournisseur de destination et de mettre en œuvre ces données ou actifs numériques au sein de ces systèmes.

(b) Le client (ou tout tiers autorisé par le client) doit tester les fonctionnalités dans son environnement ou celui du fournisseur de destination dans un délai de ... *[les parties indiquent la période convenue pour la réalisation de l'essai]* et documente pour le fournisseur tout problème découlant i) de la qualité des données ou des actifs numériques exportés ou ii) de l'insuffisance des informations transmises par le fournisseur.

(c) Le fournisseur est tenu de réagir sans retard injustifié afin que le client puisse changer de fournisseur au cours de la période transitoire obligatoire.

7. **Changement de fournisseur achevé avec succès**

Dès que le client a notifié au fournisseur que le processus de changement de fournisseur a été achevé avec succès, le fournisseur s'engage à informer le client sans retard injustifié de la résiliation du contrat. Si le client n'informe pas le fournisseur de la réussite ou de l'échec du changement de fournisseur, alors que le fournisseur a des raisons de croire que le changement de fournisseur a été achevé avec succès par le client, le fournisseur peut envoyer à ce dernier une demande de confirmation quant à l'exécution effective de ce changement. Si le client ne confirme pas l'exécution effective du changement de fournisseur dans un délai de 30 jours calendaires à compter de cette demande, le changement de fournisseur est considéré comme n'ayant pas abouti et l'accord ne sera pas résilié.

Appendice 2

Liste de contrôle relative au changement de fournisseur

Soit les informations requises sont explicitement mentionnées ci-dessous, soit les informations requises sont disponibles à l'adresse suivante: […]

(a) les spécifications exhaustives de toutes les catégories de données et d'actifs numériques qui peuvent être transférées, y compris, au minimum, toutes les données exportables: ...

(b) les spécifications exhaustives des catégories de données et d'actifs numériques spécifiques au fonctionnement interne du service de traitement de données du fournisseur, présentant un risque de violation des secrets d'affaires du fournisseur, qui sont exclues du processus de changement de fournisseur: ...

(c) les informations ayant trait aux procédures de changement de fournisseur et de portage à l'aide d'outils de changement de fournisseur: ...

(d) l'estimation du temps nécessaire pour exporter et transférer les données et les actifs numériques: ...

(e) les risques connus pour la continuité de la fourniture des fonctions ou services du fournisseur d'origine: …

(f) les ressources informatiques qui seront garanties par le fournisseur pour assurer un changement de fournisseur effectif: ...

Appendice 3

Avis de changement de fournisseur

[Nom et adresse du fournisseur aux fins de la communication]

[Date]

Avis de changement de fournisseur

Nom du client: […]

Contrat: [*intitulé du contrat et informations relatives au contrat, par exemple l'intitulé du contrat, le numéro de contrat ou la date d'exécution, conformément aux dispositions du contrat*]

Services faisant l'objet du changement de fournisseur: [*Tous les services sont couverts par le contrat*] ou [*préciser les services ou actifs numériques spécifiques faisant l'objet d'un changement de fournisseur si une partie seulement des services doit être couverte par le changement de fournisseur*]

[OPTION] [Au nom du client, je vous informe/nous vous informons que le client entame le changement de fournisseur des services concernés à compter du (*préciser la date de début*). Le délai de préavis est de (*précisé par le client: deux mois au maximum; le délai peut être plus court à la discrétion du client*)].

[OPTION] [Au nom du client, je vous informe/nous vous informons que le client entame le changement de fournisseur des services, données ou actifs numériques suivants: …

[OPTION] Le client vous informe qu'il envisage de se tourner vers [*coordonnées du nouveau fournisseur/de l'infrastructure sur site du client*].

[OPTION] [(*applicable en cas de changement de fournisseur automatique*). Le client souhaite changer de fournisseur dans la ou les fenêtres temporelles suivantes: (*préciser les dates et les informations nécessaires*). Le client demande que les ressources informatiques suivantes soient disponibles pendant ces laps de temps (*à remplir par le client*)].

Coordonnées de la personne responsable pour le changement de fournisseur: (*coordonnées du représentant du client responsable pour le processus de changement de fournisseur*).

_____

[signature du représentant autorisé du client]

Appendice 4

Notification de la sortie

Le présent formulaire est applicable si le client ne souhaite pas changer de fournisseur, mais seulement effacer ses données exportables ou ses actifs numériques dans le cadre de l'option A et de l'option B.

[Nom et adresse du fournisseur aux fins de la communication]

[Date]

Notification de la sortie

Nom du client: […]

Contrat: [*nom du contrat et informations relatives au contrat, par exemple le nom du contrat, le numéro de contrat ou la date d'exécution, conformément aux dispositions du contrat*].

Données/actifs numériques effacés: [*L'ensemble des données/actifs numériques sont couverts par le contrat*] ou [*préciser les données ou actifs numériques spécifiques concernés par l'effacement*].

[OPTION] [Au nom du client, je vous informe/nous vous informons que le client entame un changement de fournisseur consistant uniquement en l'effacement de données/d'actifs numériques à compter du (*date de début*). Le délai de préavis est de (*précisé par le client: deux mois au maximum; le délai peut être plus court à la discrétion du client*)].

[OPTION] [Coordonnées de la personne responsable pour le changement de fournisseur: (*coordonnées du représentant du client responsable pour le processus de changement de fournisseur*)].

_____

[signature du représentant autorisé du client]

Appendice 5

Notification de la période transitoire alternative

[Nom et adresse du fournisseur aux fins de la communication]

[Date]

Notification de la période transitoire alternative

Nom du client: […]

Contrat: [*intitulé du contrat et informations relatives au contrat, par exemple l'intitulé du contrat, le numéro de contrat ou la date d'exécution, conformément aux dispositions du contrat*].

Données/actifs numériques effacés: [*L'ensemble des données/actifs numériques sont couverts par le contrat*] ou [*préciser les données ou actifs numériques spécifiques concernés par l'effacement*].

[OPTION] [Au nom du client, je vous informe/nous vous informons que le client souhaite prolonger la période transitoire au plus tard jusqu'au [*date*].

[OPTION] [Coordonnées de la personne responsable pour le changement de fournisseur: (*coordonnées du représentant du client responsable pour le processus de changement de fournisseur*)].

_____

[signature du représentant autorisé du client]

ANNEXE VII

CLAUSES CONTRACTUELLES STANDARDS

relatives à la résiliation

Le règlement (UE) 2023/2854 (ci-après le «règlement sur les données») permet aux clients de services de traitement de données (c'est-à-dire des services d'informatique en nuage et en périphérie) de changer de fournisseur ou de transférer leurs données vers leur propre infrastructure TIC sur site. Le changement de fournisseur aura un effet sur la poursuite ou la résiliation de l'accord conclu entre les parties.

Les présentes CCS traitent de la résiliation de l'accord conclu entre le client et le fournisseur en ce qui concerne un service particulier dans le cadre du changement de fournisseur. Ces CCS couvrent le processus de résiliation du contrat de service. Elles sont directement liées aux CCS relatives au changement de fournisseur et à la sortie et prévoient plusieurs possibilités de résiliation et conditions connexes. Le contrat de traitement de données est généralement résilié (en tout ou en partie) une fois que le processus de changement de fournisseur a été achevé avec succès ou lorsque le client ne souhaite pas changer de fournisseur mais demande que toutes les données soient effacées, et que cet effacement est exécuté avec succès. Certaines options supplémentaires sont incluses dans les présentes CCS afin d'aider les parties confrontées à des scénarios qui ne sont pas couverts par le règlement sur les données.

L'accord conclu avec le fournisseur peut couvrir plusieurs services. Si les présentes CCS sont ajoutées à l'accord et que le client transfère un service vers un fournisseur de destination alors que les autres services restent du ressort du fournisseur d'origine, l'accord n'est résilié qu'en ce qui concerne ce service spécifique, à moins que les parties n'en conviennent autrement.

Outre la résiliation liée au changement de fournisseur couverte par ces CCS, l'accord pourrait également être résilié pour tout autre motif de résiliation figurant dans l'accord principal ou prévu par le droit applicable. Le fournisseur peut décider de résilier l'accord si le client manque à ses obligations et adresser un avis de résiliation. Dans ce cas, le client peut présenter un avis de changement de fournisseur, de sorte que l'accord serait prolongé jusqu'à ce que le processus de changement de fournisseur soit achevé avec succès.

D'autres clauses contractuelles standards recommandées par la Commission figurent en annexe et portent sur des sujets spécifiques autres que la résiliation de l'accord. Les parties sont encouragées à envisager d'utiliser également ces autres clauses, étant donné qu'elles ont été élaborées pour être cohérentes et se renforcer mutuellement.

Que comportent les CCS relatives à la résiliation?

