COMMISSION
EUROPÉENNE

Bruxelles, le 13.5.2022
COM(2022) 208 final

ANNEX

ANNEXE

de la

Proposition de

DÉCISION DU CONSEIL

relative à la conclusion de l'accord entre l'Union européenne, d'une part, et la Nouvelle-Zélande, d'autre part, sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités néo-zélandaises compétentes pour lutter contre les formes graves de criminalité et le terrorisme

ANNEXE

L'UNION EUROPÉENNE, ci-après également dénommée «Union» ou «UE»,

et

la Nouvelle-Zélande,

ci-après les «parties contractantes»,

considérant ce qui suit:

(1) En permettant l'échange de données à caractère personnel entre Europol et les autorités néo-zélandaises compétentes, le présent accord créera le cadre d'une coopération opérationnelle renforcée entre l'Union européenne et la Nouvelle-Zélande dans le domaine répressif, tout en préservant les droits de l'homme et les libertés fondamentales de toutes les personnes concernées, y compris la protection de la vie privée et des données.

(2) Le présent accord est sans préjudice des arrangements en matière d'entraide judiciaire conclus entre la Nouvelle-Zélande et les États membres de l'UE autorisant l'échange de données à caractère personnel.

(3) Le présent accord n'impose aux autorités compétentes aucune obligation de transférer des données à caractère personnel. Le partage de toutes les données à caractère personnel demandées en vertu du présent accord demeure volontaire.

(4) L'accord reconnaît que les parties appliquent des principes comparables de proportionnalité et du caractère raisonnable. L'essence commune à ces principes consiste à assurer un juste équilibre entre tous les intérêts concernés, qu'ils soient publics ou privés, à la lumière de toutes les circonstances de l'espèce. Cet équilibre doit être trouvé entre, d'une part, le droit des personnes au respect de la vie privée ainsi que d'autres droits de l'homme et intérêts humains et, d'autre part, les objectifs légitimes pouvant être poursuivis, tels que les finalités du traitement des données à caractère personnel visées dans le présent accord.

sont convenues de ce qui suit:

CHAPITRE I – DISPOSITIONS GENERALES

Article premier
Objectif

L'objectif du présent accord est de permettre le transfert de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités néo-zélandaises compétentes, afin d'appuyer et de renforcer l'action des autorités des États membres de l'Union européenne et de celles de la Nouvelle-Zélande, ainsi que leur coopération mutuelle dans la prévention et la répression des infractions pénales, en particulier contre les formes graves de criminalité et le terrorisme, tout en offrant des garanties appropriées concernant les droits de l'homme et les libertés fondamentales des personnes, y compris la protection de la vie privée et des données.

Article 2
Définitions

Aux fins du présent accord, on entend par:

a) «parties contractantes», d'une part, l'Union européenne et, d'autre part, la Nouvelle-Zélande;

b) «Europol», l'Agence de l'Union européenne pour la coopération des services répressifs, créée en vertu du règlement (UE) 2016/794[1] ou de toute modification apportée à celui-ci (ci-après dénommé le «règlement Europol»);

c) «autorité compétente», pour la Nouvelle-Zélande, les autorités répressives nationales chargées, en vertu du droit national néo-zélandais, de prévenir et de réprimer les infractions pénales énumérées à l'annexe II du présent accord (ci-après dénommées les «autorités néo-zélandaises compétentes») et, pour l'Union européenne, Europol;

d) «organes de l'Union», les institutions, organes, missions, bureaux et agences institués par le traité sur l'Union européenne et le traité sur le fonctionnement de l'Union européenne ou sur la base de ces traités, tels qu'énumérés à l'annexe III;

e) «infractions pénales», les formes de criminalité énumérées à l'annexe I et les infractions pénales connexes. Les infractions pénales sont considérées comme connexes aux formes de criminalité énumérées à l'annexe I si elles sont commises pour se procurer les moyens de commettre ces formes de criminalité, pour faciliter ou commettre ces dernières, ou pour assurer l'impunité des auteurs de ces formes de criminalité;

f) «données à caractère personnel», toute information se rapportant à une personne concernée;

g) «personne concernée», une personne physique identifiée ou identifiable, une «personne identifiable» étant une personne 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

[1] On entend par «règlement (UE) 2016/794» le règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI; JO L 135 du 24.5.2016, p. 53.

plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

h) «données génétiques», toutes les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique, et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

i) «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, 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 toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

j) «informations», les données à caractère personnel;

k) «violation de données à caractère personnel», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à celles-ci;

l) «autorité de contrôle», une ou plusieurs autorités nationales indépendantes qui sont, ensemble ou séparément, responsables de la protection des données au sens de l'article 16 du présent accord et qui ont été notifiées conformément audit article. Il peut s'agir d'autorités dont la responsabilité couvre également d'autres droits de l'homme;

m) «organisation internationale», une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.

