Journal officiel
de l'Union européenne

FR
Série L

2025/847

7.5.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/847 DE LA COMMISSION

du 6 mai 2025

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les réactions aux atteintes à la sécurité des 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 *sexies*, paragraphe 5,

considérant ce qui suit:

(1) Le cadre européen relatif à une identité numérique (ci-après le «cadre») 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) Les règlements (UE) 2016/679 ([2]) et (UE) 2018/1725 ([3]) du Parlement européen et du Conseil et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([4]) s'appliquent aux activités de traitement de données à caractère personnel au titre du présent règlement. Les règles relatives à l'évaluation et à la fourniture d'informations établies en vertu du présent règlement sont sans préjudice de l'obligation de notifier les violations de données à caractère personnel à l'autorité de contrôle compétente, le cas échéant, en application du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, et de l'obligation de communiquer les violations de données à caractère personnel aux personnes concernées, le cas échéant, en application desdits règlements.

(3) La Commission évalue régulièrement les nouvelles technologies, pratiques, normes et spécifications techniques. Afin d'atteindre le niveau d'harmonisation le plus élevé possible entre les États membres en ce qui concerne le développement et la certification des portefeuilles, les spécifications techniques énoncées dans le présent règlement s'appuient sur les travaux menés sur la base de la recommandation (UE) 2021/946 de la Commission ([5]), et en particulier sur l'architecture et le cadre de référence, qui sont une des composantes de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([6]), la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement, afin de le maintenir en adéquation avec les évolutions générales et l'architecture et le cadre de référence, et de suivre les meilleures pratiques sur le marché intérieur.

([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]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) 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).

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

([6]) Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) nº 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.

(4) Toute atteinte à la sécurité ou compromission des solutions de portefeuille ou des mécanismes de validation visés à l'article 5 *bis*, paragraphe 8, du règlement (UE) nº 910/2014, ou du schéma d'identification électronique dans le cadre duquel les solutions de portefeuille sont fournies, doit être suivie d'une réaction rapide, coordonnée et sécurisée dans tous les États membres afin de protéger les utilisateurs et de maintenir la confiance dans l'écosystème de l'identité numérique. Cette considération est sans préjudice de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([7]) et des règlements (UE) 2019/881 ([8]) et (UE) 2024/2847 ([9]) du Parlement européen et du Conseil, en particulier en ce qui concerne la gestion des incidents ou des vulnérabilités et leur prise en compte comme des atteintes à la sécurité. Par conséquent, les États membres devraient veiller à ce que la fourniture et l'utilisation des portefeuilles ayant subi une atteinte à la sécurité ou une compromission soient suspendues en temps voulu, ou, le cas échéant, que ces portefeuilles soient retirés.

(5) Afin que les réactions en cas d'atteinte à la sécurité ou de compromission soient appropriées, les États membres devraient évaluer si une atteinte à la sécurité ou une compromission d'une solution de portefeuille, des mécanismes de validation visés à l'article 5 *bis*, paragraphe 8, du règlement (UE) nº 910/2014 ou du schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie a une incidence sur la fiabilité de cette solution de portefeuille ou d'autres solutions de portefeuille. Cette évaluation devrait être fondée sur des critères uniformes, tels que le nombre et la catégorie d'utilisateurs de portefeuille, de personnes physiques et de parties utilisatrices de portefeuille concernés, la nature des données concernées, la durée de la compromission ou de l'atteinte à la sécurité, la disponibilité limitée d'un service et les pertes financières, ainsi que la compromission potentielle de données à caractère personnel. Ces critères devraient offrir aux États membres la souplesse et la marge d'appréciation nécessaires pour déterminer de manière proportionnée si la fiabilité d'une solution de portefeuille est affectée et s'il est approprié de suspendre la solution de portefeuille, voire de la retirer lorsque la gravité de l'atteinte ou de la compromission le justifie. L'application de ces critères ne devrait pas entraîner automatiquement le retrait d'une solution de portefeuille ou la suspension de sa fourniture et de son utilisation, mais les États membres devraient dûment tenir compte de ces critères lorsqu'ils décident s'il est nécessaire de retirer une solution de portefeuille ou de suspendre sa fourniture et son utilisation.