Scénarios prévus par le règlement sur les données: l'accord sera résilié dans des circonstances spécifiques une fois que le changement de fournisseur aura été achevé avec succès (*événement A*) ou si le client ne souhaite pas changer de fournisseur mais exige que toutes les données soient effacées et que cet effacement est mené à terme (*événement B*). L'accord sera considéré comme résilié si le changement de fournisseur est achevé avec succès (*événement A*) ou à l'issue du délai de préavis maximal (*événement B*). Il n'est pas nécessaire de notifier l'avis de résiliation ou de suivre la procédure de résiliation prévue par l'accord, étant donné que celui-ci prendra fin automatiquement. Le fournisseur est cependant tenu d'informer le client que le contrat est considéré comme résilié [article 25, paragraphe 2, point c), du règlement sur les données]. Cette notification est de nature informative, étant donné que l'accord est déjà résilié. Par conséquent, même si le fournisseur tarde à adresser cette notification, il ne peut facturer aucun frais au titre du contrat résilié.

Toutefois, le client doit notifier au fournisseur que le processus de changement de fournisseur a été achevé avec succès, étant donné que ce dernier peut ne pas avoir reçu l'information. Si le fournisseur a des raisons de penser que le client a déjà changé de fournisseur avec succès (par exemple, le client ne se connecte pas au service ou ne conserve aucune donnée au repos dans le cadre de ce service), il peut contacter le client et demander confirmation du changement effectif de fournisseur. En l'absence de réponse du client, le changement de fournisseur est considéré comme n'ayant pas été achevé avec succès et le contrat se poursuit (il n'est donc pas résilié) selon les conditions existantes applicables.

Le règlement sur les données ne définit pas ce que l'on entend par un changement de fournisseur achevé avec succès. C'est en principe au client qu'il appartient de décider si le changement a été achevé avec succès. Toutefois, le client, ou le client et le fournisseur, peuvent convenir de certains critères permettant de déterminer si le changement a été achevé avec succès, tels que notamment:

(a) l'achèvement du transfert de données, c'est-à-dire lorsque toutes les données exportables et, le cas échéant, les actifs numériques ont été transférés dans l'environnement du fournisseur de destination, et que leur exactitude, leur intégrité et leur exhaustivité ont été conservées: les données exportables et les actifs numériques devraient correspondre aux données et aux actifs numériques originaux sans perte ni corruption;

(b) le déploiement d'actifs numériques (le cas échéant): si le changement de fournisseur incluait le transfert d'actifs numériques, tels que les applications propres au client ou sous licence, le client devrait vérifier si ces actifs numériques sont installés et configurés et s'ils fonctionnent dans l'environnement du fournisseur de destination des données;

(c) la réalisation d'essais dans le cas d'un nouveau service: au cours de cette phase, le client devrait s'assurer que les services proposés par le fournisseur de destination fonctionnent comme prévu avant le changement de fournisseur: en particulier, le client devrait effectuer des essais de performance, de fonctionnalité et de fonctionnement du service du fournisseur de destination, y compris en ce qui concerne les données ou les actifs numériques transférés, afin d'évaluer s'il est satisfait aux critères de vérification mentionnés ci-avant concernant le changement de fournisseur.

Dans le cas d'un contrat à durée déterminée, le changement de fournisseur peut prendre fin avant l'expiration du contrat ou après celle-ci (dans ce dernier cas, voir l'événement D). Si le changement de fournisseur prend fin avant l'expiration du contrat, l'accord expire également. Dans ce cas, des pénalités liées à la résiliation anticipée peuvent être dues [article 23, point a), article 25, paragraphe 2, point c), et article 29, paragraphe 4, du règlement sur les données].

Qu'en est-il si le changement de fournisseur n'est pas achevé avec succès?

Voir les CCS relatives au changement de fournisseur et à la sortie

Pour résoudre une situation dans laquelle le changement de fournisseur n'est pas achevé avec succès et où l'accord ne peut être résilié, les parties peuvent déposer une réclamation auprès de l'autorité compétente en vertu du règlement sur les données, afin que celle-ci prenne une décision. Toutefois, il convient de préciser que les parties peuvent également utiliser tous les moyens juridiques disponibles au sein de leur juridiction (par exemple, introduire une réclamation, demander des injonctions aux juridictions civiles, etc.).

Deux autres scénarios: les clauses 1.4 et 1.5 sont facultatives et présentent deux autres scénarios à envisager par les parties. Bien qu'ils ne soient pas expressément mentionnés dans le règlement sur les données, ces scénarios peuvent se produire dans la pratique et sont ainsi prévus dans les clauses afin d'aider les parties à résoudre de telles situations. Les scénarios en question sont les suivants:

— le client souhaite prolonger la disponibilité de ses données auprès du fournisseur d'origine ou maintenir le contrat conclu avec le fournisseur d'origine en utilisant la possibilité d'acquérir un nouveau service pour une période plus longue, que cette opération soit précédée ou non d'un changement de service ou d'une simple résiliation de service sans changement de fournisseur. Il se peut que le client n'ait besoin de maintenir auprès du fournisseur d'origine qu'un service aux fonctionnalités limitées, c'est-à-dire en garantissant la disponibilité de ses données pendant cette période plus longue ou en disposant d'un contrat permettant de commander le nouveau service (*événement C*).

Dans ce cas, étant donné que les données seront disponibles dans le cadre d'un service aux fonctionnalités limitées, le fournisseur d'origine et le client devraient conclure un nouvel accord pour ce service supplémentaire ou modifier l'accord existant (voir clause 1.4.2). En particulier, les parties devraient convenir d'une nouvelle période pour la récupération des données. Dans le cas d'accords(-cadres) généraux, le client peut souhaiter maintenir la relation contractuelle avec le fournisseur d'origine afin de pouvoir acquérir rapidement de nouveaux services sans passer par la conclusion d'un nouveau contrat, ce qui, dans les grandes organisations, peut constituer un processus long et compliqué.

Exemple pour l'événement C: le client a exporté et transféré avec succès ses données du fournisseur d'origine au fournisseur de destination dans l'environnement duquel les données ont été déployées avec succès. Un autre exemple pourrait être une situation dans laquelle le client peut décider de résilier le service conclu auprès du fournisseur d'origine sans migrer par la suite vers un autre fournisseur. Dans les deux exemples, le client ne souhaite toutefois pas que ses données soient effacées et préfère au contraire qu'elles soient sauvegardées en toute sécurité auprès du fournisseur d'origine au-delà de la période convenue pour la récupération des données. Tout service supplémentaire de ce type rendu possible par le fournisseur d'origine n'empêche pas la résiliation de l'accord initial, et la fourniture du service serait fondée sur la conclusion d'un nouvel accord ou sur la modification d'un accord existant;

— un contrat à durée déterminée expire avant que le processus de changement de fournisseur n'ait eu lieu ou n'ait été achevé (événement D)

Exemple de situation pour l'événement D: le client n'adresse pas son préavis suffisamment à l'avance. Dans ce cas, les données n'ont pas été transférées au fournisseur de destination à la date d'expiration de l'accord conclu avec le fournisseur d'origine.

Les parties doivent être conscientes du fait qu'une suspension des services peut survenir pendant le processus de changement de fournisseur. Dans ce cas, la clause générale de suspension des services figurant dans l'accord s'applique.
Il existe des exclusions pour certains services personnalisés. De plus amples explications figurent dans les CCS relatives au changement de fournisseur et à la sortie.

1. **Résiliation**

1.1. **Procédure de résiliation**

1.1.1. L'accord sera considéré comme résilié entre les parties lorsque l'un des événements suivants se produit:

(a) le cas échéant, le processus de changement de fournisseur est achevé avec succès. Si le processus de changement de fournisseur est achevé avec succès avant l'expiration de la durée convenue de l'accord, les frais liés à la résiliation anticipée fixés dans ledit accord s'appliquent; ou

(b) au terme du délai de préavis maximal, le client ne souhaite pas changer de fournisseur mais souhaite effacer ses données exportables et ses actifs numériques lors de la résiliation du service.

1.1.2. L'accord comporte des clauses relatives à la résiliation qui sont soumises au droit applicable, telles que mentionnées ci-dessous:

(a) une partie demande la suspension des paiements ou une partie a été déclarée en faillite;

(b) une partie ne s'est pas acquittée, en temps utile, d'une obligation découlant de l'accord qui entraîne ou pourrait entraîner (en vertu de dispositions contractuelles ou législatives) la résiliation de l'accord;

(c) une partie a connu un changement de propriété ou de contrôle qui, en vertu de dispositions contractuelles ou législatives, entraîne ou pourrait entraîner la résiliation de l'accord;

(d) l'accord est déclaré nul et non avenu en raison d'une violation ou d'une modification du droit contraignant applicable; ou

(e) toute autre situation qui, en vertu de dispositions contractuelles ou législatives, entraîne ou pourrait entraîner la résiliation de l'accord.

Même si, au cours du processus de changement de fournisseur, un motif de résiliation apparaît, l'accord ainsi que les services et fonctions convenus ne seront pas résiliés ou n'expireront pas avant l'achèvement effectif du processus [voir la clause 1.1.1, point a)] ou au terme du délai de préavis maximal si le client souhaite uniquement effacer ses données exportables et ses actifs numériques lors de la résiliation du service [voir la clause 1.1.1, point b)], sauf disposition contraire du droit contraignant. Ce principe ne porte pas atteinte aux autres droits ou voies de recours dont dispose une partie à l'égard de l'autre partie. Il s'applique également si le processus de changement de fournisseur commence après que le fournisseur a notifié la résiliation de l'accord.

