Journal officiel
de l'Union européenne

FR
Série L

2024/2977

4.12.2024

RÈGLEMENT D'EXÉCUTION (UE) 2024/2977 DE LA COMMISSION

du 28 novembre 2024

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelle et les attestations électroniques d'attributs délivrées aux portefeuilles européens d'identité numérique

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ([1]), et notamment son article 5 *bis*, paragraphe 23,

considérant ce qui suit:

(1) Le cadre européen relatif à une identité numérique établi par le règlement (UE) nº 910/2014 est un élément essentiel pour la mise en place d'un écosystème d'identité numérique sécurisé et interopérable dans l'ensemble de l'Union. Avec pour pierre angulaire les portefeuilles européens d'identité numérique (ci-après les «portefeuilles»), il vise à faciliter l'accès aux services dans l'ensemble des États membres, tout en garantissant la protection des données à caractère personnel et le respect de la vie privée.

(2) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([2]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([3]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(3) L'article 5 *bis*, paragraphe 23, du règlement (UE) nº 910/2014 charge la Commission d'établir, au besoin, les spécifications et les procédures applicables. À cette fin, quatre règlements d'exécution ont été prévus en ce qui concerne les protocoles et les interfaces: règlement d'exécution (UE) 2024/2982 de la Commission ([4]), l'intégrité et les fonctionnalités essentielles: règlement d'exécution (UE) 2024/2979 de la Commission ([5]), les données d'identification personnelle et les attestations électroniques d'attributs: règlement d'exécution (UE) 2024/2977 de la Commission ([6]), ainsi que les notifications à la Commission: règlement d'exécution (UE) 2024/2980 de la Commission ([7]). Le présent règlement établit les exigences applicables concernant les données d'identification personnelle et les attestations électroniques d'attributs délivrées aux portefeuilles européens d'identité numérique.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([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).

([3]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) Règlement d'exécution (UE) 2024/2982 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les protocoles et les interfaces que doit prendre en charge le cadre européen relatif à une identité numérique (JO L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Règlement d'exécution (UE) 2024/2979 de la Commission 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Règlement d'exécution (UE) 2024/2977 de la Commission 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelle et les attestations électroniques d'attributs délivrées aux portefeuilles européens d'identité numérique (JO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Règlement d'exécution (UE) 2024/2980 de la Commission 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les notifications relatives à l'écosystème des portefeuilles européens d'identité numérique transmises à la Commission (JO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) La Commission évalue régulièrement les nouvelles technologies, pratiques, normes ou spécifications techniques. Afin de faire en sorte que le niveau d'harmonisation entre les États membres le plus élevé soit atteint en ce qui concerne le développement et la certification des portefeuilles, les spécifications techniques énoncées dans le présent règlement d'exécution s'appuient sur les travaux menés sur la base de la recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique ([8]), et en particulier sur l'architecture et le cadre de référence qui sont une composante de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([9]), la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement d'exécution, afin de le maintenir en adéquation avec les évolutions générales, l'architecture et le cadre de référence et de suivre les meilleures pratiques sur le marché intérieur.

(5) Afin de garantir la protection des données dès la conception et par défaut, les portefeuilles devraient être dotés de plusieurs éléments renforçant la protection de la vie privée afin d'empêcher les fournisseurs de moyens d'identification électronique et d'attestations électroniques d'attributs de combiner les données à caractère personnel obtenues lors de la fourniture d'autres services avec les données à caractère personnel traitées pour fournir les services relevant du champ d'application du règlement (UE) n° 910/2014.

(6) Dans un souci d'harmonisation, certaines fonctionnalités communes devraient être disponibles dans tous les portefeuilles, y compris la capacité de demander, d'obtenir, de sélectionner, de combiner, de stocker, de supprimer, de partager et de présenter en toute sécurité, sous le contrôle exclusif de l'utilisateur de portefeuille, les données d'identification personnelle et les attestations électroniques d'attributs. Afin que les données d'identification personnelle et les attestations électroniques d'attributs puissent être traitées par l'intermédiaire de chaque unité de portefeuille, les spécifications techniques concernant les attributs de données d'identification personnelle, le format des données et l'infrastructure nécessaire pour garantir la fiabilité appropriée des données d'identification personnelle doivent être compatibles avec toutes les solutions de portefeuille. En outre, les spécifications communes relatives aux attributs des données d'identification personnelle visent à faire en sorte que ces données puissent être utilisées pour la mise en correspondance des identités, le cas échéant.