(6) Compte tenu des conséquences de la suspension de l'utilisation d'une solution de portefeuille et des inconvénients qu'elle présente, les États membres devront déterminer s'il est nécessaire de révoquer des attestations d'unité de portefeuille ou de prendre toute autre mesure supplémentaire pour réagir de manière adéquate à l'atteinte à la sécurité ou à la compromission.

(7) Afin de tenir les utilisateurs de portefeuille informés du statut de leur portefeuille, il y a lieu de leur fournir des informations adéquates sur les atteintes à la sécurité ou les compromissions subies par leur portefeuille. Étant donné que les parties utilisatrices de portefeuille enregistrées dans l'Union peuvent aussi être affectées par des atteintes à la sécurité et des compromissions, il est également nécessaire de leur communiquer des informations pertinentes sur ces atteintes et compromissions.

(8) Afin d'améliorer la transparence et de favoriser la confiance dans l'écosystème de l'identité numérique, les informations concernant les atteintes à la sécurité ou les compromissions et leurs conséquences devraient au moins comprendre les informations requises au titre du présent règlement. Il convient toutefois d'évaluer soigneusement les informations concernant les atteintes à la sécurité ou les compromissions communiquées aux utilisateurs de portefeuille et aux parties utilisatrices de portefeuille afin d'éviter et de réduire au minimum tout risque d'exploitation par des attaquants.

([7]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Pour que les utilisateurs puissent à nouveau accéder à leurs unités de portefeuille après qu'il a été remédié à une atteinte à la sécurité ou à une compromission, l'État membre qui a fourni les solutions de portefeuille devra rétablir la fourniture et l'utilisation de ces solutions dans les meilleurs délais. Pour ce faire, il peut rétablir les unités de portefeuille, délivrer des unités de portefeuille fournies dans le cadre d'une nouvelle version des solutions de portefeuille ou délivrer à nouveau de nouvelles attestations d'unité de portefeuille valides. Les utilisateurs de portefeuille concernés, les parties utilisatrices de portefeuille, les points de contact uniques désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) nº 910/2014 et la Commission devraient en être informés en conséquence.

(10) Afin de faire en sorte que les portefeuilles soient retirés lorsqu'il n'a pas été remédié à une atteinte à la sécurité ou à une compromission dans un délai de trois mois à compter de la suspension, ou lorsque la gravité de l'atteinte à la sécurité ou de la compromission le justifie, l'État membre devrait veiller à ce que les attestations d'unité de portefeuille concernées soient révoquées, à ce que leur validité ne puisse pas être restaurée et à ce qu'elles ne puissent ni être délivrées ni fournies à des unités de portefeuille existantes. En outre, aucune nouvelle unité de portefeuille ne devrait être fournie dans le cadre de la solution de portefeuille affectée. Dans un souci de transparence, il convient d'informer du retrait les utilisateurs, les parties utilisatrices, les points de contact uniques désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) nº 910/2014 et la Commission. Les informations fournies devraient comprendre une description des incidences potentielles sur les utilisateurs de portefeuille, et notamment sur la gestion des attestations délivrées, ou sur les parties utilisatrices de portefeuille.

(11) La période de trois mois suivant la suspension de la fourniture et de l'utilisation d'une solution de portefeuille, et pendant laquelle il doit être remédié à l'atteinte à la sécurité ou à la compromission ayant conduit à cette suspension, devrait constituer un délai au-delà duquel la solution de portefeuille doit être retirée, à moins qu'une mesure correctrice appropriée n'ait été mise en œuvre. Les États membres sont toutefois libres d'exiger qu'il soit remédié à l'atteinte à la sécurité ou à la compromission dans un délai inférieur à trois mois, compte tenu, en particulier et le cas échéant, de l'ampleur, de la durée et des conséquences de cette atteinte ou compromission. Lorsqu'il n'est pas remédié ou ne peut pas être remédié à l'atteinte à la sécurité ou à la compromission dans le délai fixé par l'État membre, celui-ci peut exiger le retrait de la solution de portefeuille avant l'expiration du délai de trois mois. Les États membres devraient utiliser ce délai dans lequel il doit être remédié à l'atteinte à la sécurité ou à la compromission ayant conduit à la suspension de la fourniture et de l'utilisation d'une solution de portefeuille pour préparer le retrait potentiel de cette solution et les communications qui en résultent.

