Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/847

7.5.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/847 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 6ης Μαΐου 2025

για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την αντίδραση σε παραβιάσεις της ασφάλειας των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ ([1]), και ιδίως το άρθρο 5ε παράγραφος 5,

Εκτιμώντας τα ακόλουθα:

(1) Το ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα (στο εξής: πλαίσιο) που θεσπίστηκε με τον κανονισμό (ΕΕ) αριθ. 910/2014 αποτελεί κρίσιμη συνιστώσα της δημιουργίας ενός ασφαλούς και διαλειτουργικού οικοσυστήματος ψηφιακής ταυτότητας σε ολόκληρη την Ένωση. Με τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας (στο εξής: πορτοφόλια) ως ακρογωνιαίο λίθο του, το πλαίσιο αποσκοπεί στη διευκόλυνση της πρόσβασης σε υπηρεσίες σε όλα τα κράτη μέλη, με παράλληλη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής.

(2) Στις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του παρόντος κανονισμού εφαρμόζονται οι κανονισμοί (ΕΕ) 2016/679 ([2]) και (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]) και, κατά περίπτωση, η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]). Οι κανόνες για την αξιολόγηση και την παροχή πληροφοριών που θεσπίζονται δυνάμει του παρόντος κανονισμού δεν θίγουν την υποχρέωση κοινοποίησης των παραβιάσεων δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή, κατά περίπτωση, δυνάμει του κανονισμού (ΕΕ) 2016/679 ή του κανονισμού (ΕΕ) 2018/1725, και την υποχρέωση γνωστοποίησης των παραβιάσεων δεδομένων προσωπικού χαρακτήρα στα υποκείμενα των δεδομένων, κατά περίπτωση, δυνάμει των εν λόγω κανονισμών.

(3) Η Επιτροπή αξιολογεί τακτικά νέες τεχνολογίες, πρακτικές, πρότυπα και τεχνικές προδιαγραφές. Προκειμένου να διασφαλιστεί το υψηλότερο δυνατό επίπεδο εναρμόνισης μεταξύ των κρατών μελών για την ανάπτυξη και την πιστοποίηση των πορτοφολιών, οι τεχνικές προδιαγραφές που ορίζονται στον παρόντα κανονισμό βασίζονται στις εργασίες που πραγματοποιήθηκαν με βάση τη σύσταση (ΕΕ) 2021/946 της Επιτροπής ([5]), και ιδίως την αρχιτεκτονική και το πλαίσιο αναφοράς που αποτελεί μέρος του. Σύμφωνα με την αιτιολογική σκέψη 75 του κανονισμού (ΕΕ) 2024/1183 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]), η Επιτροπή θα πρέπει να επανεξετάζει και, εάν χρειάζεται, να επικαιροποιεί τον παρόντα κανονισμό, ώστε να συμβαδίζει με τις διεθνείς εξελίξεις, την αρχιτεκτονική και το πλαίσιο αναφοράς και να ακολουθούνται οι βέλτιστες πρακτικές στην εσωτερική αγορά.

([1]) ΕΕ L 257 της 28.8.2014, σ. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39, ELI: http://data. europa.eu/eli/reg/2018/1725/oj).

([4]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Σύσταση (ΕΕ) 2021/946 της Επιτροπής, της 3ης Ιουνίου 2021, σχετικά με κοινή εργαλειοθήκη της Ένωσης για μια συντονισμένη προσέγγιση όσον αφορά το ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα (ΕΕ L 210 της 14.6.2021, σ. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Κανονισμός (ΕΕ) 2024/1183 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Απριλίου 2024, για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά τη θέσπιση ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα (ΕΕ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) Σε περίπτωση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο των υλοποιήσεων πορτοφολιού ή των μηχανισμών επικύρωσης που αναφέρονται στο άρθρο 5α παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014, ή του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχονται οι υλοποιήσεις πορτοφολιού, η αντίδραση στις εν λόγω περιπτώσεις παραβίασης της ασφάλειας και έκθεσης σε κίνδυνο πρέπει να ακολουθεί με ταχύ, συντονισμένο και ασφαλή τρόπο σε όλα τα κράτη μέλη για την προστασία των χρηστών και τη διατήρηση της εμπιστοσύνης στο οικοσύστημα ψηφιακής ταυτότητας. Αυτό δεν θίγει τις διατάξεις της οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]) και των κανονισμών (ΕΕ) 2019/881 ([8]) και (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]), ιδίως όσον αφορά τον χειρισμό περιστατικών ή τρωτών σημείων και τον χαρακτηρισμό τους ως παραβιάσεων της ασφάλειας. Ως εκ τούτου, τα κράτη μέλη θα πρέπει να μεριμνούν για την έγκαιρη αναστολή της παροχής και της χρήσης πορτοφολιών που επηρεάζονται από παραβίαση της ασφάλειας ή έκθεση σε κίνδυνο ή, κατά περίπτωση, για την απόσυρσή τους.