Article 3
Finalités du traitement des données à caractère personnel

1. Les données à caractère personnel demandées et reçues au titre de l'accord ne sont traitées qu'à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, dans les limites de l'article 4, paragraphe 5, et des mandats respectifs des autorités compétentes.

2. Les autorités compétentes indiquent clairement, au plus tard au moment du transfert des données à caractère personnel, la ou les finalités spécifiques pour lesquelles ces données sont transférées. Pour les transferts à Europol, la ou les finalités sont précisées conformément aux finalités spécifiques du traitement énoncées dans le mandat d'Europol.

CHAPITRE II – ÉCHANGE D'INFORMATIONS ET PROTECTION DES DONNEES

Article 4
Principes généraux en matière de protection des données

1. Chaque partie contractante prévoit que les données à caractère personnel échangées dans le cadre du présent accord sont:

   a) traitées loyalement, licitement et pour la seule finalité pour laquelle elles ont été transférées conformément à l'article 3;

   b) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées;

   c) exactes et tenues à jour; Chaque partie contractante veille à ce que ses autorités compétentes prennent toutes les mesures raisonnables pour que les données à caractère personnel inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans retard indu;

   d) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées;

   e) traitées de manière à leur assurer un niveau de sécurité approprié.

2. L'autorité compétente effectuant le transfert peut indiquer, au moment du transfert de données à caractère personnel, toute limitation de l'accès à celles-ci ou de l'utilisation de celles-ci, en termes généraux ou spécifiques, y compris en ce qui concerne leur transfert ultérieur, leur effacement ou leur destruction après un certain laps de temps, ou leur traitement ultérieur. Lorsque la nécessité d'appliquer de telles limitations apparaît après la fourniture des informations, l'autorité compétente effectuant le transfert en informe l'autorité destinataire.

3. Chaque partie contractante veille à ce que l'autorité compétente destinataire respecte toute limitation de l'accès aux données à caractère personnel ou de l'utilisation ultérieure de celles-ci indiquée par l'autorité compétente effectuant le transfert comme indiqué au paragraphe 2.

4. Chaque partie contractante veille à ce que ses autorités compétentes mettent en œuvre les mesures techniques et organisationnelles appropriées de manière à pouvoir démontrer que le traitement des données sera conforme au présent accord et que les droits des personnes concernées sont protégés.

5. Chaque partie contractante veille à ce que ses autorités compétentes ne transfèrent pas les données à caractère personnel obtenues en violation manifeste des droits de l'homme reconnus par les normes du droit international qui sont contraignantes pour les parties contractantes. Chaque partie contractante veille à ce que les données à caractère personnel reçues ne soient pas utilisées pour demander, prononcer ou mettre à exécution une condamnation à la peine de mort ou toute forme de traitement cruel et inhumain.

6. Chaque partie contractante veille à ce que soit tenu un relevé de tous les transferts de données à caractère personnel effectués en vertu du présent accord ainsi que de la ou des finalités desdits transferts.

Article 5
Catégories particulières de données à caractère personnel et différentes catégories de personnes concernées

1. Le transfert de données à caractère personnel concernant des victimes d'infraction pénale, des témoins ou d'autres personnes pouvant fournir des informations sur des infractions pénales, ou concernant des personnes de moins de dix-huit ans, est interdit, sauf s'il est strictement nécessaire, raisonnable et proportionné, dans des cas particuliers, pour prévenir ou réprimer une infraction pénale.

2. Le transfert de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, ainsi que le transfert de données génétiques, de données biométriques afin d'identifier une personne physique de manière unique, de données concernant la santé ou de données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont autorisés uniquement s'ils sont strictement nécessaires, raisonnables et proportionnés, dans des cas particuliers, pour prévenir et ou réprimer une infraction pénale et si ces données, à l'exception des données biométriques, complètent d'autres données à caractère personnel.

3. Les parties contractantes veillent à ce que le traitement des données à caractère personnel visées aux paragraphes 1 et 2 soit soumis à des garanties appropriées contre les risques spécifiques encourus, y compris à des limitations d'accès, à des mesures de sécurité supplémentaires au sens de l'article 15 et à des limitations des transferts ultérieurs conformément à l'article 7.

Article 6
Traitement automatisé des données à caractère personnel

Les décisions fondées exclusivement sur le traitement automatisé des données à caractère personnel échangées, y compris sur le profilage, sans intervention humaine, qui peuvent produire des effets juridiques défavorables à l'égard de la personne concernée ou l'affecter de manière significative sont interdites, sauf si elles sont autorisées par la loi à des fins de prévention ou de répression d'une infraction pénale et si elles offrent des garanties appropriées concernant les droits et libertés de la personne concernée, dont au minimum le droit d'obtenir une intervention humaine.