(12) Afin de réduire la charge administrative pesant sur les États membres en ce qui concerne les informations à fournir à la Commission et aux autres États membres en application du présent règlement, les États membres devraient utiliser les outils de notification existants tels que le système de notification et d'analyse des incidents de cybersécurité (CIRAS) géré par l'Agence de l'Union européenne pour la cybersécurité (ENISA). Pour ce qui est des autres canaux ou moyens à utiliser pour informer les utilisateurs de portefeuille affectés par une atteinte à la sécurité ou par une compromission ainsi que les parties utilisatrices de portefeuille, les États membres devraient veiller à ce que les informations pertinentes soient fournies d'une manière claire, complète et facilement accessible. Les canaux permettant de fournir ces informations aux utilisateurs de portefeuille affectés et aux parties utilisatrices de portefeuille devraient comprendre des solutions appropriées pour la diffusion sur site web, le suivi en temps réel des mises à jour de sites web et l'agrégation d'informations.

(13) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu son avis le 31 janvier 2025.

(14) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement établit les règles applicables en ce qui concerne les réactions aux atteintes à la sécurité des portefeuilles, des mécanismes de validation visés à l'article 5 *bis*, paragraphe 8, du règlement (UE) nº 910/2014 et du schéma d'identification électronique dans le cadre duquel les portefeuilles sont fournis.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «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;

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

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

4) «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;

5) «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;

6) «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;

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

8) «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;

9) «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;

10) «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.

Article 3

Constatation d'une atteinte à la sécurité ou d'une compromission

1. Sans préjudice de la directive (UE) 2022/2555 et des règlements (UE) 2019/881 et (UE) 2024/2847, les États membres tiennent dûment compte des critères énoncés à l'annexe I afin d'évaluer si une atteinte à la sécurité ou une compromission d'une solution de portefeuille, des mécanismes de validation visés à l'article 5 *bis*, paragraphe 8, du règlement (UE) nº 910/2014 ou du schéma d'identification électronique dans le cadre duquel la solution de portefeuille est fournie affecte la fiabilité de cette solution, de ces mécanismes ou de ce schéma, ou la fiabilité d'autres solutions de portefeuille.

2. Lorsqu'un État membre constate, sur la base de l'évaluation prévue au paragraphe 1, qu'une atteinte à la sécurité ou une compromission affecte la fiabilité d'une solution de portefeuille et qu'il suspend la fourniture et l'utilisation de cette solution, il prend les mesures énoncées aux articles 4 et 5. Lorsqu'un État membre retire la solution de portefeuille, il prend les mesures énoncées aux articles 8 et 9.

3. Lorsqu'un État membre a connaissance d'informations relatives à une éventuelle atteinte à la sécurité ou à une éventuelle compromission susceptible d'affecter la fiabilité d'une ou de plusieurs solutions de portefeuille fournies par un autre État membre, il en informe sans retard injustifié la Commission et les points de contact uniques des États membres affectés, désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) nº 910/2014. Pour ce faire, il communique les informations mentionnées à l'article 5, paragraphe 2.

4. L'État membre qui reçoit des informations fournies conformément au paragraphe 3 prend les mesures énoncées aux paragraphes 1 et 2 sans retard injustifié.

Article 4

Suspension de la fourniture et de l'utilisation de portefeuilles et autres mesures correctrices

1. Les États membres veillent à ce qu'aucune unité de portefeuille ne soit fournie, utilisée ou activée dans le cadre de la solution de portefeuille suspendue.

2. Les États membres évaluent la nécessité de révoquer des attestations d'unité de portefeuille des unités de portefeuille concernées par la suspension d'une solution de portefeuille, ou de prendre toute autre mesure correctrice supplémentaire, pour réagir de manière adéquate à l'atteinte à la sécurité ou à la compromission.

3. Les mesures énoncées aux paragraphes 1 et 2 sont prises sans retard injustifié et, en tout état de cause, au plus tard 24 heures après la suspension de la fourniture et de l'utilisation de la solution de portefeuille ayant subi une atteinte à la sécurité ou une compromission.

4. Les mesures énoncées aux paragraphes 1 et 2 n'empêchent pas les utilisateurs de portefeuille affectés d'exercer leur droit à la portabilité des données établi à l'article 5 *bis*, paragraphe 4, point g), du règlement (UE) n° 910/2014, à condition que ce droit puisse être exercé par les utilisateurs de portefeuille sans compromettre la sécurité des actifs critiques des unités de portefeuille affectées, compte tenu notamment des raisons de la suspension et de la nécessité d'assurer une protection efficace de ces actifs contre toute utilisation abusive.