(5) Για τη διασφάλιση της κατάλληλης αντίδρασης σε περίπτωση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο, τα κράτη μέλη θα πρέπει να αξιολογούν αν η παραβίαση της ασφάλειας ή η έκθεση σε κίνδυνο υλοποίησης πορτοφολιού, των μηχανισμών επικύρωσης που αναφέρονται στο άρθρο 5α παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014, ή του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχεται υλοποίηση πορτοφολιού, επηρεάζει την αξιοπιστία της εν λόγω υλοποίησης πορτοφολιού ή άλλων υλοποιήσεων πορτοφολιού. Η εν λόγω αξιολόγηση θα πρέπει να βασίζεται σε ενιαία κριτήρια, όπως ο αριθμός και η κατηγορία των χρηστών πορτοφολιού, των φυσικών προσώπων και των βασιζόμενων σε πορτοφόλι μερών που επηρεάζονται, η φύση των επηρεαζόμενων δεδομένων, η διάρκεια της έκθεσης σε κίνδυνο ή της παραβίασης της ασφάλειας, η περιορισμένη διαθεσιμότητα μιας υπηρεσίας και οι οικονομικές ζημίες, καθώς και η πιθανή έκθεση σε κίνδυνο δεδομένων προσωπικού χαρακτήρα. Τα κριτήρια αυτά θα πρέπει να παρέχουν στα κράτη μέλη ευελιξία και διακριτική ευχέρεια ώστε να μπορούν να διαπιστώσουν με αναλογικό τρόπο αν επηρεάζεται η αξιοπιστία μιας υλοποίησης πορτοφολιού, καθώς και αν ενδείκνυται η αναστολή ή —όταν αυτό δικαιολογείται από τη σοβαρότητα της παραβίασης ή της έκθεσης σε κίνδυνο— η απόσυρση της υλοποίησης πορτοφολιού. Τα εν λόγω κριτήρια δεν θα πρέπει να ενεργοποιούν την αυτόματη απόσυρση μιας υλοποίησης πορτοφολιού ή την αυτόματη αναστολή της παροχής και της χρήσης μιας υλοποίησης πορτοφολιού, αλλά θα πρέπει να λαμβάνονται δεόντως υπόψη από τα κράτη μέλη κατά τη λήψη απόφασης σχετικά με την αναγκαιότητα απόσυρσης ή αναστολής της παροχής και της χρήσης μιας υλοποίησης πορτοφολιού.

(6) Λόγω των επιπτώσεων και της ταλαιπωρίας που συνεπάγεται η αναστολή της χρήσης υλοποιήσεων πορτοφολιού, τα κράτη μέλη θα πρέπει να αξιολογούν αν η ανάκληση των βεβαιώσεων μονάδας πορτοφολιού ή οποιαδήποτε άλλα πρόσθετα μέτρα είναι αναγκαία για την κατάλληλη αντίδραση σε περίπτωση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο.

(7) Προκειμένου οι χρήστες να τηρούνται ενήμεροι για το καθεστώς των πορτοφολιών τους, πρέπει να τους παρέχονται επαρκείς πληροφορίες σχετικά με περιπτώσεις παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο που επηρεάζουν τα πορτοφόλια τους. Δεδομένου ότι τα βασιζόμενα σε πορτοφόλι μέρη που είναι καταχωρισμένα στην Ένωση μπορούν επίσης να επηρεάζονται από περιπτώσεις παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο, πρέπει να τους κοινοποιούνται και σχετικές πληροφορίες που αφορούν περιπτώσεις παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο.

(8) Για την ενίσχυση της διαφάνειας και τη διαμόρφωση κλίματος εμπιστοσύνης στο οικοσύστημα ψηφιακής ταυτότητας, στις πληροφορίες σχετικά με περιπτώσεις παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο, καθώς και σχετικά με τις συνέπειές τους, θα πρέπει να περιλαμβάνονται τουλάχιστον οι πληροφορίες που απαιτούνται βάσει του παρόντος κανονισμού. Ωστόσο, οι πληροφορίες σχετικά με περιπτώσεις παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο που κοινοποιούνται στους χρήστες πορτοφολιού και στα βασιζόμενα σε πορτοφόλι μέρη θα πρέπει να υποβάλλονται σε διεξοδική αξιολόγηση, ώστε να προλαμβάνεται και να ελαχιστοποιείται ο κίνδυνος εκμετάλλευσής τους από επιτιθέμενους.

([7]) Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα) (ΕΕ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Για να καταστεί εκ νέου δυνατή η πρόσβαση των χρηστών στις οικείες μονάδες πορτοφολιού μετά την αντιμετώπιση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο, το κράτος μέλος που παρείχε τις υλοποιήσεις πορτοφολιού θα πρέπει να αποκαταστήσει την παροχή και τη χρήση των εν λόγω υλοποιήσεων πορτοφολιού χωρίς αδικαιολόγητη καθυστέρηση. Αυτό μπορεί να επιτευχθεί με την αποκατάσταση των μονάδων πορτοφολιού, με την έκδοση μονάδων πορτοφολιού που παρέχονται στο πλαίσιο νέας έκδοσης των υλοποιήσεων πορτοφολιού ή με την επανέκδοση νέων έγκυρων βεβαιώσεων μονάδας πορτοφολιού. Οι θιγόμενοι χρήστες πορτοφολιού, τα βασιζόμενα σε πορτοφόλι μέρη, τα ενιαία σημεία επαφής που ορίζονται σύμφωνα με το άρθρο 46γ παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014 και η Επιτροπή πρέπει να ενημερώνονται δεόντως.

(10) Προκειμένου να διασφαλιστεί ότι η απόσυρση πορτοφολιών σε περίπτωση που παραβίαση της ασφάλειας ή έκθεση σε κίνδυνο δεν έχει αντιμετωπιστεί εντός τριών μηνών από την αναστολή, ή σε περίπτωση που αυτό δικαιολογείται από τη σοβαρότητα της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο, το κράτος μέλος θα πρέπει να μεριμνά για την ανάκληση των σχετικών βεβαιώσεων μονάδας πορτοφολιού και να εξασφαλίζει ότι δεν είναι δυνατή η επαναφορά τους σε κατάσταση ισχύος, ούτε η έκδοση ή η παροχή τους σε υφιστάμενες μονάδες πορτοφολιού. Επιπλέον, δεν θα πρέπει να παρέχονται νέες μονάδες πορτοφολιού στο πλαίσιο της επηρεαζόμενης υλοποίησης πορτοφολιού. Για λόγους διαφάνειας, οι χρήστες, τα βασιζόμενα σε πορτοφόλι μέρη, τα ενιαία σημεία επαφής που ορίζονται σύμφωνα με το άρθρο 46γ παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014 και η Επιτροπή πρέπει να ενημερώνονται για την απόσυρση. Στο πλαίσιο αυτό περιλαμβάνεται περιγραφή των δυνητικών επιπτώσεων στους χρήστες πορτοφολιού, και συγκεκριμένα στη διαχείριση των εκδοθεισών βεβαιώσεων, ή στα βασιζόμενα σε πορτοφόλι μέρη.