Article 7
Transfert ultérieur des données à caractère personnel reçues

1. La Nouvelle-Zélande veille à ce que ses autorités compétentes ne transfèrent les données à caractère personnel reçues dans le cadre du présent accord à d'autres autorités néo-zélandaises que si:

   a) Europol a donné son accord explicite préalable;

b) la finalité du transfert ultérieur est identique à la finalité initiale du transfert effectué par Europol ou, dans les limites de l'article 3, paragraphe 1, est directement liée à cette finalité initiale; et

c) les transferts ultérieurs sont soumis aux mêmes conditions et garanties que celles qui s'appliquent au transfert initial.

2. Sans préjudice de l'article 4, paragraphe 2, aucune autorisation préalable n'est requise lorsque l'autorité destinataire est elle-même une autorité compétente néo-zélandaise. Il en va de même pour Europol, qui peut partager des données à caractère personnel avec les autorités chargées, dans les États membres de l'Union européenne, de la prévention et de la répression des infractions pénales, et avec les organes de l'Union énumérés à l'annexe III.

3. La Nouvelle-Zélande veille à ce que les transferts ultérieurs de données à caractère personnel reçues par ses autorités compétentes en vertu du présent accord aux autorités d'un pays tiers ou à une organisation internationale soient interdits, sauf si les conditions suivantes sont remplies:

a) le transfert concerne des données à caractère personnel autres que celles relevant de l'article 5 de l'accord;

b) Europol a donné son accord explicite préalable;

c) la finalité du transfert ultérieur est identique à la finalité initiale du transfert effectué par Europol; et

d) les transferts ultérieurs sont soumis aux mêmes conditions et garanties que celles qui s'appliquent au transfert initial.

4. Europol ne peut donner son accord visé au paragraphe 3, point b), pour un transfert ultérieur à l'autorité d'un pays tiers ou à une organisation internationale que si et dans la mesure où il existe une décision d'adéquation, un accord international offrant des garanties appropriées concernant la protection de la vie privée et des libertés et droits fondamentaux des personnes, un accord de coopération ou tout autre fondement juridique futur au transfert de données à caractère personnel au sens du règlement Europol couvrant le transfert ultérieur.

5. L'Union européenne veille à ce que les transferts ultérieurs de données à caractère personnel reçues par Europol en vertu du présent accord à des organes de l'Union européenne non énumérés à l'annexe III, à des autorités de pays tiers ou à une organisation internationale soient interdits, sauf si:

a) le transfert concerne des données à caractère personnel autres que celles relevant de l'article 5 de l'accord;

b) la Nouvelle-Zélande a donné son accord explicite préalable;

c) la finalité du transfert ultérieur est identique à la finalité initiale du transfert effectué par la Nouvelle-Zélande; et

d) une décision d'adéquation, un accord international prévoyant des garanties appropriées en ce qui concerne la protection de la vie privée et des libertés et droits fondamentaux des personnes, ou un accord de coopération au sens du règlement Europol est en vigueur avec ce pays tiers ou cette organisation internationale.

Article 8
Évaluation de la fiabilité de la source et de l'exactitude des informations

1. Les autorités compétentes indiquent dans la mesure du possible, au plus tard lors du transfert des informations, la fiabilité de la source des informations, sur la base d'un ou plusieurs des critères suivants:

   1) il n'existe aucun doute quant à l'authenticité, à la fiabilité et à la compétence de la source, ou l'information provient d'une source qui, dans le passé, s'est révélée fiable dans tous les cas;

   2) l'information provient d'une source dont les informations reçues se sont révélées fiables dans la plupart des cas;

   3) l'information provient d'une source dont les informations reçues se sont révélées non fiables dans la plupart des cas;

   4) la fiabilité de la source ne peut être évaluée.

2. Les autorités compétentes indiquent dans la mesure du possible, au plus tard lors du transfert des informations, l'exactitude des informations, sur la base d'un ou de plusieurs des critères suivants:

   1) l'exactitude de l'information ne fait aucun doute au moment du transfert;

   2) la source a eu directement connaissance de l'information, mais le fonctionnaire qui la transmet n'en a pas eu directement connaissance;

   3) la source n'a pas eu directement connaissance de l'information, mais celle-ci est corroborée par d'autres informations déjà enregistrées;

   4) la source n'a pas eu directement connaissance de l'information et celle-ci ne peut être corroborée d'aucune manière.

3. Lorsque, sur la base d'informations déjà en sa possession, l'autorité compétente destinataire arrive à la conclusion qu'il y a lieu de corriger l'évaluation de l'information ou de sa source fournie par l'autorité compétente qui la transfère, conformément aux paragraphes 1 et 2, elle en informe cette autorité et cherche à s'entendre avec elle sur la modification à apporter à l'évaluation. L'autorité compétente destinataire ne modifie pas l'évaluation de l'information reçue ou de sa source sans cet accord.

4. Si une autorité compétente reçoit des informations non assorties d'une évaluation, elle s'efforce, dans la mesure du possible et si possible en accord avec l'autorité compétente qui les a transférées, d'évaluer la fiabilité de la source ou l'exactitude des informations sur la base des informations déjà en sa possession.