1.1.3. Sans préjudice des autres voies de recours prévues par le droit applicable, l'accord ne sera pas résilié ou n'expirera pas avant que le processus de changement de fournisseur ne soit achevé avec succès, qu'une décision pertinente n'ait été prise par une juridiction compétente ou qu'un accord n'ait été conclu entre les parties.

1.2. **Résiliation à l'achèvement du changement de fournisseur**

1.2.1. L'accord n'est résilié que lorsque le processus de changement de fournisseur a été achevé avec succès. Dès que le client notifie au fournisseur que le processus de changement de fournisseur a été achevé avec succès, le fournisseur notifie sans retard injustifié au client la résiliation de l'accord.

1.2.2. Si le client n'informe pas le fournisseur de l'issue du changement, et que le fournisseur a des motifs justifiés de penser que le changement de fournisseur a été achevé avec succès par le client, il peut adresser au client une demande de confirmation de l'achèvement effectif du changement de fournisseur. Si le client ne confirme pas l'achèvement avec succès du changement de fournisseur dans un délai de 30 jours ouvrables à compter de la demande, le changement de fournisseur est considéré comme non réussi, de sorte que l'accord n'est pas résilié et se poursuit selon ses conditions existantes.

1.3. **Résiliation sans changement de fournisseur**

1.3.1. Si le client ne souhaite pas changer de fournisseur mais souhaite effacer ses données exportables et ses actifs numériques au moment de la résiliation du service, comme indiqué à la clause 1.1.1, point b), cette opération ne peut se produire et ne sera réputée achevée que si:

(a) le délai de préavis [maximal] convenu a expiré;

(b) le client a explicitement demandé au fournisseur de procéder à l'effacement des données et, en retour, les données ont été effacées avec succès et l'opération a été confirmée par le fournisseur; et

(c) à l'issue du délai de préavis convenu, le fournisseur a informé le client de la résiliation de l'accord.

Autres scénarios [clauses facultatives à envisager]

1.4. **Prolongation de la conservation des données**

1.4.1. À la fin de la période transitoire, le client peut décider de ne pas effacer toutes ses données exportables et ses actifs numériques au terme de la période [minimale]/convenue pour la récupération des données et de faire en sorte qu'ils soient disponibles, y compris aux fins de la fourniture d'un service aux fonctionnalités limitées, pendant une période prolongée donnée.

1.4.2. Dans ce cas, le client et le fournisseur conviennent soit i) de modifier l'accord existant de façon à couvrir la période prolongée aux fins de la récupération des données, soit ii) de conclure un nouvel accord pour un service aux fonctionnalités limitées.

1.5. **Expiration d'un contrat à durée déterminée avant le changement de fournisseur**

1.5.1. Si l'accord a été conclu pour une durée déterminée et i) que la date d'expiration est atteinte avant l'achèvement du processus de changement de fournisseur, et ii) que le client n'a pas demandé l'effacement de ses données exportables et de ses actifs numériques, alors:

(a) la période transitoire commence à la date d'expiration de l'accord; le fournisseur fournit une assistance raisonnable telle que définie dans les CCS relatives au changement de fournisseur et à la sortie;

(b) lors de l'achèvement avec succès du processus de changement de fournisseur, la clause 1.2 s'applique; et

(c) en cas d'échec du processus de changement de fournisseur, la clause 1.7 de l'option A ou la clause 2.6 de l'option B relevant des CCS relatives au changement de fournisseur et à la sortie s'appliquent.

1.6. **Notifications**

Les parties conviennent que toute notification entre elles concernant les présentes clauses relatives à la résiliation doit être effectuée [*les parties indiquent les moyens de communication choisis, y compris par des moyens électroniques adéquats*].

1.7. **Ordre de priorité**

En cas de conflit ou d'incohérence entre les présentes clauses relatives à la résiliation et toutes autres dispositions contractuelles, modalités et conditions générales applicables ou tout autre accord applicable relatifs à la résiliation de l'accord qui sous-tend la fourniture de services de traitement de données, les présentes clauses prévaudront.

ANNEXE VIII

CLAUSES CONTRACTUELLES STANDARDS

relatives à la sécurité des données et à la continuité des activités

Le considérant 94 du règlement (UE) 2023/285 (ci-après le «règlement sur les données») indique que, tout au long du processus de changement de fournisseur, un niveau élevé de sécurité devrait être maintenu et que le fournisseur devrait agir avec la diligence requise pour maintenir la continuité des activités et assurer la fourniture des fonctions ou services prévus par l'accord, ainsi que pour fournir des informations claires concernant les risques connus pour la continuité.

Le règlement sur les données impose au fournisseur l'obligation d'assurer un niveau élevé de sécurité et de continuité des activités en ce qui concerne le processus de changement de fournisseur. Cela concerne en particulier la sécurité des données pendant leur transfert et le maintien de la sécurité des données pendant la période de récupération [article 25, paragraphe 2, point a) iv), du règlement sur les données]. Si la question de la sécurité et de la continuité des activités est généralement incluse dans l'accord sur le traitement de données et d'autres documents contractuels, les présentes CCS portent plus précisément sur la sécurité des données et la continuité des activités dans le cadre du processus de changement de fournisseur et de sortie conformément aux droits et obligations introduits par le règlement sur les données.

Ces CCS combinent des clauses ayant trait aux questions spécifiques de la sécurité des données et de la continuité des activités tout au long du processus de changement de fournisseur étant donné le contexte et l'esprit similaires qui caractérisent la sécurité des données et la continuité des activités. Bien que des dispositions relatives à la sécurité des données et à la continuité des activités soient incluses dans l'accord de services, certaines spécificités liées au processus de changement de fournisseur doivent être prises en compte.

Le processus de changement de fournisseur peut entraîner des risques spécifiques en matière de sécurité susceptibles de se concrétiser au cours des différentes phases et pour les différents aspects du processus auxquels une attention particulière doit être accordée, tels que:

i. le traitement des données;
ii. la gestion de l'identité et le contrôle de l'accès;
iii. le transfert des données;
iv. la récupération des données;
v. la confidentialité, l'intégrité et la disponibilité permanentes des données; et
vi. d'autres risques liés à la préparation et à l'exécution d'un processus de changement de fournisseur effectif.

De même, les risques spécifiques pour la continuité des activités liés au processus de changement de fournisseur méritent une attention et une considération particulières. Ces risques peuvent concerner:

i. le maintien de la continuité des activités afin d'assurer un niveau élevé de sécurité du service;
ii. la poursuite de la fourniture des services prévus par l'accord;
iii. la communication d'informations claires sur les risques connus pour la continuité des services fournis.

À cet égard, l'article 25, paragraphe 2, point a) ii), du règlement sur les données oblige le fournisseur à agir avec la diligence requise pour maintenir la continuité des activités et assurer la fourniture des fonctions ou des services au titre du contrat. Le fournisseur est également tenu de communiquer des informations claires sur les risques connus, qui relèvent du fournisseur d'origine de services de traitement de données, pour la continuité de la fourniture des fonctions ou services [article 25, paragraphe 2, point a) iii), du règlement sur les données].

Sécurité et continuité des activités fondées sur les risques: Lorsque les CCS prévoient des modalités contractuelles, une approche tous risques fondée sur les risques en matière de sécurité implique une approche dynamique et contextuelle en ce qui concerne non seulement les services et les modèles de déploiement applicables, mais aussi l'utilisation, les besoins et les risques connexes. Il appartient au client et au fournisseur de définir, d'approuver, de mettre en œuvre et de suivre conjointement les mesures et les contrôles correspondants afin d'améliorer la résilience et l'intégrité globales des services.

Par exemple, une attention particulière devra être accordée en permanence au respect de niveaux appropriés et responsables en ce qui concerne:

i. l'intégrité des données;
ii. la résilience à toutes les vulnérabilités connues lors de la mise à disposition des données à des fins de récupération;
iii. les signatures de cryptage;
iv. la gestion spéciale de l'accès multicritères;
v. la vérification de l'identité, y compris l'autorisation;

vi. la sécurité du site web, du portail, de la plateforme et des interfaces de programmation d'applications (API) connexes:
vii. la sécurité des éléments relevant du fournisseur;
viii. la fourniture et l'assurance du côté du client, y compris la sécurité du ou des fournisseurs de destination concernés;
ix. l'activité de réseau;
x. l'enregistrement des attaques par force brute;
xi. la sécurité de la couche de transport (TLS) et autres sécurités pendant le transfert;
xii. la protection contre les attaques par déni de service distribué (DDOS); et
xiii. les politiques et pratiques strictes en matière d'effacement des données.

Le fournisseur devrait être en mesure de démontrer, dans l'intérêt du client, que les mesures techniques, opérationnelles et organisationnelles en matière de sécurité et de protection des données sont garanties de manière continue et appropriée.

Cette idée est similaire à la structure et à l'approche prévues i) respectivement à l'article 25 et à l'article 32 du RGPD [règlement (UE) 2016/679]; ii) dans la directive SRI 2 [EUR-Lex)]; iii) dans le schéma de certification de cybersécurité prévu par le règlement (UE) 2019/881 sur la cybersécurité.