Article 5

Informations concernant les suspensions et les mesures correctrices

1. Des informations concernant la suspension de la fourniture et de l'utilisation d'une solution de portefeuille sont fournies d'une manière claire, complète et facilement accessible, sans retard injustifié et au plus tard 24 heures après cette suspension:

a) aux points de contact uniques désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014;

b) à la Commission;

c) aux utilisateurs de portefeuille affectés;

d) aux parties utilisatrices de portefeuille enregistrées conformément à l'article 5 *ter* du règlement (UE) n° 910/2014.

2. Les informations fournies conformément au paragraphe 1 incluent au moins les éléments suivants:

a) le nom du fournisseur de la solution de portefeuille dont la fourniture et l'utilisation ont été suspendues;

b) le nom et l'identifiant de référence de cette solution de portefeuille, tels qu'ils figurent sur la liste des portefeuilles certifiés établie conformément à l'article 5 *quinquies* du règlement (UE) n° 910/2014 et, le cas échéant, les versions concernées;

c) la date et l'heure auxquelles l'atteinte à la sécurité ou la compromission a été détectée;

d) si elles sont connues, la date et l'heure auxquelles l'atteinte à la sécurité ou la compromission est devenue effective, sur la base des journaux du réseau ou du système ou d'autres sources de données;

e) la date et l'heure de la suspension de la solution de portefeuille;

f) les coordonnées, y compris au moins une adresse électronique et un numéro de téléphone, de l'État membre notifiant et, si elles sont différentes, du fournisseur de portefeuille visé au point a);

g) une description de l'atteinte à la sécurité ou de la compromission;

h) une description des données compromises, y compris, le cas échéant, les catégories de données à caractère personnel définies à l'article 9, paragraphe 1, et à l'article 10 du règlement (UE) 2016/679;

i) dans la mesure du possible, une estimation du nombre approximatif d'utilisateurs de portefeuille et d'autres personnes physiques affectés;

j) une description des incidences potentielles sur les parties utilisatrices de portefeuille ou sur les utilisateurs de portefeuille et, dans ce dernier cas, si nécessaire, une indication des mesures que les utilisateurs de portefeuille peuvent prendre pour atténuer ces incidences potentielles;

k) une description des mesures prises ou prévues pour remédier à l'atteinte à la sécurité ou à la compromission, ainsi qu'un calendrier et un délai pour cette remédiation;

l) le cas échéant et s'il y a lieu, une description des mesures prises ou prévues pour faire migrer les utilisateurs de portefeuille affectés vers d'autres solutions de portefeuille ou services.

Article 6

Rétablissement de la fourniture et de l'utilisation de portefeuilles

Lorsque cela est nécessaire pour rétablir la fourniture, l'activation et l'utilisation d'une solution de portefeuille, les États membres procèdent, sans retard injustifié;

1) au rétablissement de la fourniture et de l'utilisation des unités de portefeuille fournies dans le cadre de cette solution de portefeuille en délivrant à tous les utilisateurs affectés une unité de portefeuille fournie dans le cadre d'une nouvelle version de cette solution de portefeuille;

2) à la délivrance de nouvelles attestations d'unité de portefeuille à de nouvelles unités de portefeuille ou, le cas échéant, à des unités de portefeuille précédemment délivrées, à condition que ces unités de portefeuille satisfassent aux exigences de sécurité en vigueur après qu'il a été remédié à l'atteinte à la sécurité ou à la compromission;

3) à l'abrogation de toute mesure mise en œuvre conformément à l'article 4 et empêchant la fourniture de nouvelles unités de portefeuille dans le cadre de la solution de portefeuille affectée, lorsque cette mesure était uniquement liée à l'atteinte à la sécurité ou à la compromission ayant fait l'objet d'une remédiation.