(7) Les États membres doivent veiller à ce que les portefeuilles soient capables d'authentifier les parties utilisatrices, les fournisseurs de données d'identification personnelle et les fournisseurs d'attestations électroniques d'attributs, quel que soit le lieu où ils sont établis dans l'Union. À cette fin, ces entités devraient utiliser des certificats d'accès de partie utilisatrice de portefeuille lorsqu'elles s'identifient auprès des unités de portefeuille. Afin de garantir l'interopérabilité de ces certificats entre tous les portefeuilles fournis au sein de l'Union, les certificats d'accès de partie utilisatrice de portefeuille devraient être conformes à des normes communes. La Commission, en collaboration avec les États membres, devrait suivre de près l'élaboration de normes nouvelles ou de remplacement sur la base desquelles les certificats d'accès de partie utilisatrice de portefeuille pourraient être établis. En particulier, il convient d'évaluer les modèles de confiance dont l'efficacité et la sécurité sont vérifiées dans les États membres.

(8) Afin de garantir la transparence à l'égard des utilisateurs de portefeuilles, les États membres devraient publier des informations indiquant quelles solutions de portefeuille sont prises en charge par les fournisseurs de données d'identification personnelle établis sur leur territoire. Étant donné que l'identité de l'utilisateur doit être aussi fiable que possible, il convient d'imposer un niveau de garantie élevé commun en ce qui concerne la preuve de l'identité des utilisateurs de portefeuille avant la délivrance des données d'identification personnelle, conformément au niveau de garantie élevé prévu pour les moyens d'identification électronique en vertu du règlement (UE) n° 910/2014. De cette manière, les unités de portefeuille garantissent le plus haut degré de fiabilité disponible pour les moyens d'identification dans l'ensemble de l'Union. Lors de l'inscription des utilisateurs de portefeuilles à un niveau de garantie élevé, divers processus sécurisés sont possibles; par exemple lorsqu'il a été vérifié que l'utilisateur de portefeuille est en possession d'éléments de preuve photographiques ou biométriques reconnus mais non délivrés par l'État membre dans lequel la demande de moyen d'identification électronique est introduite et que ces éléments de preuve correspondent à l'identité revendiquée, il convient de vérifier les éléments de preuve afin d'établir qu'ils sont valables selon une source pertinente faisant autorité.

(9) Pour favoriser l'interopérabilité, les attestations électroniques d'attributs devraient être conformes aux exigences harmonisées en matière de format.

(10) Dans un souci de protection des données des utilisateurs de portefeuille et de garantie de l'authenticité des attestations électroniques d'attributs, des mécanismes d'authentification des fournisseurs d'attestations électroniques d'attributs et de vérification, par ces fournisseurs, de l'authenticité et de la validité des unités de portefeuille devraient s'appliquer avant la délivrance des attestations aux unités de portefeuille.

([8]) JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([9]) Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(11) Pour éviter que des données d'identification personnelle et des attestations électroniques d'attributs ayant perdu leur validité juridique après leur délivrance à une unité de portefeuille ne soient utilisées, et que l'on s'y fie, les fournisseurs de données d'identification personnelle et d'attestations électroniques d'attributs devraient publier des règles décrivant les circonstances et les procédures de révocation.

(12) Afin de garantir que les données d'identification personnelle représentent de manière univoque l'utilisateur du portefeuille, les États membres devraient, outre les attributs obligatoires dans les données d'identification personnelle établis dans le présent règlement, fournir des attributs facultatifs nécessaires pour assurer le caractère univoque de l'ensemble de données d'identification personnelle.

(13) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([10]) et a rendu son avis le 30 septembre 2024.