(11) Η περίοδος των τριών μηνών μετά την αναστολή της παροχής και της χρήσης μιας υλοποίησης πορτοφολιού, και κατά τη διάρκεια της οποίας πρέπει να αντιμετωπιστεί η παραβίαση της ασφάλειας ή η έκθεση σε κίνδυνο που οδήγησε στην εν λόγω αναστολή, θα πρέπει να προβλέπει προθεσμία μετά την οποία πρέπει να αποσυρθεί η υλοποίηση πορτοφολιού, εκτός εάν έχει εφαρμοστεί κατάλληλο διορθωτικό μέτρο. Ωστόσο, τα κράτη μέλη είναι ελεύθερα να απαιτούν την αντιμετώπιση της παραβίασης ή της έκθεσης σε κίνδυνο εντός προθεσμίας μικρότερης των τριών μηνών, λαμβάνοντας υπόψη, ειδικότερα και κατά περίπτωση, την έκταση, τη διάρκεια και τις συνέπειες της εν λόγω παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο. Όταν η παραβίαση της ασφάλειας ή η έκθεση σε κίνδυνο δεν αντιμετωπίζεται ή δεν μπορεί να αντιμετωπιστεί εντός της προθεσμίας που ορίζεται από το κράτος μέλος, το κράτος μέλος μπορεί να απαιτήσει την απόσυρση της υλοποίησης πορτοφολιού πριν από τη λήξη της περιόδου των τριών μηνών. Τα κράτη μέλη θα πρέπει να χρησιμοποιούν αυτή τη χρονική περίοδο κατά τη διάρκεια της οποίας πρέπει να αντιμετωπιστεί η παραβίαση της ασφάλειας ή η έκθεση σε κίνδυνο που οδήγησε στην αναστολή της παροχής και της χρήσης μιας υλοποίησης πορτοφολιού για την προετοιμασία της πιθανής απόσυρσης της εν λόγω υλοποίησης πορτοφολιού και των κοινοποιήσεων που προκύπτουν από την απόσυρση.

(12) Προκειμένου να μειωθεί ο διοικητικός φόρτος για τα κράτη μέλη όσον αφορά τις πληροφορίες που πρέπει να παρέχονται, σύμφωνα με τον παρόντα κανονισμό, στην Επιτροπή και σε άλλα κράτη μέλη, τα κράτη μέλη θα πρέπει να χρησιμοποιούν υφιστάμενα μέσα κοινοποίησης, όπως το σύστημα αναφοράς και ανάλυσης κυβερνοπεριστατικών (στο εξής: CIRAS), το οποίο διαχειρίζεται ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (στο εξής: ENISA). Όσον αφορά τους εναλλακτικούς διαύλους ή τα εναλλακτικά μέσα που πρέπει να χρησιμοποιούνται για την ενημέρωση τόσο των θιγόμενων χρηστών πορτοφολιού λόγω παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο όσο και των βασιζόμενων σε πορτοφόλι μερών, τα κράτη μέλη θα πρέπει να μεριμνούν ώστε οι σχετικές πληροφορίες να παρέχονται με σαφή, ολοκληρωμένο και εύκολα προσβάσιμο τρόπο. Οι δίαυλοι για την παροχή των εν λόγω πληροφοριών στους θιγόμενους χρήστες πορτοφολιού και στα βασιζόμενα σε πορτοφόλι μέρη θα πρέπει να περιλαμβάνουν κατάλληλες λύσεις για τη μετάδοση μέσω ιστοτόπου, την παρακολούθηση σε πραγματικό χρόνο των επικαιροποιήσεων ιστοτόπου και τη συνάθροιση ειδήσεων.

(13) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725, η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε την 31η Ιανουαρίου 2025.

(14) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 48 του κανονισμού (ΕΕ) αριθ. 910/2014,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Αντικείμενο

Ο παρών κανονισμός θεσπίζει κανόνες για την αντίδραση σε περιπτώσεις παραβίασης της ασφάλειας των πορτοφολιών, των μηχανισμών επικύρωσης που αναφέρονται στο άρθρο 5α παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014, καθώς και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχονται τα πορτοφόλια.

Άρθρο 2

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) «υλοποίηση πορτοφολιού»: συνδυασμός λογισμικού, υλισμικού, υπηρεσιών, ρυθμίσεων και διαμορφώσεων, συμπεριλαμβανομένων των στιγμιότυπων πορτοφολιού, μίας ή περισσότερων ασφαλών κρυπτογραφικών εφαρμογών πορτοφολιού και μίας ή περισσότερων ασφαλών κρυπτογραφικών διατάξεων πορτοφολιού·

2) «χρήστης πορτοφολιού»: χρήστης που έχει τον έλεγχο της μονάδας πορτοφολιού·

3) «βασιζόμενο σε πορτοφόλι μέρος»: βασιζόμενο μέρος που προτίθεται να βασίζεται σε μονάδες πορτοφολιού για την παροχή δημόσιων ή ιδιωτικών υπηρεσιών μέσω ψηφιακής αλληλεπίδρασης·

4) «στιγμιότυπο πορτοφολιού»: η εφαρμογή όπως έχει εγκατασταθεί και έχει διαμορφωθεί σε διάταξη ή περιβάλλον χρήστη πορτοφολιού, η οποία αποτελεί μέρος μονάδας πορτοφολιού, και την οποία χρησιμοποιεί ο χρήστης πορτοφολιού για να αλληλεπιδρά με τη μονάδα πορτοφολιού·

5) «ασφαλής κρυπτογραφική εφαρμογή πορτοφολιού»: εφαρμογή που διαχειρίζεται κρίσιμα περιουσιακά στοιχεία μέσω της σύνδεσής της με τις κρυπτογραφικές και μη κρυπτογραφικές λειτουργίες που παρέχει η ασφαλής κρυπτογραφική διάταξη πορτοφολιού και μέσω της χρήσης αυτών·