Des exemples de ce que le fournisseur devrait démontrer comprennent notamment:
i. les politiques en matière de sécurité interne, de contrôle de l'assurance et de gestion des atteintes à la sécurité ou d'autres incidents;
ii. le respect de certaines normes ouvertes et non propriétaires communément utilisées dans le secteur concerné;
iii. la certification ou autre assurance conforme, ou autres formes de conformité, au droit national applicable en vigueur ou aux schémas européens de certification de cybersécurité pertinents élaborés en vertu du règlement (UE) 2019/881 (règlement sur la cybersécurité); ou
iv. les normes techniques de réglementation applicables, le cas échéant, dans le ou les secteurs concernés.

Réglementations fondées sur les risques: pour de nombreux fournisseurs actifs dans l'UE, ainsi que pour certains clients, certaines réglementations fondées sur les risques peuvent s'appliquer. Cela se traduit généralement par un renforcement des obligations et des responsabilités en matière de sécurité, avec comme conséquence que les infractions et autres incidents entraînent des effets plus graves sur le plan juridique, sur le plan de la réputation et sur d'autres plans. Aussi est-il fortement recommandé de tenir compte de ces réglementations fondées sur les risques avant la conclusion d'un contrat de services ou pendant son exécution.

Voici quelques exemples de réglementations fondées sur les risques susceptibles de s'appliquer: la directive SRI 2, la directive sur la résilience des entités critiques (CER), le règlement sur la résilience opérationnelle numérique du secteur financier (DORA), le règlement sur la cyberrésilience (CRA), le règlement sur la cybersécurité et le règlement général sur la protection des données (RGPD), ainsi que les éventuelles règles prévues par les législations nationales.

Les présentes CCS utilisent le terme «incident» tant dans le cadre de la sécurité que dans le cadre de la continuité des activités (*voir la section «Définitions»*).

Par exemple, la clause 1.4 englobe également les notifications au titre de l'article 33 du RGPD et de l'article 23 de la directive SRI 2.

D'autres clauses contractuelles standards recommandées par la Commission figurent en annexe et couvrent des sujets spécifiques autres que la sécurité et la continuité des activités. Les parties sont encouragées à envisager d'utiliser également ces autres clauses, étant donné qu'elles ont été élaborées de façon à être cohérentes et à se renforcer mutuellement.

1. **Sécurité et continuité des activités**

1.1. **Généralités**

1.1.1. Le fournisseur s'engage à appliquer les mesures techniques et organisationnelles les plus appropriées afin que le niveau de sécurité et de résilience soit proportionné aux risques présentés par les services ainsi que par leur utilisation prévue et raisonnablement prévisible en ce qui concerne le processus de changement de fournisseur.

1.1.2. En outre, le fournisseur s'engage à prévenir les perturbations du service et à maintenir la continuité des services pendant le processus de changement de fournisseur. Il s'agit notamment de prévoir et de maintenir une gestion adéquate de la continuité des activités comprenant la planification de mesures d'urgence et des mesures de reprise des activités après sinistre fondées sur les meilleures pratiques établies et les normes du marché. Ces mesures doivent être tenues à jour et régulièrement réexaminées et évaluées par le fournisseur.

1.2. **Sécurité**

1.2.1. Conformément à la clause 1.1.1, le fournisseur doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir le maintien d'un niveau élevé de sécurité pendant le processus de changement de fournisseur. Cela concerne, en particulier, la sécurité des données pendant leur transfert ainsi que le maintien de la sécurité des données pendant la période de récupération.

1.2.2. Le fournisseur est tenu de mettre en œuvre les mesures techniques et organisationnelles appropriées pour maintenir, pendant le processus de changement de fournisseur, un niveau de sécurité proportionné au niveau des risques. Cela comprend notamment: les risques pertinents liés à la sécurité du traitement des données, à la gestion de l'identité et au contrôle de l'accès, à la portabilité des données, à la récupération des données, à la confidentialité, à l'intégrité et à la disponibilité permanentes des données, ainsi que tout autre risque lié au changement effectif de fournisseur.

1.2.3. Les mesures couvertes par les clauses 1.1.1 et 1.2.1 doivent à tout le moins garantir, sans limitation:

(a) la confidentialité, l'intégrité et la disponibilité en permanence des données, ainsi que la résilience des services, des données exportables et des actifs numériques;

(b) le rétablissement de la disponibilité et de l'intégrité des données et de l'accès à celles-ci dans un délai raisonnable en cas d'incident; et

(c) un suivi continu ainsi que la réalisation régulière de tests, analyses et évaluations de l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité des services, des données exportables et des actifs numériques.

1.3. **Continuité des activités**

1.3.1. Conformément à la clause 1.1.2, le fournisseur doit en particulier:

(a) agir avec la diligence requise pour maintenir la continuité des activités et poursuivre la fourniture des services au titre de l'accord; et

(b) communiquer des informations claires sur les risques connus pour la continuité des services fournis.

1.4. **Notifications**

1.4.1. Les parties conviennent de toute notification à effectuer entre elles concernant les présentes clauses relatives à la sécurité et à la continuité des activités [*les parties indiquent les moyens de communication choisis, y compris par des moyens électroniques adéquats*].

1.4.2. Le fournisseur est tenu d'informer le client de tout incident. Il doit l'en informer dans les meilleurs délais et, en tout état de cause, dans les 72 (soixante-douze) heures suivant la prise de connaissance de l'incident, à moins que des obligations réglementaires n'exigent un avertissement ou une notification similaire dans un délai plus court.

1.4.3. La notification du fournisseur doit inclure les informations nécessaires au client pour évaluer les conséquences de l'incident. Le fournisseur doit, de manière rapide, efficace et raisonnable, et sans frais supplémentaires, assister le client et coopérer avec lui (y compris avec des tiers autorisés par le client) pour toute mesure d'enquête que le client est habilité à prendre conformément au droit de l'Union et au droit national applicables.

1.4.4. Si l'incident a, ou risque d'avoir, des répercussions négatives sur le fournisseur, ce dernier doit prendre les mesures les plus appropriées nécessaires pour réduire au minimum les effets de l'incident et éviter qu'il ne se reproduise. Ce principe ne porte pas atteinte aux autres droits que le client peut détenir en vertu de l'accord ou du droit de l'Union ou du droit national applicable.

1.5. **Divers**

1.5.1. À la demande du client, le fournisseur doit lui fournir, sans retard injustifié, un récapitulatif des principaux éléments constituant les mesures de sécurité et de gestion de la sécurité correspondante qu'il a prises, de même que les principaux éléments sous-tendant la continuité de ses activités et la gestion des situations d'urgence qui en découle, ainsi que toute modification importante apportée à l'un des éléments mentionnés ci-avant.

1.5.2. À la demande du client, le fournisseur doit lui communiquer, dans les meilleurs délais, des informations supplémentaires complétant le récapitulatif mentionné ci-dessus, tels que des résultats de tests ou des éléments probants en matière d'assurance. Dans ce cas, le fournisseur peut exiger du client qu'il signe un accord de non-divulgation avant de partager ces informations. Cet accord de non-divulgation doit toutefois comporter des exceptions d'usage et ne pas avoir d'effet sur les autres dispositions du présent paragraphe, de l'accord ou du droit de l'Union ou du droit national applicable. Le fournisseur a le droit de demander que les informations soient partagées uniquement sur la base du besoin d'en connaître, y compris avec son ou ses fournisseurs désignés ou avec d'autres fournisseurs tiers du client concernés par l'accord.

Ces exceptions d'usage comprennent toute information (ou partie pertinente d'information) i) qui relève déjà du domaine public, ii) que le client est tenu de divulguer lorsque l'obligation lui en est faite a) en vertu du droit applicable, ou b) par toute autorité gouvernementale ou autre autorité réglementaire (les obligations émanant de ces deux dernières entités comprenant, entre autres, les décisions de justice ou toute décision au titre du RGPD ou de la directive SRI 2).

1.6. **Ordre de priorité**

Sans préjudice des clauses contractuelles standards prévues par le RGPD, en cas de conflit ou d'incohérence entre les présentes clauses relatives à la sécurité et à la continuité des activités et toutes autres dispositions contractuelles, modalités ou conditions applicables ou tout autre accord applicable relatifs à la sécurité et à la continuité des activités, les présentes clauses prévaudront.

ANNEXE IX

CLAUSES CONTRACTUELLES STANDARDS

relatives à la non-dispersion

Les accords de traitement de données comprennent souvent divers documents complémentaires faisant référence à du matériel et à des informations supplémentaires qui peuvent être largement dispersés dans différents répertoires. Il est donc difficile pour les clients potentiels de trouver toutes les informations dont ils ont besoin pour évaluer les obligations contractuelles et juridiques des parties et leurs implications.

Dans le cadre du processus de changement de fournisseur, la transparence est très importante. Un client potentiel a besoin d'un accès aisé aux informations, documents, matériels et coordonnées pertinents et actualisés, avant même de conclure un contrat avec le fournisseur. La non-dispersion des CCS assure la symétrie de l'information et de la communication.

Les présentes CCS aident tant le client que le fournisseur à accéder facilement et concrètement à des informations, documents, matériels et coordonnées pertinents et actualisés. Elles visent à créer un environnement de transparence entre les parties et à faire en sorte qu'il n'y ait pas d'obstacles contractuels au changement de fournisseur, en permettant au client de trouver dans l'accord toutes les informations pertinentes et actualisées sur ses droits et obligations. Cela contribuera à l'instauration d'une relation juridique juste et équilibrée entre le client et le fournisseur et, de manière générale, à l'équité contractuelle, ainsi que le préconise le règlement (UE) 2023/285 (ci-après le «règlement sur les données»).