(14) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet et champ d'application

Le présent règlement établit des règles pour la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs aux unités de portefeuille, qui doivent être régulièrement mises à jour pour tenir compte de l'évolution des technologies et des normes ainsi que des travaux menés sur la base de la recommandation (UE) 2021/946, et en particulier de l'architecture et du cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;

2) «unité de portefeuille»: une configuration unique d'une solution de portefeuille comprenant des instances de portefeuille, des applications cryptographiques sécurisées de portefeuille et des dispositifs cryptographiques sécurisés de portefeuille, fournie par un fournisseur de portefeuille à un utilisateur de portefeuille donné;

3) «solution de portefeuille»: une combinaison de logiciels, de matériel, de services, de paramètres et de configurations, y compris des instances de portefeuille, une ou plusieurs applications cryptographiques sécurisées de portefeuille et un ou plusieurs dispositifs cryptographiques sécurisés de portefeuille;

4) «fournisseur de données d'identification personnelle»: une personne physique ou morale chargée de délivrer et de révoquer les données d'identification personnelle et de veiller à ce que les données d'identification personnelle d'un utilisateur soient liées de manière cryptographique à une unité de portefeuille;

5) «attestation d'unité de portefeuille»: un objet de données qui décrit les composants de l'unité de portefeuille ou permet l'authentification et la validation de ces composants;

6) «instance de portefeuille»: l'application installée et configurée sur l'appareil ou dans l'environnement d'un utilisateur de portefeuille, qui fait partie d'une unité de portefeuille et dont l'utilisateur de portefeuille se sert pour interagir avec l'unité de portefeuille;

7) «application cryptographique sécurisée de portefeuille»: une application qui gère des actifs critiques en étant liée aux fonctions cryptographiques et non cryptographiques fournies par le dispositif cryptographique sécurisé de portefeuille et en utilisant ces fonctions;

([10]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

8) «dispositif cryptographique sécurisé de portefeuille»: un dispositif inviolable qui fournit un environnement lié à l'application cryptographique sécurisée de portefeuille et utilisé par celle-ci pour protéger les actifs critiques et fournir des fonctions cryptographiques pour l'exécution sécurisée d'opérations critiques;

9) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;

10) «actifs critiques»: les actifs se trouvant à l'intérieur d'une unité de portefeuille ou en rapport avec celle-ci et dont l'importance est tellement exceptionnelle que la capacité de se fier à l'unité de portefeuille serait très sérieusement affaiblie si leur disponibilité, leur confidentialité ou leur intégrité étaient compromises;

11) «partie utilisatrice de portefeuille»: une partie utilisatrice qui a l'intention de se fier à des unités de portefeuille pour la fourniture de services publics ou privés au moyen d'une interaction numérique;

12) «certificat d'accès de partie utilisatrice de portefeuille»: un certificat de cachet électronique ou de signature électronique qui authentifie et valide la partie utilisatrice de portefeuille et qui est délivré par un fournisseur de certificats d'accès de partie utilisatrice de portefeuille;

13) «fournisseur de certificats d'accès de partie utilisatrice de portefeuille»: une personne physique ou morale mandatée par un État membre pour délivrer des certificats d'accès de partie utilisatrice aux parties utilisatrices de portefeuille enregistrées dans cet État membre.

Article 3

Délivrance de données d'identification personnelle aux unités de portefeuille

1. Les fournisseurs de données d'identification personnelle délivrent des données d'identification personnelle aux unités de portefeuille conformément aux schémas d'identification électronique dans le cadre desquels des solutions de portefeuille sont fournies.

2. Les fournisseurs de données d'identification personnelle veillent à ce que les données d'identification personnelle délivrées aux unités de portefeuille contiennent les informations nécessaires à l'authentification et à la validation des données d'identification personnelle.

3. Les fournisseurs de données d'identification personnelle veillent à ce que les données d'identification personnelle délivrées aux unités de portefeuille soient conformes aux spécifications techniques énoncées dans l'annexe.

4. Les États membres veillent à ce que les données d'identification personnelle délivrées à un utilisateur de portefeuille donné soient uniques pour l'État membre.

5. Les fournisseurs de données d'identification personnelle veillent à ce que les données d'identification personnelle qu'ils délivrent soient liées de manière cryptographique à l'unité de portefeuille à laquelle elles sont délivrées.