6) «ασφαλής κρυπτογραφική διάταξη πορτοφολιού»: ανθεκτική στην παραβίαση διάταξη η οποία παρέχει περιβάλλον που συνδέεται με την ασφαλή κρυπτογραφική εφαρμογή πορτοφολιού και χρησιμοποιείται από αυτή για την προστασία κρίσιμων περιουσιακών στοιχείων και την παροχή κρυπτογραφικών λειτουργιών για την ασφαλή εκτέλεση κρίσιμων λειτουργιών·

7) «πάροχος πορτοφολιού»: φυσικό ή νομικό πρόσωπο το οποίο παρέχει υλοποιήσεις πορτοφολιού·

8) «μονάδα πορτοφολιού»: μοναδική διαμόρφωση μιας υλοποίησης πορτοφολιού που περιλαμβάνει στιγμιότυπα πορτοφολιού, ασφαλείς κρυπτογραφικές εφαρμογές πορτοφολιού και ασφαλείς κρυπτογραφικές διατάξεις πορτοφολιού, που παρέχονται από έναν πάροχο πορτοφολιού σε μεμονωμένο χρήστη πορτοφολιού·

9) «κρίσιμα περιουσιακά στοιχεία»: περιουσιακά στοιχεία εντός μονάδας πορτοφολιού ή σχετιζόμενα με μονάδα πορτοφολιού, τα οποία είναι τόσο εξέχουσας σημασίας ώστε όταν τίθεται σε κίνδυνο η διαθεσιμότητα, η εμπιστευτικότητα ή η ακεραιότητά τους, αυτό μπορεί να έχει πολύ σοβαρές, ανεπανόρθωτες επιπτώσεις στην ικανότητα των ατόμων να βασίζονται στη μονάδα πορτοφολιού·

10) «βεβαίωση μονάδας πορτοφολιού»: αντικείμενο δεδομένων που περιγράφει τα συστατικά στοιχεία της μονάδας πορτοφολιού ή καθιστά δυνατή την επαλήθευση ταυτότητας και την επικύρωση των εν λόγω συστατικών στοιχείων.

Άρθρο 3

Διαπίστωση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο

1. Με την επιφύλαξη των διατάξεων της οδηγίας (ΕΕ) 2022/2555 και των κανονισμών (ΕΕ) 2019/881 και (ΕΕ) 2024/2847, τα κράτη μέλη λαμβάνουν δεόντως υπόψη τα κριτήρια που καθορίζονται στο παράρτημα Ι του παρόντος κανονισμού προκειμένου να αξιολογηθεί αν η παραβίαση της ασφάλειας ή η έκθεση σε κίνδυνο υλοποίησης πορτοφολιού, των μηχανισμών επικύρωσης που αναφέρονται στο άρθρο 5α παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014, ή του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχεται υλοποίηση πορτοφολιού, επηρεάζει την αξιοπιστία τους ή την αξιοπιστία άλλων υλοποιήσεων πορτοφολιού.

2. Σε περίπτωση που κράτος μέλος διαπιστώσει, βάσει της αξιολόγησης που προβλέπεται στην παράγραφο 1, ότι μια περίπτωση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο επηρεάζει την αξιοπιστία μιας υλοποίησης πορτοφολιού και αναστέλλει την παροχή και τη χρήση της συγκεκριμένης υλοποίησης πορτοφολιού, το εν λόγω κράτος μέλος λαμβάνει τα μέτρα που προβλέπονται στα άρθρα 4 και 5. Σε περίπτωση που κράτος μέλος αποσύρει την υλοποίηση πορτοφολιού, το εν λόγω κράτος μέλος λαμβάνει τα μέτρα που προβλέπονται στα άρθρα 8 και 9.

3. Σε περίπτωση που κράτος μέλος λάβει γνώση πληροφοριών σχετικά με πιθανή περίπτωση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο η οποία ενδέχεται να επηρεάσει την αξιοπιστία μίας ή περισσότερων υλοποιήσεων πορτοφολιού που παρέχονται από άλλο κράτος μέλος, το εν λόγω κράτος μέλος ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση, την Επιτροπή και τα ενιαία σημεία επαφής των θιγόμενων κρατών μελών που έχουν οριστεί σύμφωνα με το άρθρο 46γ παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014 σχετικά με το γεγονός αυτό. Στη σχετική κοινοποίηση περιλαμβάνονται οι πληροφορίες που καθορίζονται στο άρθρο 5 παράγραφος 2.

4. Το κράτος μέλος που παραλαμβάνει τις πληροφορίες που παρέχονται σύμφωνα με την παράγραφο 3 λαμβάνει τα μέτρα που προβλέπονται στις παραγράφους 1 και 2 χωρίς αδικαιολόγητη καθυστέρηση.

Άρθρο 4

Αναστολή της παροχής και της χρήσης πορτοφολιών και άλλα νομικά διορθωτικά μέτρα

1. Τα κράτη μέλη διασφαλίζουν ότι δεν παρέχονται, χρησιμοποιούνται ή ενεργοποιούνται μονάδες πορτοφολιού στο πλαίσιο της ανασταλείσας υλοποίησης πορτοφολιού.

2. Τα κράτη μέλη αξιολογούν αν η ανάκληση βεβαιώσεων μονάδας πορτοφολιού των μονάδων πορτοφολιού που επηρεάζονται από την αναστολή υλοποίησης πορτοφολιού, ή από οποιοδήποτε άλλο πρόσθετο νομικό διορθωτικό μέτρο, είναι αναγκαία για την κατάλληλη αντίδραση σε περίπτωση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο.

3. Τα μέτρα που προβλέπονται στις παραγράφους 1 και 2 λαμβάνονται χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, το αργότερο εντός 24 ωρών από την αναστολή της παροχής και τη χρήση της υλοποίησης πορτοφολιού που επηρεάζεται από την παραβίαση ή την έκθεση σε κίνδυνο.