D'autres clauses contractuelles standards recommandées par la Commission figurent en annexe et couvrent des sujets spécifiques autres que la dispersion. Les parties sont encouragées à envisager d'utiliser également ces autres clauses, étant donné qu'elles ont été élaborées pour être cohérentes et se renforcer mutuellement.

1. **Non-dispersion**

1.1. **Conditions introductives et modalités**

1.1.1. Le fournisseur veille à ce que tous les accords contractuels soient facilement, immédiatement et constamment disponibles et accessibles pour le client a) dans un espace en ligne sécurisé et réservé à cet effet, et b) dans un format compréhensible et lisible tant par l'homme que par la machine. En outre, le fournisseur veille à ce que les modalités contractuelles soient téléchargeables ou exportables d'une autre manière pour le client, de manière complète et structurée.

1.1.2. Les modalités contractuelles doivent comprendre au minimum:

(a) **les nom et adresse:** la raison sociale officielle complète du fournisseur en tant qu'entité juridique, comprenant, sans s'y limiter, sa forme juridique officielle, son numéro d'enregistrement national, son adresse officielle complète, et son numéro d'immatriculation à la TVA;

(b) **l'accord actualisé:** l'accord en vigueur et horodaté (ainsi que, le cas échéant, les copies revêtues de la formule exécutoire), comprenant l'ensemble des termes, offres acceptées, conditions, politiques, informations, documents, calendriers, pièces et annexes qui sont applicables entre le fournisseur et le client;

(c) **l'historique:** l'historique des contrats horodatés, accompagné, si possible, des termes et conditions connexes, comprenant les politiques, informations, documents, calendriers, pièces, annexes ou autres éléments qui ont été applicables entre le fournisseur et le client

i) y compris la preuve des modifications unilatérales autorisées et les dates d'entrée en vigueur respectives des modifications unilatérales autorisées, telles que fixées par les CCS relatives à la non-modification.

En ce qui concerne les modifications unilatérales autorisées et les dates d'entrée en vigueur respectives, voir les CCS relatives à la non-modification.

(d) **traitement de données et écosystème de la fourniture de données:** l'historique actualisé et la liste détaillée des entreprises sous-traitantes, des sous-traitants de données et/ou des autres parties prenantes pertinentes du fournisseur intervenant dans l'écosystème de la chaîne d'approvisionnement, y compris les noms et adresses mentionnés à la clause 1.1.2 a) ci-dessus;

(e) **coordonnées:** les coordonnées en vigueur du fournisseur, y compris les informations relatives aux fonctions du contact principal, du contact technique principal et du contact administratif et contractuel principal, comprenant les intitulés de fonction, numéros de téléphone et adresses électroniques respectifs convenus par les parties;

(f) **rapports sur la performance opérationnelle:** lorsque cela est techniquement possible, une vue d'ensemble actualisée et historique des rapports sur la performance opérationnelle établis par le fournisseur en ce qui concerne le service fourni et les autres obligations au titre de l'accord; et

(g) **notification:** toute notification légale et autre notification horodatée pertinente échangée entre les parties ou adressée à une partie concernant les modalités contractuelles visées à la clause 1.1.2, points a) et b).

Dans plusieurs situations, le règlement sur les données oblige le fournisseur à communiquer les informations requises au client. Ces obligations sont prises en compte dans les CCS respectives. Par exemple, des informations concernant les procédures disponibles pour le changement de fournisseur et le transfert de données (article 26 du règlement sur les données) sont incluses dans les CCS relatives au changement de fournisseur et à la sortie; l'obligation de fournir des informations claires concernant les risques connus pour la poursuite de la fourniture de fonctions/services se reflète dans les CCS relatives à la sécurité et à la continuité des activités, ainsi que dans les CCS relatives au changement de fournisseur et à la sortie.

1.2. **Ordre de priorité**

En cas de conflit ou d'incohérence entre les présentes clauses relatives à la non-dispersion de la documentation contractuelle applicable et toutes autres dispositions contractuelles, modalités ou conditions applicables ou tout autre accord applicable en rapport avec le thème des présentes clauses, ces dernières prévaudront.

ANNEXE X

CLAUSES CONTRACTUELLES STANDARDS

relatives à la responsabilité

Bien qu'une clause relative à la responsabilité soit généralement incluse dans l'accord général conclu par le client et le fournisseur, les dispositions des présentes CCS relatives à la responsabilité reflètent l'esprit du règlement (UE) 2023/2854 (ci-après le «règlement sur les données») en ce qui concerne l'importance de droits et d'obligations équitables, raisonnables et non discriminatoires et, à ce titre, peuvent constituer un complément utile aux dispositions types d'un accord sur la responsabilité.

Par conséquent, l'inclusion d'une telle clause est recommandée car elle est essentielle à l'équilibre de la relation contractuelle liant les parties et incite au respect des droits et obligations convenus par les parties. En particulier, les petites et moyennes entreprises ainsi que d'autres organisations peuvent trouver les présentes CCS utiles lorsqu'elles conviennent dans leurs accords de dispositions en matière de responsabilité. Le client et le fournisseur sont libres de convenir dans leur contrat de droits et d'obligations supplémentaires. L'utilisation de la présente clause ne dispense pas les parties de veiller au respect des dispositions contraignantes applicables du droit de l'Union ou du droit national et d'adapter les clauses en conséquence.

Avant de conclure un accord, le client peut vérifier sur le marché de l'assurance le produit d'assurance le plus approprié à ses besoins. Il est recommandé de demander le conseil d'un expert spécialisé en matière d'assurance.

D'autres clauses contractuelles standards recommandées par la Commission figurent en annexe et couvrent des sujets spécifiques autres que la responsabilité. Les parties sont encouragées à envisager d'utiliser également ces autres clauses, étant donné qu'elles ont été élaborées de façon à être cohérentes et à se renforcer mutuellement.

Responsabilité illimitée

En règle générale, la responsabilité de chaque partie à l'accord devrait être illimitée en cas d'intention délictueuse, d'inconduite délibérée ou de négligence grave, y compris en cas de manquement d'une partie aux obligations de confidentialité des données de l'autre partie ou à l'obligation de ne pas utiliser les données à des fins autres que celles expressément convenues par les parties.

Les CCS recommandent de distinguer les cas où la violation est intentionnelle de ceux où elle est causée par une inconduite délibérée, et de préciser que tous les actes intentionnels sont couverts, quelle que soit la législation régissant le contrat. Dans certaines juridictions, l'inconduite délibérée peut être synonyme d'intention délictueuse. En pareils cas, les parties peuvent décider de ne pas faire de distinction entre inconduite délibérée et intention délictueuse.

Dérogations à la responsabilité illimitée

Les services de traitement de données fournis en tant que versions non destinées à la production à des fins d'essai et d'évaluation et pour une durée limitée (article 31, paragraphe 2, du règlement sur les données) ne sont généralement pas destinés au traitement de données sensibles (par exemple, les secrets d'affaires, les données à caractère personnel ou les données de production réelles). En outre, ces versions non destinées à la production ne sont généralement pas suffisamment développées pour ce type de traitement et ne sont pas dotées des capacités, des contrôles et de la configuration que l'on pourrait raisonnablement attendre de la version destinée à la production. Le client est fortement encouragé à ne pas traiter des données de production réelles dans les versions non destinées à la production. Il est proposé dans les présentes CCS que, si le client décide de traiter de telles données, cette opération se fasse à ses propres risques et que le fournisseur ne soit pas responsable en cas de violation de la confidentialité des données en pareilles circonstances. Dans ce cas, des dispositions spécifiques en matière de responsabilité convenues entre les parties peuvent s'appliquer.

De même, le règlement sur les données envisage des situations dans lesquelles certaines obligations ne s'appliquent pas aux services lorsque la majorité des caractéristiques principales ont été conçues sur mesure ou que tous les composants ont été développés pour les besoins d'un client donné, ou lorsque les services sont fournis dans un environnement non destiné à la production. Par conséquent, la responsabilité applicable en pareils cas devrait également faire l'objet d'un accord explicite.

Responsabilité limitée

Il est de pratique commerciale courante que les parties conviennent de limiter leur responsabilité (en particulier celle du fournisseur) dans certains cas. Les présentes CCS proposent trois grandes options pour la limitation de la responsabilité:

— **Option A:** la responsabilité est limitée au montant déterminé par les parties sur la base d'une évaluation des risques. Dans le cadre de cette option, les deux parties procèdent à une évaluation des risques et communiquent leurs conclusions à l'autre partie au cours de la phase précontractuelle. L'autre partie peut rejeter l'évaluation des risques qu'elle a reçue. Si l'évaluation des risques est rejetée, les parties peuvent appliquer l'une des autres options prévues pour la limitation de la responsabilité.