5. Si aucune évaluation fiable ne peut être réalisée, les informations sont évaluées conformément au paragraphe 1, point 4), et au paragraphe 2, point 4), ci-dessus.

DROITS DES PERSONNES CONCERNÉES

Article 9
Droit d'accès

1. Les parties contractantes veillent à ce que la personne concernée ait le droit d'obtenir, à intervalles raisonnables, des informations indiquant si des données à caractère personnel la concernant sont traitées en vertu du présent accord et, si tel est le cas, d'avoir accès au moins aux informations suivantes:

   a) la confirmation que des données la concernant ont fait ou non l'objet d'un traitement;

   b) des informations portant au moins sur les finalités de l'opération de traitement, les catégories de données concernées et, le cas échéant, sur les destinataires ou les catégories de destinataires auxquels les données sont communiquées;

   c) l'existence du droit de demander à l'autorité compétente la rectification/correction ou l'effacement/la suppression des données à caractère personnel, ou la limitation du traitement des données à caractère personnel relatives à la personne concernée;

   d) une indication du fondement juridique du traitement des données;

   e) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, à défaut, les critères utilisés pour déterminer cette durée;

   f) la communication, sous une forme intelligible, des données à caractère personnel faisant l'objet des traitements ainsi que de toute information disponible sur leurs sources.

2. Dans les cas où le droit d'accès est exercé, la partie qui effectue le transfert est consultée sur une base non contraignante avant qu'une décision définitive sur la demande ne soit prise.

3. Les parties contractantes peuvent prévoir que la fourniture d'informations en réponse à toute demande au titre du paragraphe 1 est retardée, refusée ou limitée si et aussi longtemps que ce retard, ce refus ou cette limitation constitue une mesure nécessaire, raisonnable et proportionnée, compte tenu des droits fondamentaux et des intérêts de la personne concernée, pour:

   a) que des enquêtes pénales et des poursuites pénales ne soient pas compromises; ou

   b) protéger les droits et les libertés de tiers, ou

   c) protéger la sécurité nationale et l'ordre public ou prévenir la criminalité.

4. Les parties contractantes veillent à ce que l'autorité compétente informe la personne concernée par écrit de tout retard, refus ou de toute limitation d'accès ainsi que des motifs de ce retard, de ce refus ou de cette limitation. Ces motifs peuvent être omis si et aussi longtemps que cela porte atteinte à la finalité du retard, du refus ou de la limitation visés au paragraphe 3. L'autorité compétente informe la personne concernée de la possibilité d'introduire une réclamation auprès des autorités de contrôle concernées ainsi que des autres voies de recours prévues dans leurs cadres juridiques respectifs.

Article 10
Droit de rectification/correction, d'effacement/de suppression et de limitation

1. Les parties contractantes veillent à ce que toute personne concernée ait le droit de demander aux autorités compétentes de corriger/rectifier les données à caractère personnel la concernant qui sont inexactes et qui ont été transférées en vertu du présent accord. Compte tenu des finalités du traitement, cela inclut le droit à ce que soient complétées des données à caractère personnel incomplètes qui ont été transférées en vertu du présent accord.

2. La rectification/correction comprend l'effacement/la suppression des données à caractère personnel qui ne sont plus nécessaires au regard des finalités pour lesquelles elles sont traitées.

3. Les parties contractantes peuvent prévoir la limitation du traitement plutôt que l'effacement/la suppression des données à caractère personnel visées au paragraphe 2 s'il y a de bonnes raisons de croire que leur effacement/suppression pourrait porter atteinte aux intérêts légitimes de la personne concernée.

4. Les autorités compétentes s'informent mutuellement des mesures prises en application des paragraphes 1, 2 et 3. L'autorité compétente destinataire rectifie/corrige ou efface ces données ou en limite le traitement conformément aux mesures prises par l'autorité compétente qui effectue le transfert.

5. Les parties contractantes prévoient que l'autorité compétente ayant reçu la demande informe la personne concernée par écrit, sans retard injustifié, et en tout état de cause, dans un délai de trois mois à compter de la réception d'une demande au titre du paragraphe 1 ou 2, que les données la concernant ont été rectifiées/corrigées ou effacées/supprimées ou que leur traitement a été limité.

6. Les parties contractantes veillent à ce que l'autorité compétente ayant reçu la demande informe la personne concernée par écrit, sans retard injustifié, et en tout état de cause, dans un délai de trois mois à compter de la réception d'une demande, de tout refus de rectification/correction, d'effacement/de suppression ou de limitation du traitement, des motifs de ce refus, ainsi que de la possibilité d'introduire une réclamation auprès des autorités de contrôle concernées et des autres voies de recours prévues dans leurs cadres juridiques respectifs.

Article 11
Notification aux autorités concernées d'une violation de données à caractère personnel

1. Les parties contractantes veillent à ce que, en cas de violation de données à caractère personnel concernant des données à caractère personnel transférées en vertu du

présent accord, les autorités compétentes respectives se notifient sans délai cette violation et la notifient, sans délai, à leur autorité de contrôle respective, et prennent des mesures pour en atténuer les éventuelles conséquences négatives.