4. Τα μέτρα που προβλέπονται στις παραγράφους 1 και 2 δεν εμποδίζουν τους θιγόμενους χρήστες πορτοφολιού να ασκούν το δικαίωμά τους όσον αφορά τη φορητότητα των δεδομένων που ορίζεται στο άρθρο 5α παράγραφος 4 στοιχείο ζ) του κανονισμού (ΕΕ) αριθ. 910/2014. Αυτό ισχύει υπό την προϋπόθεση ότι το εν λόγω δικαίωμα μπορεί να ασκείται από χρήστες πορτοφολιού χωρίς να υπονομεύεται η ασφάλεια των κρίσιμων περιουσιακών στοιχείων των επηρεαζόμενων μονάδων πορτοφολιού, λαμβανομένων ιδίως υπόψη των λόγων αναστολής και της ανάγκης διασφάλισης της αποτελεσματικής προστασίας των εν λόγω περιουσιακών στοιχείων από καταχρήσεις.

Άρθρο 5

Πληροφορίες σχετικά με αναστολές και νομικά διορθωτικά μέτρα

1. Παρέχονται πληροφορίες με σαφή, ολοκληρωμένο και εύκολα προσβάσιμο τρόπο σχετικά με την αναστολή της παροχής και τη χρήση υλοποίησης πορτοφολιού, χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 24 ωρών από την αναστολή της παροχής και της χρήσης της υλοποίησης πορτοφολιού:

α) στα ενιαία σημεία επαφής που ορίζονται σύμφωνα με το άρθρο 46γ παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014·

β) στην Επιτροπή·

γ) στους θιγόμενους χρήστες πορτοφολιού·

δ) στα βασιζόμενα σε πορτοφόλι μέρη που έχουν καταχωριστεί σύμφωνα με το άρθρο 5β του κανονισμού (ΕΕ) αριθ. 910/2014.

2. Οι πληροφορίες που παρέχονται σύμφωνα με την παράγραφο 1 περιλαμβάνουν τουλάχιστον τα ακόλουθα:

α) το όνομα / την επωνυμία του παρόχου της υλοποίησης πορτοφολιού, η παροχή και η χρήση της οποίας έχει ανασταλεί·

β) την ονομασία και το αναγνωριστικό αναφοράς της εν λόγω υλοποίησης πορτοφολιού, όπως αναφέρεται στον κατάλογο πιστοποιημένων πορτοφολιών που καταρτίζεται σύμφωνα με το άρθρο 5δ του κανονισμού (ΕΕ) αριθ. 910/2014 και, κατά περίπτωση, τις σχετικές εκδόσεις·

γ) την ημερομηνία και την ώρα εντοπισμού της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο·

δ) εάν είναι γνωστή, την ημερομηνία και την ώρα κατά την οποία συντελέστηκε η παραβίαση της ασφάλειας ή η έκθεση σε κίνδυνο, με βάση τα αρχεία καταγραφής του δικτύου ή του συστήματος ή άλλες πηγές δεδομένων·

ε) την ημερομηνία και την ώρα αναστολής της υλοποίησης πορτοφολιού·

στ) τα στοιχεία επικοινωνίας, συμπεριλαμβανομένων τουλάχιστον διεύθυνσης ηλεκτρονικού ταχυδρομείου και αριθμού τηλεφώνου του κοινοποιούντος κράτους μέλους και, εάν διαφέρει, του παρόχου πορτοφολιού που αναφέρεται στο στοιχείο α)·

ζ) περιγραφή της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο·

η) περιγραφή των δεδομένων που έχουν εκτεθεί σε κίνδυνο, συμπεριλαμβανομένων, κατά περίπτωση, των κατηγοριών δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 9 παράγραφος 1 και στο άρθρο 10 του κανονισμού (ΕΕ) 2016/679·

θ) όπου είναι δυνατόν, εκτίμηση του κατά προσέγγιση αριθμού των θιγόμενων χρηστών πορτοφολιού και άλλων φυσικών προσώπων που επηρεάζονται·

ι) περιγραφή των δυνητικών επιπτώσεων στα βασιζόμενα σε πορτοφόλι μέρη ή στους χρήστες πορτοφολιού και, στη δεύτερη περίπτωση, τυχόν ενδείξεις μέτρων που μπορούν να λάβουν οι χρήστες πορτοφολιού για τον μετριασμό των εν λόγω δυνητικών επιπτώσεων, κατά περίπτωση·

ια) περιγραφή των μέτρων που έχουν ληφθεί ή πρόκειται να ληφθούν για την αντιμετώπιση της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο, μαζί με προγραμματισμό και προθεσμία για τη σχετική αντιμετώπιση·

ιβ) κατά περίπτωση και όπου αυτό κρίνεται σκόπιμο, περιγραφή των μέτρων που έχουν ληφθεί ή πρόκειται να ληφθούν για τη μετάβαση των θιγόμενων χρηστών πορτοφολιού σε εναλλακτικές υλοποιήσεις πορτοφολιού ή υπηρεσίες.

Άρθρο 6

Αποκατάσταση της παροχής και της χρήσης πορτοφολιών

Σε περίπτωση που κρίνεται αναγκαίο να διασφαλιστεί η αποκατάσταση της παροχής, της ενεργοποίησης και της χρήσης υλοποίησης πορτοφολιού, τα κράτη μέλη μεριμνούν, χωρίς αδικαιολόγητη καθυστέρηση, για:

1) την αποκατάσταση της παροχής και της χρήσης των μονάδων πορτοφολιού που παρέχονται στο πλαίσιο της εν λόγω υλοποίησης πορτοφολιού, με την έκδοση μονάδας πορτοφολιού που παρέχεται στο πλαίσιο νέας έκδοσης της υλοποίησης πορτοφολιού σε όλους τους θιγόμενους χρήστες·

2) την έκδοση νέων βεβαιώσεων μονάδας πορτοφολιού σε νέες μονάδες πορτοφολιού ή, κατά περίπτωση, σε μονάδες πορτοφολιού που είχαν εκδοθεί προηγουμένως, υπό την προϋπόθεση ότι οι εν λόγω μονάδες πορτοφολιού πληρούν τις απαιτήσεις ασφάλειας που ισχύουν μετά την αντιμετώπιση της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο·

3) την κατάργηση τυχόν μέτρων που εφαρμόζονται σύμφωνα με το άρθρο 4 και εμποδίζουν την παροχή νέων μονάδων πορτοφολιού στο πλαίσιο της επηρεαζόμενης υλοποίησης πορτοφολιού, σε περίπτωση που τα εν λόγω μέτρα συνδέονταν αποκλειστικά και μόνο με την παραβίαση της ασφάλειας ή την έκθεση σε κίνδυνο που έχει πλέον αντιμετωπιστεί.