Il peut y avoir des changements dans le volume des services reçus du fournisseur, ainsi qu'une modification de l'étendue du contrat (ajout de nouveaux services ou suppression de certains services). Cela peut nécessiter d'apporter des modifications à l'évaluation des risques, de sorte que les parties devraient adapter la limite de responsabilité afin de tenir compte de la situation réelle en matière de risques. Les parties sont encouragées à examiner l'exemple fourni dans le modèle d'évaluation des risques proposé dans le cadre de l'option A afin d'être informées des risques pour leur activité particulière qui sont liés aux services de traitement de données.

— **Option B**: la responsabilité est limitée aux dommages directs. Les dommages indirects tels que le manque à gagner ou les économies non réalisées sont exclus. Cette option peut également être combinée avec les options A et C (c'est-à-dire limiter la responsabilité aux dommages directs sans toutefois dépasser le montant fixé par les parties à la suite d'une évaluation des risques ou un montant déterminé sur une autre base).

— **Option C**: la responsabilité des parties est limitée à un montant maximal convenu au préalable, qui peut être calculé, par exemple, sur la base i) de l'équivalent des frais annuels uniques/multiples (payés et dus) par le client au fournisseur; ii) de la couverture d'assurance souscrite par le fournisseur en rapport avec les services; iii) du montant maximal couvert par l'assurance de responsabilité professionnelle générale du fournisseur; ou iv) d'une combinaison de différentes formules, par exemple une formule liée à la valeur monétaire des services multipliée par le montant égal aux frais annuels globaux [payés ou (non encore) dus en vertu de l'accord] pour les services.

Indemnisation: les CCS ne contiennent pas de dispositions relatives à l'indemnisation. Les parties sont encouragées à examiner si et, le cas échéant, dans quelle mesure une partie peut être tenue d'indemniser l'autre partie et de la prémunir contre toute plainte de tiers résultant d'une violation substantielle des obligations découlant de l'accord ou liée à une telle violation du fait d'actes ou d'omissions de la partie responsable, de ses employés, de ses représentants ou de ses sous-traitants. Dans le cas des clients, l'indemnisation peut s'appliquer, par exemple, en cas de violation par le fournisseur de ses obligations de confidentialité ou de non-utilisation des données, ou en cas de violation des droits de propriété intellectuelle de tiers. Dans le cas des fournisseurs, l'indemnisation peut couvrir la violation par le client des droits de propriété intellectuelle de tiers ou les réclamations de tiers auprès du fournisseur concernant l'hébergement de contenus illicites par le client.

1. **Responsabilité**

1.1. **Responsabilité illimitée**

1.1.1. En cas de violation des obligations découlant du présent accord commise intentionnellement ou causée par une inconduite délibérée ou une négligence grave, la partie contrevenante est responsable de l'intégralité des dommages, sous réserve de la clause 1.2 ci-dessous. [OPTION] [Sauf disposition contraire figurant dans la clause 1.2, le fournisseur est responsable sans limitation de tous les dommages causés au client par une violation de la confidentialité des données du client traitées dans le cadre du présent contrat.]

1.1.2. En cas de violation de l'obligation de ne pas utiliser les données d'une partie à des fins autres que celles expressément convenues par les parties, la partie contrevenante est responsable de l'intégralité des dommages, sans limitation.

L'objectif de l'option prévue à la clause 1.1.1 est de garantir la confidentialité de toutes les données du client conformément aux droits et obligations en matière de confidentialité et dans la mesure convenue dans l'accord. En vertu du droit applicable (par exemple, le RGPD, la SRI 2, etc.), un destinataire d'informations confidentielles peut avoir, dans certains cas, l'obligation de divulguer certaines informations à certaines personnes/organisations à des fins convenues et explicitement décrites dans l'accord.

1.2. **Dérogations à la responsabilité illimitée**

1.2.1. Si les parties conviennent d'une responsabilité illimitée conformément à la clause 1.1.1, la responsabilité illimitée du fournisseur ne s'applique pas aux données du client traitées dans une version des services de traitement des données du fournisseur non destinée à la production.

Voir l'article 31, paragraphe 2, du règlement sur les données ainsi que la note explicative «Dérogations à la responsabilité illimitée» des présentes CCS.

1.2.2. Le fournisseur n'est pas responsable:

(a) dans le cas d'obligations non applicables aux services de traitement des données en vertu i) de l'article 23, point d), du règlement sur les données (réalisation de l'équivalence fonctionnelle); ii) de l'article 29 (suppression progressive des frais de changement de fournisseur); ou iii) de l'article 30, paragraphes 1 et 3, du règlement sur les données (aspects techniques du changement de fournisseur) si la majorité des caractéristiques principales des services de traitement de données du fournisseur sont conçues sur mesure pour répondre aux besoins spécifiques du client ou si tous les composants ont été développés pour les besoins du client, et si ces services de traitement de données ne sont pas proposés à grande échelle sur le plan commercial par l'intermédiaire du catalogue de services du fournisseur de services de traitement de données. La dérogation s'applique si le fournisseur a informé le client, avant la conclusion du contrat de services de traitement de données, que les dispositions mentionnées ci-dessus du règlement sur les données ne s'appliquent pas auxdits services;

(b) en cas de violation des obligations liées au changement de fournisseur lors du passage de services de traitement de données vers des services de traitement de données fournis en tant que version non destinée à la production à des fins d'essai et d'évaluation et pour une durée limitée.

1.3. **Responsabilité limitée**

Option A: montant déterminé à l'issue d'une évaluation des risques

1.3.1. Les parties conviennent de limiter leur responsabilité en cas de manquement par négligence aux obligations découlant du présent accord au montant de […] par événement, y compris lorsqu'une série d'événements connexes s'applique en tant qu'événement unique. Le montant est déterminé de bonne foi par la partie lésée sur la base d'une évaluation des risques ou d'autres estimations convenues par les parties à l'annexe 1 (modèle d'évaluation des risques). L'évaluation des risques est effectuée et communiquée à l'autre partie [.... jours] avant la conclusion de l'accord. Si l'évaluation des risques n'est pas rejetée par l'autre partie, l'accord est conclu sur cette base.

Les parties peuvent convenir à tout moment de réévaluer les risques afin de tenir compte de l'évolution de la situation des risques en ce qui concerne les services. À cette fin, elles peuvent utiliser le modèle figurant dans l'exemple [modèle d'évaluation des risques]. Si la réévaluation entraîne une augmentation ou une diminution du risque pour la partie concernée, ladite partie peut demander de négocier le plafond de responsabilité fixé pour les services afin de tenir compte de l'évolution du risque associé à ces services ou de conditions supplémentaires qu'il conviendrait de remplir, lesquelles peuvent porter sur la tarification ou sur les modifications à apporter à l'accord de niveau de service convenu. Les parties pourraient s'entendre sur le fait que, si aucun accord n'est conclu dans un délai de [trois mois à compter de la demande de la partie], le plafond de responsabilité initialement convenu reste inchangé.

Option B: dommages directs

1.3.2. En cas de manquement par négligence aux obligations découlant du présent accord, les parties conviennent de limiter leur responsabilité aux dommages directs causés.

1.3.3. Les dommages directs comprennent également: i) les coûts exposés pour déterminer la cause et l'étendue des dommages; ii) les coûts exposés par la partie lésée afin d'éviter ou de limiter des dommages directs, à condition que ces coûts aient effectivement permis d'éviter ou de limiter ces dommages; iii) les dommages découlant de la corruption, de l'indisponibilité ou de la perte de données; et iv) les coûts supportés par une partie pour faire en sorte que les services respectent les niveaux d'utilisation convenus dans l'accord, dès lors que l'autre partie n'a pas remédié à cette violation dans le délai convenu.

1.3.4. Lorsqu'une série d'événements connexes s'applique en tant qu'événement unique, la responsabilité cumulée de l'une des parties à l'égard de l'autre partie pour ces dommages directs, tels que définis dans la phrase précédente, est limitée au montant de […].

Option C: montant maximal

1.3.5. En cas de manquement par négligence aux obligations découlant du présent accord, y compris lorsqu'une série d'événements connexes s'applique en tant qu'événement unique, les parties conviennent de limiter leur responsabilité à un montant maximal de […].

1.4. **Notifications**

Les parties conviennent que toute notification entre elles concernant les présentes clauses relatives à la responsabilité doit être effectuée [*les parties indiquent les moyens de communication choisis, y compris par des moyens électroniques adéquats*].

1.5. **Ordre de priorité**

En cas de conflit ou d'incohérence entre les présentes clauses relatives à la responsabilité et toutes autres dispositions contractuelles, modalités ou conditions applicables ou tout autre accord applicable en matière de responsabilité relevant des présentes clauses, ces dernières prévaudront.

Appendice 1

Modèle d'évaluation des risques

Afin de déterminer les risques associés au service, une partie procède à une évaluation en tenant compte des risques spécifiques d'inexécution par négligence de la part de l'autre partie dans le cadre de l'accord.

Cette évaluation des risques doit être effectuée de bonne foi. Elle doit refléter de manière réaliste les dommages potentiels. Si les montants estimés sont trop faibles, l'engagement de responsabilité pour des dommages plus élevés sera exclu. Si les montants estimés sont trop élevés, l'autre partie peut refuser d'engager sa responsabilité ou exiger des frais plus élevés.

Des risques supplémentaires peuvent être inclus au besoin.