2. La notification, à tout le moins:

   a) décrit la nature de la violation des données à caractère personnel y compris, si possible, les catégories et le nombre de personnes concernées par la violation et les catégories et le nombre d'enregistrements de données à caractère personnel concernés;

   b) décrit les conséquences probables de la violation de données à caractère personnel;

   c) décrit les mesures prises ou proposées par l'autorité compétente pour remédier à la violation de données à caractère personnel, y compris les mesures prises pour en atténuer les éventuelles conséquences négatives.

3. S'il n'est pas possible de fournir toutes les informations requises en même temps, celles-ci peuvent être communiquées de manière échelonnée. Les informations restant à fournir sont communiquées sans autre retard indu.

4. Les parties contractantes veillent à ce que leurs autorités compétentes respectives documentent toute violation de données à caractère personnel concernant des données à caractère personnel transférées en vertu du présent accord, y compris le contexte, les effets de la violation et les mesures prises pour y remédier, permettant ainsi aux autorités de contrôle concernées de vérifier le respect des exigences légales applicables.

Article 12
Communication à la personne concernée d'une violation de données à caractère personnel

1. Les parties contractantes prévoient que, lorsqu'une violation de données à caractère personnel visée à l'article 11 est susceptible d'avoir de graves conséquences négatives pour les droits et libertés de la personne concernée, leurs autorités compétentes respectives communiquent sans retard indu la violation à la personne concernée.

2. La communication à la personne concernée visée au paragraphe 1 décrit, si possible, la nature de la violation des données à caractère personnel, recommande des mesures à prendre pour atténuer les éventuelles conséquences négatives de cette violation, et contient le nom et les coordonnées du point de contact auprès duquel de plus amples informations peuvent être obtenues.

3. La communication à la personne concernée prévue au paragraphe 1 n'est pas nécessaire si:

   a) les données à caractère personnel concernées par la violation ont fait l'objet de mesures de protection technologiques appropriées qui rendent les données inintelligibles pour toute personne qui n'est pas autorisée à y avoir accès;

b) des mesures ultérieures, qui garantissent que les droits et les libertés de la personne concernée ne risquent plus de subir une grave atteinte, ont été prises; ou

c) cette communication demanderait des efforts disproportionnés, eu égard notamment au nombre de cas concernés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. La communication à la personne concernée peut être retardée, limitée ou omise lorsqu'elle est susceptible:

a) d'entraver des enquêtes, des recherches ou des procédures officielles ou judiciaires;

b) de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, à l'ordre public ou à la sécurité nationale;

c) de porter atteinte aux droits et aux libertés de tiers,

lorsque cela constitue une mesure nécessaire, raisonnable et proportionnée, compte tenu des intérêts légitimes de la personne concernée.

Article 13
Conservation, réexamen, correction et suppression de données à caractère personnel

1. Les parties contractantes prévoient la fixation de délais appropriés pour la conservation des données à caractère personnel reçues dans le cadre du présent accord ou pour la vérification régulière de la nécessité de conserver ces données, de sorte qu'elles ne soient conservées qu'aussi longtemps que nécessaire aux fins pour lesquelles elles ont été transférées.

2. En tout état de cause, la nécessité de continuer à conserver des données à caractère personnel est réexaminée au plus tard trois ans après leur transfert et, s'il n'est pas décidé, de manière justifiée et documentée, de les conserver plus longtemps, elles sont automatiquement effacées après trois ans.

3. Lorsqu'une autorité compétente a des raisons de croire que des données à caractère personnel qu'elle a précédemment transférées sont incorrectes, inexactes, ne sont plus à jour ou n'auraient pas dû être transférées, elle en informe l'autorité compétente destinataire, qui rectifie ou supprime les données à caractère personnel et le notifie à l'autorité ayant effectué le transfert.

4. Lorsqu'une autorité compétente a des raisons de croire que des données à caractère personnel qu'elle a précédemment reçues sont incorrectes, inexactes, ne sont plus à jour ou n'auraient pas dû être transférées, elle en informe l'autorité compétente ayant effectué le transfert, qui fait part de son avis sur la question. Lorsque l'autorité compétente ayant effectué le transfert conclut que les données à caractère personnel sont incorrectes, inexactes, ne sont plus à jour ou n'auraient pas dû être transférées, elle en informe l'autorité compétente destinataire, qui rectifie ou supprime les données à caractère personnel et le notifie à l'autorité ayant effectué le transfert.

Article 14
Registres et traces documentaires

Les parties contractantes prévoient l'établissement de registres concernant la collecte, la modification, l'accès, la communication, y compris les transferts ultérieurs, l'interconnexion et l'effacement des données à caractère personnel.

Ces registres ou ces traces documentaires sont mis, sur demande, à la disposition de l'autorité de contrôle concernée aux fins de vérification de la licéité du traitement des données, d'autocontrôle et de garantie de l'intégrité et de la sécurité des données.