Article 7

Informations sur le rétablissement

Lorsqu'un État membre rétablit une solution de portefeuille, il veille à ce que:

1) toutes les parties ayant reçu des informations sur la suspension de la fourniture et de l'utilisation de cette solution de portefeuille conformément à l'article 5, paragraphe 1, en soient informées sans retard injustifié;

2) les informations fournies conformément au point 1) comprennent au moins les éléments énumérés à l'article 5, paragraphe 2, points a), b) et f) à h), ainsi que les éléments suivants:

   a) la date et l'heure auxquelles il a été remédié à l'atteinte à la sécurité ou à la compromission;

   b) la date et l'heure du rétablissement de la solution de portefeuille affectée et, le cas échéant, des unités de portefeuille affectées fournies dans le cadre de cette solution de portefeuille;

   c) une description des mesures prises pour remédier à l'atteinte à la sécurité ou à la compromission;

   d) une description des incidences résiduelles potentielles sur les parties utilisatrices de portefeuille ou sur les utilisateurs de portefeuille et, dans ce dernier cas, si nécessaire, une indication des mesures que les utilisateurs de portefeuille peuvent prendre pour atténuer ces incidences résiduelles potentielles.

Article 8

Retrait de portefeuilles

1. S'il n'est pas remédié à une atteinte à la sécurité ou à une compromission ayant conduit à la suspension de la fourniture et de l'utilisation d'une solution de portefeuille dans un délai de trois mois à compter de la date de cette suspension, l'État membre qui fournit la solution affectée veille à ce qu'elle soit retirée et à ce que sa validité soit révoquée, sans retard injustifié et, en tout état de cause, dans les 72 heures suivant l'expiration du délai de trois mois.

2. Lorsqu'un État membre retire une solution de portefeuille, il veille à ce que:

a) les attestations d'unité de portefeuille de l'unité de portefeuille de la solution de portefeuille affectée soient révoquées;

b) la validité des attestations d'unité de portefeuille ne puisse pas être restaurée;

c) aucune nouvelle attestation d'unité de portefeuille ne puisse être délivrée aux unités de portefeuille existantes fournies dans le cadre de la solution de portefeuille affectée;

d) aucune nouvelle unité de portefeuille ne puisse être fournie dans le cadre de la solution de portefeuille affectée.

3. Les mesures énoncées aux paragraphes 1 et 2 n'empêchent pas les utilisateurs de portefeuille affectés d'exercer leur droit à la portabilité des données établi à l'article 5 *bis*, paragraphe 4, point g), du règlement (UE) nº 910/2014, à condition que ce droit puisse être exercé par les utilisateurs de portefeuille sans compromettre la sécurité des actifs critiques des unités de portefeuille affectées, compte tenu notamment des raisons du retrait et de la nécessité d'assurer une protection efficace de ces actifs contre toute utilisation abusive.

Article 9

Informations sur le retrait

1. Des informations concernant le retrait d'une solution de portefeuille sont fournies d'une manière claire, complète et facilement accessible, sans retard injustifié et au plus tard 24 heures après ce retrait:

a) aux points de contact uniques désignés conformément à l'article 46 *quater*, paragraphe 1, du règlement (UE) nº 910/2014;

b) à la Commission;

c) aux utilisateurs de portefeuille affectés;

d) aux parties utilisatrices de portefeuille enregistrées conformément à l'article 5 *ter* du règlement (UE) nº 910/2014.

2. Les informations fournies conformément au paragraphe 1 incluent au moins les éléments suivants:

a) le nom du fournisseur de la solution de portefeuille qui a été retirée;

b) le nom et l'identifiant de référence de cette solution de portefeuille, tels qu'ils figurent sur la liste des portefeuilles certifiés établie conformément à l'article 5 *quinquies* du règlement (UE) nº 910/2014 et, le cas échéant, les versions concernées;

c) la date et l'heure de la détection de l'atteinte à la sécurité ou de la compromission qui a conduit au retrait de la solution de portefeuille affectée en raison de la gravité de ces incidents ou parce qu'ils n'ont pas fait l'objet d'une remédiation dans un délai de trois mois;

d) si elles sont connues, la date et l'heure auxquelles l'atteinte à la sécurité ou la compromission est devenue effective, sur la base des journaux du réseau ou du système ou d'autres sources de données;

e) la date et l'heure du retrait de la solution de portefeuille et de la révocation effective des attestations d'unité de portefeuille des unités de portefeuille fournies dans le cadre de la solution de portefeuille;

f) une mention indiquant si le retrait résulte de la gravité de l'atteinte à la sécurité ou de la compromission ou du fait que celles-ci n'ont pas fait l'objet d'une remédiation;

g) les coordonnées, y compris au moins une adresse électronique et un numéro de téléphone, de l'État membre notifiant et, si elles sont différentes, du fournisseur de portefeuille visé au point a);

h) une description de l'atteinte à la sécurité ou de la compromission;