6. Les États membres mettent à la disposition du public une liste de solutions de portefeuille prises en charge par les fournisseurs de données d'identification personnelle qui font partie des schémas d'identification électronique de cet État membre.

7. Les États membres inscrivent les utilisateurs de portefeuille conformément aux exigences relatives à l'inscription à un niveau de garantie élevé, telles qu'énoncées dans le règlement d'exécution (UE) 2015/1502 de la Commission ([11]). Dans le cadre du processus d'inscription, les fournisseurs de données d'identification personnelle procèdent à une vérification de l'identité de l'utilisateur de portefeuille, conformément aux exigences concernant la preuve et la vérification d'identité, avant de délivrer les données d'identification personnelle à l'unité de portefeuille de l'utilisateur de portefeuille correspondant.

8. Lorsqu'ils délivrent des données d'identification personnelle à des unités de portefeuille, les fournisseurs de données d'identification personnelle s'identifient auprès des unités de portefeuille en utilisant leur certificat d'accès de partie utilisatrice de portefeuille ou un autre mécanisme d'authentification conformément à un schéma d'identification électronique notifié au niveau de garantie élevé.

([11]) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

9. Avant de délivrer des données d'identification personnelle à une unité de portefeuille, les fournisseurs de données d'identification personnelle authentifient et valident l'attestation d'unité de portefeuille de l'unité de portefeuille et vérifient que l'unité de portefeuille appartient à une solution de portefeuille que le fournisseur de données d'identification personnelle accepte, ou utilisent un autre mécanisme d'authentification conformément à un schéma d'identification électronique notifié au niveau de garantie élevé.

Article 4

Délivrance d'attestations électroniques d'attributs aux unités de portefeuille

1. Les attestations électroniques d'attributs délivrées aux unités de portefeuille sont conformes à au moins une des normes figurant dans la liste de l'annexe I du règlement d'exécution (UE) 2024/2979.

2. Les fournisseurs d'attestations électroniques d'attributs s'identifient auprès des unités de portefeuille en utilisant leur certificat d'accès de partie utilisatrice de portefeuille.

3. Les fournisseurs d'attestations électroniques d'attributs veillent à ce que les attestations électroniques d'attributs délivrées aux unités de portefeuille contiennent les informations nécessaires à l'authentification et à la validation de ces attestations électroniques d'attributs.

Article 5

Révocation de données d'identification personnelle

1. Les fournisseurs de données d'identification personnelle délivrées à une unité de portefeuille disposent de règles écrites et accessibles au public concernant la gestion du statut de validité, y compris, le cas échéant, les conditions dans lesquelles ces données d'identification personnelle peuvent être révoquées sans délai.

2. Seuls les fournisseurs de données d'identification personnelle ou d'attestations électroniques d'attributs peuvent révoquer les données d'identification personnelle ou les attestations électroniques d'attributs qu'ils ont délivrées.

3. Lorsque les fournisseurs de données d'identification personnelle ont révoqué des données d'identification personnelle, ils en informent, par des canaux spécialisés et sécurisés, les utilisateurs de portefeuilles faisant l'objet de ces données d'identification personnelle dans un délai de 24 heures à compter de la révocation en indiquant les motifs de la révocation. Cela doit se faire de manière concise et facilement accessible, dans un langage clair et simple.

4. Les fournisseurs de données d'identification personnelle sont tenus de révoquer les données d'identification personnelle délivrées à des unités de portefeuille dans chacun des cas suivants:

a) à la demande explicite de l'utilisateur du portefeuille à l'unité de portefeuille duquel les données d'identification personnelle ou l'attestation électronique d'attributs ont été délivrées;

b) lorsque l'attestation d'unité du portefeuille à laquelle les données d'identification personnelle ont été délivrées a été révoquée;

c) dans d'autres situations déterminées par les fournisseurs de données d'identification personnelle ou d'attestations électroniques d'attributs dans leurs règles visées au paragraphe 1.

5. Les fournisseurs de données d'identification personnelle délivrées à une unité de portefeuille veillent à ce que les révocations ne puissent pas être annulées.