Article 15
Sécurité des données

Les parties contractantes veillent à la mise en œuvre des mesures techniques et organisationnelles visant à protéger les données à caractère personnel échangées dans le cadre du présent accord.

En ce qui concerne le traitement automatisé des données, les parties contractantes veillent à la mise en œuvre des mesures qui sont propres à:

a) interdire à toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle de l'accès des installations);

b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);

c) empêcher l'introduction non autorisée de données à caractère personnel, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation);

d) empêcher que les systèmes de traitement automatisé des données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);

e) garantir que les personnes autorisées à utiliser un système de traitement automatisé des données ne peuvent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données);

f) garantir qu'il est possible de vérifier et de déterminer à quelles instances des données à caractère personnel peuvent être ou ont été transmises en utilisant le système de transmission de données (contrôle de la transmission);

g) garantir qu'il est possible de vérifier et de déterminer quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé des données, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);

h) garantir qu'il soit possible de vérifier et de déterminer quelles données ont été consultées, par quel membre du personnel, à quelle date et à quelle heure (registre d'accès);

i) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);

j) veiller à ce que les systèmes employés puissent être réparés immédiatement en cas de dérangement (remise en état);

k) garantir que les fonctions du système ne sont pas défectueuses, que les erreurs de fonctionnement sont immédiatement signalées (fiabilité) et que les données à caractère personnel conservées ne peuvent être corrompues par un dysfonctionnement du système (intégrité).

Article 16
Autorité de contrôle

1. Chaque partie contractante veille à ce qu'une autorité publique indépendante chargée de la protection des données (autorité de contrôle) supervise les cas susceptibles de porter atteinte à la vie privée des personnes, y compris les règles nationales pertinentes en vertu du présent accord, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel. Chaque partie contractante notifie à l'autre partie le nom de l'autorité qu'elle considère comme l'autorité de contrôle au sens du présent article.

2. Les parties contractantes veillent à ce que l'autorité de contrôle agisse en toute indépendance dans l'exécution de ses tâches et l'exercice de ses pouvoirs. L'autorité de contrôle agit en dehors de toute influence extérieure et ne sollicite ni n'accepte aucune instruction. Ses membres bénéficient de la sécurité de mandat, y compris de garanties contre les destitutions arbitraires.

3. Les parties contractantes veillent à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières, des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs.

4. Les parties contractantes veillent à ce que chaque autorité de contrôle soit investie de réels pouvoirs d'enquête et d'intervention pour surveiller les organismes qu'elle supervise et pour ester en justice.

5. Les parties contractantes veillent à ce que chaque autorité de contrôle ait le pouvoir de connaître des réclamations de personnes physiques sur l'utilisation des données à caractère personnel les concernant faite par les autorités compétentes placées sous son contrôle.

Article 17
Recours administratif et juridictionnel

Les personnes concernées ont droit à un recours administratif et juridictionnel effectif en cas de violation des droits et garanties reconnus dans le présent accord, consécutive au traitement de leurs données à caractère personnel. Chaque partie contractante notifie à l'autre partie la législation interne qu'elle considère comme prévoyant les droits garantis par le présent article.

CHAPITRE III – DIFFERENDS

Article 18
Règlement des différends

Tous les différends susceptibles de naître au sujet de l'interprétation, de l'application ou de la mise en œuvre du présent accord et de toutes les questions y afférentes donnent lieu à des consultations et à des négociations entre les représentants des parties contractantes en vue de parvenir à une solution mutuellement acceptable.

Article 19
Clause de suspension

1. En cas de violation substantielle ou d'inexécution des obligations découlant des dispositions du présent accord, chaque partie contractante peut suspendre le présent accord temporairement, en tout ou en partie, par notification écrite adressée à l'autre partie contractante par la voie diplomatique. Une telle notification écrite n'intervient qu'en cas d'échec des consultations menées, pendant une durée raisonnable, entre les parties contractantes pour trouver une solution; la suspension prend effet vingt jours après la date de réception de la notification. Une telle suspension peut être levée par la partie contractante à l'origine de la suspension, moyennant notification écrite à l'autre partie contractante. La suspension est levée dès réception de cette notification.

2. Nonobstant toute suspension du présent accord, les données à caractère personnel relevant du champ d'application du présent accord et transférées avant sa suspension continuent à être traitées conformément à ses dispositions.

Article 20
Dénonciation de l'accord

1. Le présent accord peut être dénoncé à tout moment par l'une ou l'autre des parties contractantes par notification écrite par la voie diplomatique, moyennant un préavis de trois mois.

2. Les données à caractère personnel relevant du champ d'application du présent accord et transférées avant sa dénonciation continuent à être traitées conformément aux dispositions du présent accord tel qu'applicable au moment de la dénonciation.

3. En cas de dénonciation, les parties contractantes parviennent à un accord sur la poursuite de l'utilisation et de la conservation des informations qu'elles se sont déjà communiquées.