i) une description des données compromises, y compris, le cas échéant, les catégories de données à caractère personnel précisées à l'article 9, paragraphe 1, et à l'article 10 du règlement (UE) 2016/679;

j) dans la mesure du possible, une estimation du nombre approximatif d'utilisateurs de portefeuille et d'autres personnes physiques affectés;

k) une description des incidences potentielles sur les parties utilisatrices de portefeuille ou sur les utilisateurs de portefeuille et, dans ce dernier cas, si nécessaire, une indication des mesures que les utilisateurs de portefeuille peuvent prendre pour atténuer ces incidences potentielles;

l) une description des mesures prises ou prévues pour faire migrer les utilisateurs de portefeuille affectés vers d'autres solutions de portefeuille, ou le cas échéant et s'il y a lieu, vers d'autres services.

Article 10

Système d'information

Les États membres transmettent les informations prévues aux articles 3, 5, 7 et 9 à la Commission et aux points de contact uniques des États membres désignés en vertu de l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014, par l'intermédiaire du CIRAS géré par l'ENISA, ou d'un système équivalent approuvé par les États membres et la Commission.

Article 11

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, à l'exception de l'article 10, qui est applicable à partir du 7 mai 2026.

Fait à Bruxelles, le 6 mai 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Critères applicables à l'évaluation d'une atteinte à la sécurité ou d'une compromission

1. Les États membres fondent leur évaluation d'une atteinte à la sécurité ou d'une compromission sur les critères suivants:

   a) l'atteinte à la sécurité ou la compromission a causé ou est susceptible de causer la mort d'une personne physique ou des dommages considérables à la santé d'une personne physique;

   b) un accès effectif non autorisé, ou suspecté d'être malveillant, au réseau et aux systèmes d'information d'un fournisseur de portefeuille, du fournisseur des mécanismes de validation mentionnés à l'article 5 *bis*, paragraphe 8, du règlement (UE) nº 910/2014, ou du fournisseur du schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie (entité concernée), s'est produit ou peut se produire et pourrait entraîner une perturbation opérationnelle grave, et ces systèmes sont des éléments essentiels de la solution de portefeuille affectée, des mécanismes de validation affectés mentionnés à l'article 5 *bis*, paragraphe 8, du règlement (UE) nº 910/2014 ou du schéma d'identification électronique affecté dans le cadre duquel une solution de portefeuille est fournie;

   c) une solution de portefeuille, un mécanisme de validation mentionné à l'article 5 *bis*, paragraphe 8, du règlement (UE) nº 910/2014, ou un schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie, ou une partie de ceux-ci:

      — est entièrement indisponible, ou il est prévisible qu'il ou elle le soit, pour les utilisateurs de portefeuille ou les parties utilisatrices de portefeuille pendant plus de 12 heures consécutives,

      — est indisponible, ou il est prévisible qu'il ou elle le soit, pour les utilisateurs de portefeuille ou les parties utilisatrices de portefeuille pendant plus de 16 heures, le calcul étant effectué sur la base d'une semaine civile;

   d) on estime que plus de 1 % des utilisateurs de portefeuille ou des parties utilisatrices de portefeuille sont touchés, ou devraient l'être, par la disponibilité limitée de la solution de portefeuille ou des services fournis par les entités concernées en ce qui concerne la solution de portefeuille;

   e) il existe une possibilité de compromission, ou il y a eu une compromission de l'accès physique limité au personnel de confiance des entités concernées, ou de la protection de cet accès, sur un ou plusieurs des sites de réseaux et de systèmes d'information sur lesquels reposent la solution de portefeuille, la fourniture des mécanismes de validation mentionnés à l'article 5 *bis*, paragraphe 8, du règlement (UE) nº 910/2014 associés à une solution de portefeuille ou le schéma d'identification électronique dans le cadre duquel une solution de portefeuille est fournie;

   f) les aspects relatifs à la vie privée, l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées dans la solution de portefeuille sont compromis, ou peuvent l'être, d'une ou de plusieurs des manières suivantes:

      — la compromission a un impact sur plus de 1 % des utilisateurs de portefeuille de la solution de portefeuille affectée ou sur plus de 100 000 de ces utilisateurs, le nombre le plus petit étant retenu,

      — elle résulte d'une activité suspectée d'être malveillante qui a atteint son but,