6. Les données d'identification personnelle révoquées restent accessibles aussi longtemps que le droit de l'Union ou le droit national l'exige.

7. Lorsque les fournisseurs de données d'identification personnelle révoquent les données d'identification personnelle délivrées aux unités de portefeuille, ils rendent public le statut de validité des données d'identification personnelle qu'ils délivrent, dans le respect de la vie privée, et indiquent l'emplacement de cette information dans les données d'identification personnelle.

8. Les fournisseurs de données d'identification personnelle mettent en place des techniques de protection de la vie privée qui garantissent la non-associabilité, lorsque l'attestation d'attributs n'exige pas l'identification de l'utilisateur.

Article 6

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 28 novembre 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

SPÉCIFICATIONS TECHNIQUES RELATIVES AUX DONNÉES D'IDENTIFICATION PERSONNELLE VISÉES À L'ARTICLE 3, PARAGRAPHE 3

1. **Ensemble de donnés d'identification des personnes physiques**

Tableau 1

Données d'identification personnelle obligatoires pour les personnes physiques

Identifiant de données	Définition	Présence
family_name	Nom(s) de famille actuel(s) de l'utilisateur auquel se rapportent les données d'identification personnelle.	Obligatoire
given_name	Prénom(s) actuel(s), y compris, le cas échéant, le(s) deuxième(s) prénom(s) de l'utilisateur auquel se rapportent les données d'identification personnelle.	Obligatoire
birth_date	Jour, mois et année de naissance de l'utilisateur auquel se rapportent les données d'identification personnelle.	Obligatoire
birth_place	Le code pays alpha-2, tel que spécifié dans la norme ISO 3166-1, ou la subdivision de l'État, la province, le district, le territoire ou la municipalité, la ville ou le village où est né l'utilisateur auquel les données d'identification personnelle se rapportent.	Obligatoire
nationality	Un ou plusieurs codes pays alpha-2 spécifiés dans la norme ISO 3166-1, représentant la nationalité de l'utilisateur auquel se rapportent les données d'identification personnelle.	Obligatoire

Lorsqu'une valeur d'attribut n'est pas connue pour la personne ou ne peut pas être délivrée autrement dans le cadre de l'ensemble de données d'identification personnelle, les États membres utilisent à la place une valeur d'attribut adaptée à la situation.

Tableau 2

Données d'identification personnelle facultatives pour les personnes physiques

Identifiant de données	Définition	Présence
resident_address	L'adresse complète du lieu où l'utilisateur auquel se rapportent les données d'identification personnelle réside actuellement ou peut être contacté (nom de rue, numéro de maison, ville, etc.).	Facultatif
resident_country	Le pays où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle, sous la forme d'un code pays alpha-2, tel que spécifié dans la norme ISO 3166-1.	Facultatif
resident_state	La subdivision de l'État, la province, le district ou le territoire où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.	Facultatif

Identifiant de données	Définition	Présence
resident_city	La municipalité, la ville ou le village où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.	Facultatif
resident_postal_code	Le code postal du lieu où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.	Facultatif
resident_street	Le nom de la rue où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.	Facultatif
resident_house_number	Le numéro de la maison où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle, y compris tout affixe ou suffixe.	Facultatif
personal_administrative_number	Une valeur attribuée à la personne physique qui est unique parmi tous les numéros administratifs personnels délivrés par le fournisseur de données d'identification personnelle. Lorsque les États membres choisissent d'inclure cet attribut, ils décrivent dans leurs schémas d'identification électronique en vertu desquels les données d'identification personnelle sont délivrées la politique qu'ils appliquent aux valeurs de cet attribut, y compris, le cas échéant, les conditions spécifiques applicables au traitement de cette valeur.	Facultatif
portrait	Image faciale de l'utilisateur du portefeuille conforme aux spécifications ISO 19794-5 ou ISO 39794	Facultatif
family_name_birth	Nom(s) de l'utilisateur de données d'identification personnelle au moment de la naissance.	Facultatif
given_name_birth	Prénom(s), y compris deuxième(s) prénom(s), de l'utilisateur de données d'identification personnelle au moment de la naissance.	Facultatif
sex	La valeur est l'une des suivantes: 0 = inconnu; 1 = masculin; 2 = féminin; 3 = autre; 4 = inter; 5 = divers; 6 = ouvert; 9 = sans objet. Pour les valeurs 0, 1, 2 et 9, la norme ISO/IEC 5218 s'applique.	Facultatif
email_address	Adresse de courrier électronique de l'utilisateur auquel se rapportent les données d'identification personnelle [conformément à la norme RFC 5322].	Facultatif
mobile_phone_number	Numéro de téléphone portable de l'utilisateur auquel se rapportent les données d'identification personnelle, commençant par le symbole «+», comme préfixe d'appel international, et l'indicatif téléphonique international, suivis de numéros uniquement.	Facultatif