CHAPITRE IV – DISPOSITIONS FINALES

Article 21
Relations avec d'autres instruments internationaux

1. Le présent accord ne porte pas atteinte à l'application des dispositions juridiques relatives à l'échange d'informations prévues par tout traité d'entraide judiciaire, tout autre accord ou arrangement de coopération ou toute relation de travail entre services répressifs pour l'échange d'informations entre la Nouvelle-Zélande et tout État

membre de l'Union européenne, ne modifie en rien ces dispositions ni n'a d'incidence sur elles.

2. Le présent accord complète l'arrangement de travail établissant des relations de coopération entre la police néo-zélandaise et l'Agence de l'Union européenne pour la coopération des services répressifs.

Article 22
Arrangement administratif d'application

Les modalités de la coopération entre les parties contractantes aux fins de la mise en œuvre du présent accord font l'objet d'un arrangement administratif d'application conclu entre Europol et les autorités néo-zélandaises compétentes conformément au règlement Europol.

Article 23
Arrangement administratif relatif à la confidentialité

L'échange d'informations classifiées de l'Union européenne, s'il est nécessaire dans le cadre du présent accord, est régi par un arrangement administratif relatif à la confidentialité conclu entre Europol et les autorités néo-zélandaises compétentes.

Article 24
Point de contact national et officiers de liaison

1. La Nouvelle-Zélande désigne un point de contact national qui fera office de point de contact central entre Europol et les autorités néo-zélandaises compétentes. Les tâches spécifiques du point de contact national sont énumérées dans l'arrangement administratif d'application visé à l'article 22, paragraphe 1. Le point de contact national désigné par la Nouvelle-Zélande est mentionné à l'annexe IV.

2. Europol et la Nouvelle-Zélande renforcent leur coopération conformément au présent accord par le déploiement d'un ou de plusieurs officiers de liaison par la Nouvelle-Zélande. Europol peut déployer un ou plusieurs officiers de liaison en Nouvelle-Zélande.

Article 25
Frais

Sauf disposition contraire du présent accord ou de l'arrangement administratif, les parties contractantes veillent à ce que les autorités compétentes prennent en charge leurs propres dépenses, liées à la mise en œuvre du présent accord.

Article 26
Notification de mise en œuvre

1. Chaque partie contractante prévoit que ses autorités compétentes mettent à la disposition du public un document exposant, sous une forme intelligible, les dispositions applicables en matière de traitement des données à caractère personnel transférées en vertu du présent accord, y compris les moyens disponibles permettant aux personnes concernées d'exercer leurs droits. Chaque partie contractante veille à ce qu'une copie de ce document soit fournie à l'autre partie contractante.

2. Les autorités compétentes adoptent des règles précisant de quelle manière le respect des dispositions applicables en matière de traitement des données à caractère personnel sera assuré dans la pratique si de telles règles n'existent pas encore. Une copie de ces règles est transmise à l'autre partie contractante et aux autorités de contrôle concernées.

Article 27
Entrée en vigueur et application

1. Le présent accord est approuvé par les parties contractantes selon les procédures qui leur sont propres.

2. Le présent accord entre en vigueur à la date de réception de la dernière notification écrite par laquelle les parties contractantes se seront mutuellement notifié, par la voie diplomatique, l'achèvement des procédures visées au paragraphe 1.

3. Le présent accord entre en application le premier jour suivant la date à laquelle il aura été satisfait à l'ensemble des conditions suivantes:

   a) l'arrangement administratif d'application prévu à l'article 22 est devenu applicable; et

   b) les parties contractantes se sont mutuellement notifié le fait que les obligations énoncées dans le présent accord ont été mises en œuvre, y compris conformément à l'article 26, et cette notification a été acceptée.

4. Les parties contractantes échangent des notifications écrites confirmant le respect des conditions susmentionnées par la voie diplomatique.

Article 28
Modifications et compléments

1. Le présent accord peut être modifié par écrit, à tout moment, d'un commun accord entre les parties contractantes, par notification écrite échangée par la voie diplomatique. Les modifications entrent en vigueur selon la même procédure juridique que celle prévue à l'article 27, paragraphes 1 et 2.

2. Les annexes du présent accord peuvent être actualisées, en tant que de besoin, par échange de notes diplomatiques. Ces actualisations entrent en vigueur conformément à l'article 27, paragraphes 1 et 2.

3. Les parties contractantes procèdent à des consultations concernant la modification du présent accord ou de ses annexes à la demande de l'une ou l'autre des parties.

Article 29
Réexamen et évaluation

1. Les parties contractantes procèdent au réexamen conjoint de la mise en œuvre du présent accord un an après son entrée en vigueur, et à intervalles réguliers par la suite et, en outre, à la demande de l'une ou de l'autre partie et sur décision conjointe.