      — elle résulte ou est susceptible de résulter d'une ou de plusieurs vulnérabilités connues, y compris celles qui sont gérées conformément au règlement d'exécution (UE) 2024/2981 de la Commission ([1]),

      — elle est susceptible d'affecter les données à caractère personnel de telle sorte que les droits et les libertés des personnes physiques concernées pourraient être menacés et, en particulier, en cas de violation de données à caractère au sens de l'article 9, paragraphe 1, et de l'article 10 du règlement (UE) 2016/679,

([1]) Règlement d'exécution (UE) 2024/2981 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 la certification des portefeuilles européens d'identité numérique (JO L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— elle est susceptible d'affecter les communications électroniques personnelles,

— elle est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques,

— elle est susceptible d'affecter les personnes vulnérables;

g) la certification de la solution de portefeuille a été annulée ou il est prévu qu'elle le soit;

h) l'atteinte à la sécurité ou la compromission a causé ou peut causer à une entité concernée une perte financière directe, et cette perte est supérieure à 500 000 EUR ou, le cas échéant, à 5 % du chiffre d'affaires annuel total de l'entité concernée au cours de l'exercice précédent, le montant le plus faible étant retenu.

2. Les États membres ne tiennent pas compte des conséquences prévues d'une opération de maintenance effectuée par les entités concernées ou en leur nom, à condition que cette opération de maintenance:

a) ait fait l'objet d'une notification préalable aux utilisateurs de portefeuille, aux parties utilisatrices de portefeuille et aux organes de contrôle compétents potentiellement affectés;

b) ne remplisse aucun des critères énoncés au paragraphe 1 de la présente annexe.

3. En ce qui concerne le paragraphe 1, point c), la durée d'un incident affectant la disponibilité est mesurée à partir du moment où la fourniture normale du service concerné est interrompue et jusqu'au moment où le service est rétabli et opérationnel. Lorsqu'une entité concernée n'est pas en mesure de déterminer le moment à partir duquel l'interruption a commencé, la durée de l'incident est mesurée à partir du moment où l'incident a été détecté, ou de celui où l'incident a été enregistré dans les journaux du réseau, du système ou dans d'autres sources de données, selon l'éventualité qui intervient en premier. L'indisponibilité totale d'un service est mesurée à partir du moment où le service est totalement indisponible pour les utilisateurs, jusqu'au moment où les activités ou opérations régulières ont retrouvé le niveau de service fourni avant l'incident. Lorsqu'une entité concernée n'est pas en mesure de déterminer quand l'indisponibilité totale d'un service a commencé, cette indisponibilité est mesurée à partir du moment où elle a été détectée par cette entité.

4. En ce qui concerne le paragraphe 1, point d), il est considéré que la disponibilité d'un service est limitée en particulier lorsque son délai de réponse est considérablement plus long que la moyenne, ou lorsque toutes les fonctionnalités d'un service ne sont pas disponibles. Dans la mesure du possible, des critères objectifs fondés sur les délais moyens de réponse des services sont utilisés pour évaluer les retards dans le délai de réponse.

5. Afin de déterminer les pertes financières directes résultant d'une atteinte ou d'une compromission visée au paragraphe 1, point h), les entités concernées tiennent compte de toutes les pertes financières qu'elles ont subies à la suite de l'incident, telles que les coûts du remplacement ou du déplacement de logiciels, de matériel ou d'infrastructures, les frais de personnel, y compris les coûts liés au remplacement ou au déménagement du personnel, au recrutement de personnel supplémentaire, à la rémunération des heures supplémentaires et à la récupération des compétences perdues ou altérées, les frais dus au non-respect d'obligations contractuelles, les coûts de dédommagement et d'indemnisation des clients, les pertes dues aux recettes non perçues, les coûts liés à la communication interne et externe et les frais de conseil, notamment les coûts liés au conseil juridique, aux services d'investigation numérique et aux services de remédiation. Les coûts nécessaires au fonctionnement quotidien de l'activité, tels que les coûts de maintenance générale des infrastructures, des équipements, du matériel et des logiciels, les améliorations et les initiatives d'évaluation des risques, ainsi que les primes d'assurance, ne sont pas considérés comme des pertes financières résultant d'un incident. Les entités concernées calculent le montant des pertes financières sur la base des données disponibles et ont recours à une estimation lorsqu'il est impossible de déterminer le montant réel de ces pertes.