Άρθρο 7

Πληροφορίες σχετικά με την αποκατάσταση

Σε περίπτωση που κράτος μέλος αποκαθιστά υλοποίηση πορτοφολιού, το εν λόγω κράτος μέλος διασφαλίζει ότι:

1) παρέχονται, χωρίς αδικαιολόγητη καθυστέρηση, πληροφορίες σχετικά με το γεγονός αυτό σε όλα τα μέρη που έχουν λάβει πληροφορίες σχετικά με την αναστολή της παροχής και της χρήσης της εν λόγω υλοποίησης πορτοφολιού σύμφωνα με το άρθρο 5 παράγραφος 1·

2) οι πληροφορίες που παρέχονται σύμφωνα με το σημείο 1) περιλαμβάνουν τουλάχιστον τα στοιχεία που αναφέρονται στο άρθρο 5 παράγραφος 2 στοιχεία α), β), στ), ζ) και η), καθώς και τα ακόλουθα:

   α) την ημερομηνία και την ώρα αντιμετώπισης της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο·

   β) την ημερομηνία και την ώρα αποκατάστασης της επηρεαζόμενης υλοποίησης πορτοφολιού και, κατά περίπτωση, των επηρεαζόμενων μονάδων πορτοφολιού που παρέχονται στο πλαίσιο της εν λόγω υλοποίησης πορτοφολιού·

   γ) περιγραφή των μέτρων που έχουν ληφθεί για την αντιμετώπιση της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο·

   δ) περιγραφή των δυνητικών υπολειπόμενων επιπτώσεων στα βασιζόμενα σε πορτοφόλι μέρη ή στους χρήστες πορτοφολιού και, στη δεύτερη περίπτωση, τυχόν ενδείξεις μέτρων που μπορούν να λάβουν οι χρήστες πορτοφολιού για τον μετριασμό των εν λόγω δυνητικών υπολειπόμενων επιπτώσεων, κατά περίπτωση.

Άρθρο 8

Απόσυρση πορτοφολιών

1. Σε περίπτωση που μια παραβίαση της ασφάλειας ή έκθεση σε κίνδυνο που οδήγησε στην αναστολή της παροχής και της χρήσης μιας υλοποίησης πορτοφολιού δεν έχει αντιμετωπιστεί εντός τριών μηνών από την ημερομηνία αναστολής της παροχής και της χρήσης της εν λόγω υλοποίησης πορτοφολιού, το κράτος μέλος που παρέχει την εν λόγω υλοποίηση πορτοφολιού μεριμνά για την απόσυρση της επηρεαζόμενης υλοποίησης πορτοφολιού και για την ανάκληση της ισχύος της, χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, εντός 72 ωρών από τη λήξη της περιόδου των τριών μηνών.

2. Σε περίπτωση που κράτος μέλος αποσύρει υλοποίηση πορτοφολιού, διασφαλίζει ότι:

α) ανακαλούνται οι βεβαιώσεις μονάδας πορτοφολιού της μονάδας πορτοφολιού της επηρεαζόμενης υλοποίησης πορτοφολιού·

β) δεν είναι δυνατή η επαναφορά των βεβαιώσεων μονάδας πορτοφολιού σε κατάσταση ισχύος·

γ) δεν είναι δυνατή η έκδοση νέας βεβαίωσης μονάδας πορτοφολιού σε υφιστάμενες μονάδες πορτοφολιού που παρέχονται στο πλαίσιο της επηρεαζόμενης υλοποίησης πορτοφολιού·

δ) δεν είναι δυνατή η παροχή νέας μονάδας πορτοφολιού στο πλαίσιο της επηρεαζόμενης υλοποίησης πορτοφολιού.

3. Τα μέτρα που προβλέπονται στις παραγράφους 1 και 2 δεν εμποδίζουν τους θιγόμενους χρήστες πορτοφολιού να ασκούν το δικαίωμά τους όσον αφορά τη φορητότητα των δεδομένων που ορίζεται στο άρθρο 5α παράγραφος 4 στοιχείο ζ) του κανονισμού (ΕΕ) αριθ. 910/2014. Αυτό ισχύει υπό την προϋπόθεση ότι το δικαίωμα αυτό μπορεί να ασκείται από χρήστες πορτοφολιού χωρίς να υπονομεύεται η ασφάλεια των κρίσιμων περιουσιακών στοιχείων των επηρεαζόμενων μονάδων πορτοφολιού, λαμβανομένων ιδίως υπόψη των λόγων απόσυρσης και της ανάγκης διασφάλισης της αποτελεσματικής προστασίας των εν λόγω περιουσιακών στοιχείων από καταχρήσεις.

Άρθρο 9

Πληροφορίες σχετικά με την απόσυρση

1. Παρέχονται πληροφορίες με σαφή, ολοκληρωμένο και εύκολα προσβάσιμο τρόπο σχετικά με την απόσυρση υλοποίησης πορτοφολιού, χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 24 ωρών από την απόσυρση της υλοποίησης πορτοφολιού:

α) στα ενιαία σημεία επαφής που ορίζονται σύμφωνα με το άρθρο 46γ παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014·

β) στην Επιτροπή·

γ) στους θιγόμενους χρήστες πορτοφολιού·

δ) στα βασιζόμενα σε πορτοφόλι μέρη που έχουν καταχωριστεί σύμφωνα με το άρθρο 5β του κανονισμού (ΕΕ) αριθ. 910/2014.