2. **Ensemble de donnés d'identification des personnes morales**

Tableau 3

Données d'identification personnelle obligatoires pour les personnes morales

Élément de données	Présence
Dénomination sociale actuelle	Obligatoire
Un identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontière et qui soit aussi persistant que possible dans le temps	Obligatoire

Lorsqu'un élément de donnée n'est pas connu pour la personne ou ne peut pas être délivré autrement dans le cadre de l'ensemble de données d'identification personnelle, les États membres utilisent à la place une valeur d'attribut adaptée à la situation.

Tableau 4

Données d'identification personnelle facultatives pour les personnes morales

Élément de données	Présence
Adresse actuelle	Facultatif
Numéro d'identification TVA	Facultatif
Numéro de référence fiscal	Facultatif
Identifiant unique européen visé dans la directive (UE) 2017/1132 du Parlement européen et du Conseil	Facultatif
Identifiant d'entité juridique (LEI) visé dans le règlement d'exécution (UE) 2022/1860 de la Commission	Facultatif
Numéro d'enregistrement et d'identification des opérateurs économiques (numéro EORI) visé dans le règlement d'exécution (UE) nº 1352/2013 de la Commission	Facultatif
Numéro d'accise visé à l'article 2, point 12), du règlement (UE) nº 389/2012 du Conseil	Facultatif

3. **Ensemble de métadonnées relatives aux données d'identification des personnes**

Tableau 5

Métadonnées relatives aux données d'identification des personnes

Identifiant de données	Définition	Présence
expiry_date	Date (et, si possible, heure) à laquelle les données d'identification personnelle expirent.	Obligatoire
issuing_authority	Nom de l'autorité administrative qui a délivré les données d'identification personnelle, ou code pays ISO 3166 alpha-2 de l'État membre concerné s'il n'existe pas d'autorité distincte habilitée à délivrer les données d'identification personnelle.	Obligatoire
issuing_country	Code du pays alpha-2, tel que spécifié dans la norme ISO 3166-1, du pays ou territoire du fournisseur des données d'identification personnelle.	Obligatoire

Identifiant de données	Définition	Présence
document_number	Un numéro pour les données d'identification personnelle, attribué par le fournisseur de données d'identification personnelle.	Facultatif
issuing_jurisdiction	Code de subdivision du pays correspondant à l'entité territoriale qui a émis les données d'identification personnelle, conformément à la clause 8 de la norme ISO 3166-2:2020. La première partie du code est identique à la valeur correspondant au pays de délivrance.	Facultatif
location_status	L'emplacement des informations relatives au statut de validité des données d'identification personnelle lorsque les fournisseurs de données d'identification personnelle révoquent les données d'identification personnelle.	Facultatif

4. **Encodage des attributs de données d'identification personnelle**

Les données d'identification personnelle sont délivrées dans deux formats:

1) le format spécifié dans la norme ISO/IEC 18013-5:2021;

2) «Verifiable Credentials Data Model 1.1.», Recommandation W3C, 3 mars 2022.

5. **Détails de l'infrastructure de confiance**

La liste des fournisseurs de données d'identification personnelle mise à disposition par la Commission conformément au règlement d'exécution (UE) 2024/2980 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les notifications relatives à l'écosystème des portefeuilles européens d'identité numérique transmises à la Commission permet d'authentifier les données d'identification personnelle.