Description du risque		Estimation du préjudice
Interruption d'activité Perte de chiffre d'affaires causée par une violation du contrat. L'éventuelle interruption des services et les conséquences de cette interruption sur les activités ou les opérations de la partie peuvent être pris envisagées.	EUR	
Récupération des données Coûts estimés pour la récupération des données perdues, indisponibles ou corrompues. Les parties peuvent être tenues de mettre en œuvre des mesures visant à atténuer les risques auxquels elles sont exposées, par exemple en disposant de données de sauvegarde conservées auprès d'un autre fournisseur ou sur site.	EUR	
Amendes infligées par les pouvoirs publics Les amendes infligées par les pouvoirs publics aux entreprises consistent, par exemple, en des amendes pour violation de la législation en matière de protection des données ou de dispositions réglementaires résultant de l'exploitation du service par le fournisseur.	EUR	
Perte de secrets d'affaires La divulgation de secrets d'affaires peut entraîner une perte d'opportunités commerciales. Ces dommages peuvent faire l'objet d'une action judiciaire en réparation.	EUR	
Violation de données à caractère personnel et mesures correctives Une violation de données à caractère personnel peut entraîner plusieurs types de coûts directs liés aux frais juridiques, aux frais de contentieux ainsi qu'aux mesures de réparation des données afin d'éliminer tout problème de qualité des données découlant de la violation.	EUR	
Atteinte à la réputation Les parties peuvent prendre en considération l'atteinte à la réputation de l'entreprise ainsi que les mesures qui seront nécessaires (par exemple, la réalisation de publicités et de campagnes afin de compenser l'atteinte à la réputation). Ces coûts peuvent être difficiles à recouvrer intégralement dans le cadre d'une procédure judiciaire.	EUR	
Responsabilité civile La responsabilité civile couvre la responsabilité potentielle à l'égard, par exemple, de fournisseurs, de clients, de sous-traitants et de tiers.	EUR	
Risque total de dommages potentiels (somme)	**EUR**	

Étant donné que les services de traitement de données sont fournis de manière modulable et variable, tant l'utilisation du service fourni par le fournisseur que la responsabilité potentielle peuvent varier au cours de l'accord, souvent dans la fourchette fixée dans les accords de niveau de service. Lors de l'évaluation des risques, qu'elle soit réalisée à la conclusion de l'accord ou sur une base récurrente, il est conseillé aux parties de tenir compte de l'évolution de la nature et du volume des services en plus du préjudice théorique maximal potentiel. Une valeur plus réaliste pourrait ainsi être obtenue pour l'utilisation moyenne ou pour l'utilisation prévue du service. Les parties devraient également aligner l'évaluation sur leur planification interne. Il se peut que les catégories de risques énumérées ne s'appliquent pas toutes de la même manière à un client et à un fournisseur ou à une ligne d'activité spécifique d'un client.

ANNEXE XI

CLAUSES CONTRACTUELLES STANDARDS

relatives à la non-modification

Il importe que les parties puissent se fonder sur les droits et obligations convenus contractuellement et que ces droits et obligations ne soient pas modifiés unilatéralement, si ce n'est dans le cadre de conditions définies de manière claire et d'un commun accord. Cela est particulièrement vrai pour les petites et moyennes entreprises ou autres organisations qui peuvent ne pas disposer de ressources suffisantes pour évaluer l'incidence possible de ces modifications unilatérales sur leurs activités ou leur mission. Les CCS relatives à la non-modification visent à procurer plus de clarté et de confiance aux parties lorsqu'elles conviennent des conditions régissant les modifications unilatérales. Les présentes clauses contractuelles standards couvrent des scénarios pertinents ainsi que les éventuelles modalités contractuelles qui y sont associées. Elles visent à garantir que ces modifications unilatérales ne portent pas atteinte aux intérêts de l'une ou de l'autre des parties.

Approche concernant les modifications unilatérales

En règle générale, l'accord (y compris les CCS) ne peut être modifié unilatéralement par l'une ou l'autre des parties et doit faire l'objet d'un consensus. Ce n'est que sous certaines conditions strictes, telles que prévues dans les présentes CCS, que certaines modifications unilatérales sont autorisées. Ce principe se reflète dans les clauses 1.1.1 à 1.1.3 des présentes CCS.

Ces CCS reconnaissent que, dans certaines circonstances, le fournisseur devrait être en mesure de proposer unilatéralement que des modifications soient apportées aux services fournis. Ces modifications sont appelées «modifications unilatérales autorisées» et sont énoncées dans les clauses 1.1.3 à 1.1.6 des présentes CCS. Une ou plusieurs modifications unilatérales autorisées ne peuvent être proposées qu'une seule fois et doivent remplir les conditions suivantes:

(1) elle améliore/elles améliorent la situation du client en lien avec l'utilisation du service, tant sur le plan contractuel, financier, organisationnel et opérationnel qu'en ce qui concerne le niveau du service, la conformité juridique ou d'autres points de vue; et

(2) elle est notifiée/elles sont notifiées au client au plus tard 30 jours calendaires avant que la ou les modifications unilatérales autorisées proposées ne soient effectives pour le client.

Le délai de notification permettra au client d'évaluer les informations et la faisabilité ainsi que l'incidence tant pour le client que pour les parties prenantes, les systèmes et les services du client.

D'autres clauses contractuelles standards recommandées par la Commission figurent en annexe et portent sur des sujets spécifiques autres que la non-modification. Les parties sont encouragées à envisager d'utiliser également ces autres clauses, étant donné qu'elles ont été élaborées de façon à être cohérentes et à se renforcer mutuellement.

1. **Non-modification**

1.1. **Modification**

1.1.1. Toute modification de l'accord (ci-après la «modification») doit être effectuée par écrit, y compris par des moyens électroniques adéquats, et sera soumise à un consentement mutuel préalable, y compris par des moyens électroniques adéquats.

1.1.2. Nonobstant la clause 1.1.1, le fournisseur est autorisé à modifier l'accord si cela est nécessaire pour se conformer aux dispositions du droit applicable obligatoire qui n'étaient pas encore en vigueur avant la date effective d'entrée en vigueur de l'accord.

1.1.3. Sous réserve des dispositions de la clause 1.1.2, le fournisseur n'est autorisé à proposer une modification unilatérale aux services que si:

(a) cette modification est bénéfique pour l'utilisation par le client des services de traitement de données, par exemple parce qu'elle consiste en des mises à jour permettant d'améliorer sensiblement le service ou parce qu'elle est nécessaire pour des raisons de sécurité; et

(b) toutes les conditions énoncées dans les clauses 1.1.4 à 1.1.6 («Modification unilatérale autorisée») sont remplies.

1.1.4. Aucune modification unilatérale proposée au titre de la clause 1.1.3 ne peut être utilisée par le fournisseur pour mettre en œuvre ou appliquer, directement ou indirectement, des modifications rétroactives, ou pour modifier des clauses de l'accord relatives à un ou plusieurs des aspects suivants:

(a) le choix du droit applicable ou la clause attributive de compétence;

(b) les modifications ou la procédure de modification de l'accord;

(c) la durée et la résiliation;

(d) la responsabilité;

(e) la confidentialité;

(f) les méthodes régissant le recours à la sous-traitance ou le changement de sous-traitants;

(g) les droits d'accès et en matière d'information;

(h) les objectifs qualitatifs du niveau de service;

Des modifications concernant des objectifs de performance du service quantitatifs et qualitatifs déjà approuvés dans le cadre des niveaux de service convenus, assortis de pénalités et/ou de crédits de service, peuvent être proposées en tant que modification unilatérale autorisée conformément à la clause 1.1.3.

(i) les règles de tarification ou autres règles financières;

Une modification des frais convenus peut être proposée en tant que modification unilatérale autorisée conformément à la clause 1.1.3, mais les règles sous-jacentes, telles que la méthode d'indexation des prix, doivent elles-mêmes être convenues d'un commun accord entre les parties.

(j) l'espace où les données sont traitées ou stockées si cet espace se situe en dehors de l'UE.

Des modifications entre différents espaces de l'UE peuvent être convenues par les parties dès le début de leur relation contractuelle ou peuvent être proposées par le fournisseur en tant que modification unilatérale autorisée. Toutefois, lorsque l'espace où les données sont traitées ou stockées passe d'un emplacement situé dans l'UE à un emplacement situé en dehors de l'UE ou d'un emplacement situé en dehors de l'UE à un autre emplacement situé en dehors de l'UE, les parties devraient convenir mutuellement de ce changement.

1.1.5. En cas de proposition de modification unilatérale autorisée, le fournisseur est tenu:

(a) d'informer le client au plus tard 30 jours calendaires, sauf disposition contraire du droit applicable, avant que la proposition de modification unilatérale autorisée ne prenne effet;

(b) de fournir au client, de manière claire et compréhensible, des informations comprenant:

i) la portée, les modalités et le calendrier de la modification unilatérale autorisée proposée;

ii) les raisons pour lesquelles la modification unilatérale autorisée proposée est nécessaire, y compris en ce qui concerne les effets positifs pour l'utilisation par le client des services de traitement des données;

iii) la différence entre la situation actuelle et la situation en vigueur après la modification unilatérale autorisée proposée. Cela inclut, en particulier, toute conséquence éventuelle pour le client sur le plan contractuel, financier, organisationnel ou opérationnel, ainsi que toute conséquence liée au niveau de service et à la conformité juridique;

La description de cette différence devrait englober la situation prévue pour les types de clients existants concernés, en tenant compte des catégories indiquées à la clause 1.1.5 b) iii). Il s'agit de veiller à ce que les conséquences les plus probables d'une modification unilatérale notifiée soient visibles et comprises par le client. À cet égard, cette clause n'impose pas au fournisseur de notifier une modification adaptée aux différents clients.

iv) le calendrier envisagé pour le déploiement et la mise en œuvre, ainsi que la date effective d'entrée en vigueur de la modification unilatérale autorisée proposée.