2. Les parties contractantes évaluent conjointement le présent accord quatre ans après son entrée en application.

3. Les parties contractantes fixent à l'avance les modalités du réexamen de la mise en œuvre de l'accord et se communiquent mutuellement la composition de leurs équipes respectives. Ces équipes comprennent des experts dans le domaine de la protection des données et de la répression. Sous réserve des lois applicables, les participants à un réexamen sont tenus de respecter la confidentialité des débats et de posséder les habilitations de sécurité appropriées. Aux fins de tout réexamen, la Nouvelle-Zélande et l'Union européenne garantissent l'accès aux documents et aux systèmes concernés ainsi qu'au personnel compétent.

Article 30
Applicabilité territoriale

1. Le présent accord s'applique au territoire sur lequel le traité sur l'Union européenne et le traité sur le fonctionnement de l'Union européenne sont applicables et dans la mesure où ils le sont, ainsi qu'au territoire de la Nouvelle-Zélande.

2. Le présent accord ne s'appliquera au territoire du Danemark ou de l'Irlande que si l'Union européenne notifie par écrit à la Nouvelle-Zélande que le Danemark ou l'Irlande a choisi d'être lié(e) par le présent accord.

3. Si l'Union européenne notifie à la Nouvelle-Zélande, avant l'entrée en application du présent accord, que celui-ci s'appliquera au territoire du Danemark ou de l'Irlande, le présent accord s'applique au territoire de l'État membre concerné le même jour qu'il s'applique aux autres États membres de l'Union européenne.

4. Si l'Union européenne notifie à la Nouvelle-Zélande, après l'entrée en application du présent accord, que celui-ci s'applique au territoire du Danemark ou de l'Irlande, le présent accord s'applique au territoire de l'État membre concerné trente jours après la date de la notification.

Fait à , le , en double exemplaire, en langues allemande, anglaise, bulgare, croate, danoise, espagnole, estonienne, finnoise, française, grecque, hongroise, italienne, lettonne, lituanienne, maltaise, néerlandaise, polonaise, portugaise, roumaine, slovaque, slovène, suédoise et tchèque, tous les textes faisant également foi.

Par **la Nouvelle-Zélande** Par **l'Union européenne**

ANNEXE I – FORMES DE CRIMINALITE

Les infractions pénales définies à l'article 2, point e), sont les suivantes:

– terrorisme,

– criminalité organisée,

– trafic de stupéfiants,

– activités de blanchiment de capitaux,

– criminalité liée aux matières nucléaires et radioactives,

– filière d'immigration,

– traite d'êtres humains,

– criminalité liée au trafic de véhicules volés,

– meurtre, coups et blessures graves,

– trafic d'organes et de tissus humains,

– enlèvement, séquestration et prise d'otage,

– racisme et xénophobie,

– vol qualifié et vol aggravé,

– trafic de biens culturels, y compris les antiquités et les œuvres d'art,

– escroquerie et fraude,

– infractions portant atteinte aux intérêts financiers de l'Union,

– délits d'initiés et manipulation des marchés financiers,

– racket et extorsion de fonds,

– contrefaçon et piratage de produits,

– falsification de documents administratifs et trafic de faux,

– faux-monnayage et falsification de moyens de paiement,

– criminalité informatique,

– corruption,

– trafic d'armes, de munitions et d'explosifs,

– trafic d'espèces animales menacées,

– trafic d’espèces et d’essences végétales menacées,

– criminalité au détriment de l’environnement, y compris la pollution causée par les navires,

– trafic de substances hormonales et d’autres facteurs de croissance,

– abus sexuels et exploitation sexuelle, y compris matériel pédopornographique et sollicitation d’enfants à des fins sexuelles,

– génocides, crimes contre l’humanité et crimes de guerre.

Les formes de criminalité énumérées dans la présente annexe sont évaluées par les autorités compétentes de la Nouvelle-Zélande conformément à la législation de la Nouvelle-Zélande.

ANNEXE II – AUTORITES NEO-ZELANDAISES COMPETENTES ET LEURS COMPETENCES

Les autorités néo-zélandaises compétentes auxquelles Europol peut transférer des données sont les suivantes:

Autorité
Police néo-zélandaise (en tant que principale autorité compétente)
Service des douanes néo-zélandais
Service de l'immigration néo-zélandais

ANNEXE III — LISTE DES ORGANES DE L'UNION

Missions/opérations relevant de la politique de sécurité et de défense commune, limitées aux activités répressives

Office européen de lutte antifraude (OLAF)

Agence européenne de garde-frontières et de garde-côtes (Frontex)

Banque centrale européenne (BCE)

Parquet européen

Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust)

Office de l'Union européenne pour la propriété intellectuelle (OUEPI)

ANNEXE IV – POINT DE CONTACT NATIONAL

Le point de contact national de la Nouvelle-Zélande, qui fera office de point de contact central entre Europol et les autorités néo-zélandaises compétentes, est désigné ci-après:

Police néo-zélandaise

La Nouvelle-Zélande est tenue d'informer Europol en cas de changement du point de contact.