1.1.6. Si le fournisseur remplit les conditions énoncées à la clause 1.1.5, le client sera réputé avoir accepté la modification unilatérale autorisée proposée à la date d'entrée en vigueur de la modification unilatérale autorisée.

1.1.7. Si le fournisseur enfreint les clauses 1.1.2 à 1.1.5 en ce qui concerne la modification de l'accord, le client aura le droit de résilier l'accord sans frais supplémentaires et d'obtenir réparation pour le préjudice subi (y compris pour les coûts liés au changement de fournisseur de services de traitement de données). Cela n'affecte pas les autres droits et voies de recours dont bénéficie le client, y compris en ce qui concerne la demande de mesures injonctives devant toute juridiction compétente applicable afin d'ordonner au fournisseur de continuer à fournir les services comme convenu et afin d'obtenir réparation pour le préjudice subi, le cas échéant.

Si la modification de l'accord par le fournisseur n'est pas conforme aux dispositions contractuelles, le client devrait avoir le droit de résilier l'accord, ce qui, dans la pratique, devrait également impliquer la notification d'un changement de fournisseur afin de lancer le processus de changement (voir les CCS relatives au changement de fournisseur et à la sortie, option A, si les parties ont convenu d'un plan de changement de fournisseur et de sortie, et option B, en cas de changement de fournisseur automatique en libre-service). Toutefois, en pareils cas, le client devrait avoir le droit d'être dédommagé pour le préjudice subi du fait de l'«obligation» de changer de fournisseur, y compris pour les coûts qu'il a supportés et les autres dommages connexes (voir les CCS relatives à la responsabilité).

1.2. **Notifications**

Les parties conviennent de toute notification à effectuer entre elles concernant les présentes clauses relatives à la non-modification [*les parties indiquent les moyens de communication choisis, y compris par des moyens électroniques adéquats*].

1.3. **Ordre de priorité**

En cas de conflit ou d'incohérence entre les présentes clauses relatives à la non-modification et toutes autres dispositions contractuelles, modalités ou conditions applicables ou tout autre accord applicable relatifs aux modifications apportées à l'accord au titre des présentes clauses, ces dernières prévaudront.

ANNEXE XII

CLAUSES CONTRACTUELLES STANDARDS

définitions

Aux fins des présentes CCS, les termes utilisés seront définis comme suit:

«accord»: l'accord écrit conclu entre les parties en ce qui concerne la fourniture de services, ou toute modification ou tout complément apporté à cet accord, ainsi que tous les actes liés à l'exécution du ou des accords, y compris, en particulier, les appendices respectifs;

«appendice»: un appendice, un échéancier ou toute pièce explicitement mentionnée dans l'accord;

«client de service de traitement de données (client)», au sens de l'article 2, point 30), du règlement sur les données: une personne physique ou morale qui a noué une relation contractuelle avec un fournisseur de services de traitement de données dans le but d'utiliser un ou plusieurs services de traitement de données;

«données», au sens de l'article 2, point 1), du règlement sur les données: toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels;

«règlement sur les données»: le règlement (UE) 2023/2854;

«frais de transfert des données», au sens de l'article 2, point 35), du règlement sur les données: les frais de transfert de données facturés aux clients pour l'extraction de leurs données au moyen du réseau depuis l'infrastructure TIC d'un fournisseur de services de traitement de données vers le système d'un fournisseur différent ou vers une infrastructure TIC sur site;

«service de traitement de données», au sens de l'article 2, point 8), du règlement sur les données: un service numérique qui est fourni à un client et qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services. Aux fins du présent accord, lesdits services de traitement de données concernent les services fournis ou à fournir par le fournisseur au client, tels que convenus dans le cadre de l'accord;

«fournisseur de destination», au sens de l'article 2, point 34), du règlement sur les données: le fournisseur de destination de services de traitement de données vers lequel se tourne le client de services de traitement de données afin d'utiliser soit un autre service de traitement de données du même type de service, soit d'autres services;

«fournisseur d'origine», au sens de l'article 2, point 34), du règlement sur les données: l'entité juridique avec laquelle le client a noué une relation contractuelle concernant la fourniture de services de traitement de données et d'autres services par le fournisseur en vertu de l'accord, et dont le client souhaite à présent se défaire pour se tourner vers un autre fournisseur;

«actifs numériques», au sens de l'article 2, point 32), du règlement sur les données: des éléments en format numérique, y compris des applications, pour lesquels le client est titulaire du droit d'utilisation, indépendamment de la relation contractuelle que le client a avec le service de traitement de données qu'il a l'intention de quitter;

«données exportables», au sens de l'article 2, point 38), du règlement sur les données: les données d'entrée et de sortie, y compris les métadonnées, générées directement ou indirectement, ou cogénérées, par l'utilisation par le client du service de traitement de données, à l'exclusion des actifs ou des données protégés par des droits de propriété intellectuelle, ou constituant un secret d'affaires, des fournisseurs de services de traitement de données ou des tiers;

«incident»: une atteinte à la sécurité physique, technique ou organisationnelle, un incident ou un événement similaire susceptible d'avoir une incidence significative sur la sécurité et la continuité des activités, dans la mesure où cela a entraîné ou est susceptible d'entraîner une perturbation grave de tout système ou de toute opération informatiques applicables utilisés entre le fournisseur et le client au cours du processus de changement de fournisseur, ou sur l'utilisation des services par le client des services, ainsi que sur les données exportables et les actifs numériques du client. Voir les CCS relatives à la sécurité et à la continuité des activités;

«interopérabilité», au sens de l'article 2, point 40), du règlement sur les données: la capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits connectés, applications, services de traitement de données ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions;

«métadonnées», au sens de l'article 2, point 2), du règlement sur les données: une description structurée du contenu ou de l'utilisation des données qui facilite la découverte ou l'utilisation de ces données;

«données à caractère non personnel», au sens de l'article 2, point 4), du règlement sur les données: les données autres que les données à caractère personnel;

«infrastructure TIC sur site», au sens de l'article 2, point 33), du règlement sur les données: une infrastructure TIC et des ressources informatiques qui appartiennent au client, qu'il loue ou qu'il utilise en crédit-bail, situées dans le centre de données du client lui-même et exploitées par le client ou par un tiers;

«autres services»: tous les services professionnels de quelque nature que ce soit fournis par le fournisseur au client en vertu de l'accord tels qu'ils y sont définis, qui ne sont pas des services de traitement de données;

«partie»: le client ou le fournisseur;

«parties», le client et le fournisseur;

«données à caractère personnel», au sens de l'article 4, point 1), du règlement (UE) 2016/679 [règlement général sur la protection des données (RGPD)];

«plan»: le plan de changement de fournisseur et de sortie mentionné dans l'option A des CCS relatives au changement de fournisseur et à la sortie, tel que convenu entre les parties dans le cadre de l'accord;

«traitement», au sens de l'article 2, point 7), du règlement sur les données: toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou à des ensembles de données, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou d'autres moyens de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

«fournisseur de services de traitement de données (fournisseur)»: une personne physique ou morale qui a noué une relation contractuelle avec un client dans le but de fournir un ou plusieurs services de traitement de données;

«même type de service», au sens de l'article 2, point 9), du règlement sur les données: un ensemble de services de traitement de données qui partagent le même objectif principal, le même modèle de service de traitement de données et les principales fonctionnalités;

«services»: les services de traitement de données ainsi que tous les autres services convenus par les parties dans le cadre de l'accord;

«frais de service»: les frais dus par le client au fournisseur en contrepartie de la fourniture de services convenus par les parties dans le cadre de l'accord;

«changement de fournisseur», au sens de l'article 2, point 34), du règlement sur les données: le processus impliquant un fournisseur d'origine de services de traitement de données, un client d'un service de traitement de données et, le cas échéant, un fournisseur de destination de services de traitement de données, par lequel le client d'un service de traitement de données passe de l'utilisation d'un service de traitement de données à l'utilisation d'un autre service de traitement de données du même type de service, ou un autre service, proposé par un fournisseur de services de traitement de données différent, ou à une infrastructure TIC sur site, y compris par l'extraction, la transformation et le téléversement des données;

«frais de changement de fournisseur», au sens de l'article 2, point 36), du règlement sur les données: les frais, autres que les frais de service standards ou les pénalités de résiliation anticipée, imposés par un fournisseur de services de traitement de données à un client pour les actions requises par le règlement sur les données pour changer de fournisseur en passant au système d'un fournisseur différent ou à une infrastructure TIC sur site, y compris les frais de transfert des données.