2. Οι πληροφορίες που παρέχονται σύμφωνα με την παράγραφο 1 περιλαμβάνουν τουλάχιστον τα ακόλουθα:

α) το όνομα / την επωνυμία του παρόχου της υλοποίησης πορτοφολιού που αποσύρθηκε·

β) την ονομασία και το αναγνωριστικό αναφοράς της εν λόγω υλοποίησης πορτοφολιού, όπως αναφέρεται στον κατάλογο πιστοποιημένων πορτοφολιών που καταρτίζεται σύμφωνα με το άρθρο 5δ του κανονισμού (ΕΕ) αριθ. 910/2014 και, κατά περίπτωση, τις σχετικές εκδόσεις·

γ) την ημερομηνία και την ώρα εντοπισμού της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο που οδήγησε στην απόσυρση της επηρεαζόμενης υλοποίησης πορτοφολιού λόγω της σοβαρότητάς της ή επειδή δεν αντιμετωπίστηκε εντός τριών μηνών·

δ) εάν είναι γνωστή, την ημερομηνία και την ώρα κατά την οποία συντελέστηκε η παραβίαση της ασφάλειας ή η έκθεση σε κίνδυνο, με βάση τα αρχεία καταγραφής του δικτύου ή του συστήματος ή άλλες πηγές δεδομένων·

ε) την ημερομηνία και την ώρα απόσυρσης της υλοποίησης πορτοφολιού και της πραγματικής ανάκλησης των βεβαιώσεων μονάδας πορτοφολιού των μονάδων πορτοφολιού που παρέχονται στο πλαίσιο της υλοποίησης πορτοφολιού·

στ) αν η απόσυρση είναι αποτέλεσμα της σοβαρότητας της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο ή συνέπεια της μη αντιμετώπισης της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο·

ζ) τα στοιχεία επικοινωνίας, συμπεριλαμβανομένων τουλάχιστον διεύθυνσης ηλεκτρονικού ταχυδρομείου και αριθμού τηλεφώνου του κοινοποιούντος κράτους μέλους και, εάν διαφέρει, του παρόχου πορτοφολιού που αναφέρεται στο στοιχείο α)·

η) περιγραφή της παραβίασης της ασφάλειας ή της έκθεσης σε κίνδυνο·

θ) περιγραφή των δεδομένων που έχουν εκτεθεί σε κίνδυνο, συμπεριλαμβανομένων, κατά περίπτωση, των κατηγοριών δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 9 παράγραφος 1 και στο άρθρο 10 του κανονισμού (ΕΕ) 2016/679·

ι) όπου είναι δυνατόν, εκτίμηση του κατά προσέγγιση αριθμού των θιγόμενων χρηστών πορτοφολιού και άλλων φυσικών προσώπων που επηρεάζονται·

ια) περιγραφή των δυνητικών επιπτώσεων στα βασιζόμενα σε πορτοφόλι μέρη ή στους χρήστες πορτοφολιού και, στη δεύτερη περίπτωση, τυχόν ενδείξεις μέτρων που μπορούν να λάβουν οι χρήστες πορτοφολιού για τον μετριασμό των εν λόγω δυνητικών επιπτώσεων, κατά περίπτωση·

ιβ) περιγραφή των μέτρων που έχουν ληφθεί ή πρόκειται να ληφθούν για τη μετάβαση των θιγόμενων χρηστών πορτοφολιού σε εναλλακτικές υλοποιήσεις πορτοφολιού ή, κατά περίπτωση και όπου αυτό κρίνεται σκόπιμο, σε εναλλακτικές υπηρεσίες.

Άρθρο 10

Συστήματα πληροφοριών

Τα κράτη μέλη αποστέλλουν τις πληροφορίες που προβλέπονται στα άρθρα 3, 5, 7 και 9 στην Επιτροπή και στα ενιαία σημεία επαφής των κρατών μελών που ορίζονται σύμφωνα με το άρθρο 46γ παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014, μέσω του CIRAS, το οποίο διαχειρίζεται ο ENISA, ή μέσω ισοδύναμου συστήματος που έχει συμφωνηθεί από τα κράτη μέλη και την Επιτροπή.

Άρθρο 11

Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος, εκτός από το άρθρο 10, το οποίο εφαρμόζεται από την 7η Μαΐου 2026.

Βρυξέλλες, 6 Μαΐου 2025.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ

Κριτήρια για την αξιολόγηση παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο

1. Η αξιολόγηση περιπτώσεων παραβίασης της ασφάλειας ή έκθεσης σε κίνδυνο που διενεργούν τα κράτη μέλη βασίζεται στα ακόλουθα κριτήρια:

α) η παραβίαση της ασφάλειας ή η έκθεση σε κίνδυνο έχει προκαλέσει ή μπορεί να προκαλέσει τον θάνατο φυσικού προσώπου ή σημαντική βλάβη στην υγεία φυσικού προσώπου·

β) υπήρξε, ή μπορεί να υπάρξει, επιτυχής, ύποπτα κακόβουλη ή μη εξουσιοδοτημένη πρόσβαση στα συστήματα δικτύου και πληροφοριών παρόχου πορτοφολιού, παρόχου μηχανισμών επικύρωσης που αναφέρονται στο άρθρο 5α παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014 ή παρόχου του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχεται υλοποίηση πορτοφολιού (στο εξής: οικείες οντότητες) κατά τρόπο ώστε να είναι ικανή να προκαλέσει σοβαρή λειτουργική διατάραξη, και τα εν λόγω συστήματα αποτελούν κρίσιμα συστατικά στοιχεία της επηρεαζόμενης υλοποίησης πορτοφολιού, των επηρεαζόμενων μηχανισμών επικύρωσης που αναφέρονται στο άρθρο 5α παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014, ή του επηρεαζόμενου συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχεται υλοποίηση πορτοφολιού·

γ) υλοποίηση πορτοφολιού, μηχανισμός επικύρωσης που αναφέρεται στο άρθρο 5α παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014 ή σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχεται υλοποίηση πορτοφολιού, ή μέρος αυτών:

— είναι πλήρως μη διαθέσιμο ή προβλέπεται να είναι πλήρως μη διαθέσιμο στους χρήστες πορτοφολιού ή στα βασιζόμενα σε πορτοφόλι μέρη για διάρκεια μεγαλύτερη των 12 συνεχόμενων ωρών·

— είναι μη διαθέσιμο στους χρήστες ή στα βασιζόμενα σε πορτοφόλι μέρη για διάρκεια μεγαλύτερη των 16 ωρών, η οποία υπολογίζεται ανά ημερολογιακή εβδομάδα;

δ) υπάρχουν υπόνοιες ότι πάνω από το 1 % των χρηστών πορτοφολιού ή των βασιζόμενων σε πορτοφόλι μερών επηρεάζεται ή προβλέπεται να επηρεαστεί από την περιορισμένη διαθεσιμότητα της υλοποίησης πορτοφολιού ή των υπηρεσιών που παρέχονται από τις οικείες οντότητες όσον αφορά την υλοποίηση πορτοφολιού·

ε) υπάρχει πιθανότητα να διακυβεύεται ή έχει διακυβευθεί η φυσική πρόσβαση, η οποία περιορίζεται σε αξιόπιστο προσωπικό των οικείων οντοτήτων, ή η προστασία της εν λόγω φυσικής πρόσβασης, σε μία ή περισσότερες από τις τοποθεσίες των συστημάτων δικτύου και πληροφοριών που υποστηρίζουν την υλοποίηση πορτοφολιού, την παροχή των μηχανισμών επικύρωσης που αναφέρονται στο άρθρο 5α παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014 και συνδέονται με υλοποίηση πορτοφολιού, ή το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχεται υλοποίηση πορτοφολιού·

στ) διακυβεύεται, ή υπάρχει πιθανότητα να διακυβεύεται, η ιδιωτική ζωή, η ακεραιότητα, η εμπιστευτικότητα ή η γνησιότητα των δεδομένων που αποθηκεύονται, διαβιβάζονται ή υποβάλλονται σε επεξεργασία στο πλαίσιο της υλοποίησης πορτοφολιού, με έναν ή περισσότερους από τους ακόλουθους τρόπους:

— έχει αντίκτυπο σε περισσότερο από το 1 % των χρηστών πορτοφολιού της επηρεαζόμενης υλοποίησης πορτοφολιού ή σε περισσότερους από 100 000 από τους εν λόγω χρήστες πορτοφολιού, όποιος από τους δύο αριθμούς είναι μικρότερος·

— είναι αποτέλεσμα επιτυχούς, ύποπτα κακόβουλης δραστηριότητας·

— οφείλεται ή είναι πιθανό να οφείλεται σε ένα ή περισσότερα γνωστά τρωτά σημεία, συμπεριλαμβανομένων εκείνων των οποίων ο χειρισμός διέπεται από τις διατάξεις του εκτελεστικού κανονισμού (ΕΕ) 2024/2981 της Επιτροπής ([1])·

— είναι πιθανό να έχει αντίκτυπο σε δεδομένα προσωπικού χαρακτήρα κατά τρόπο που ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των ενδιαφερόμενων φυσικών προσώπων και, ιδίως, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 9 παράγραφος 1 και στο άρθρο 10 του κανονισμού (ΕΕ) 2016/679·

([1]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2981 της Επιτροπής, της 28ης Νοεμβρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την πιστοποίηση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας (ΕΕ L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— είναι πιθανό να έχει αντίκτυπο στις προσωπικές ηλεκτρονικές επικοινωνίες·

— είναι πιθανό να συνεπάγεται υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων·

— είναι πιθανό να έχει αντίκτυπο σε ευάλωτα φυσικά πρόσωπα;

ζ) έχει ακυρωθεί ή προβλέπεται να ακυρωθεί η πιστοποίηση της υλοποίησης πορτοφολιού·

η) η παραβίαση ή η έκθεση σε κίνδυνο έχει προκαλέσει ή μπορεί να προκαλέσει άμεση οικονομική ζημία για την οικεία οντότητα και η εν λόγω ζημία υπερβαίνει τα 500 000 EUR ή, κατά περίπτωση, το 5 % του συνολικού ετήσιου κύκλου εργασιών της οικείας οντότητας κατά το προηγούμενο οικονομικό έτος, όποιο από τα δύο ποσά είναι χαμηλότερο.

2. Τα κράτη μέλη δεν λαμβάνουν υπόψη τις αναμενόμενες συνέπειες εργασίας συντήρησης που εκτελείται από τις οικείες οντότητες ή για λογαριασμό τους, υπό την προϋπόθεση ότι η εν λόγω εργασία συντήρησης:

α) έχει κοινοποιηθεί εκ των προτέρων σε δυνητικά θιγόμενους χρήστες πορτοφολιού, σε βασιζόμενα σε πορτοφόλι μέρη και στους σχετικούς αρμόδιους εποπτικούς φορείς·

β) δεν πληροί κανένα από τα κριτήρια που καθορίζονται στο σημείο 1) του παρόντος παραρτήματος.

3. Όσον αφορά το στοιχείο γ) του σημείου 1), η διάρκεια ενός περιστατικού που επηρεάζει τη διαθεσιμότητα μετράται από τη χρονική στιγμή κατά την οποία διακόπτεται η ορθή παροχή της επηρεαζόμενης υπηρεσίας έως τη χρονική στιγμή κατά την οποία η υπηρεσία αποκαθίσταται και τίθεται εκ νέου σε λειτουργία. Σε περίπτωση που μια οικεία οντότητα αδυνατεί να προσδιορίσει τη χρονική στιγμή έναρξης της διατάραξης, η διάρκεια του περιστατικού μετράται από τη χρονική στιγμή κατά την οποία εντοπίστηκε το περιστατικό ή από τη χρονική στιγμή κατά την οποία το περιστατικό καταγράφηκε στα αρχεία καταγραφής του δικτύου ή του συστήματος ή σε άλλες πηγές δεδομένων, ανάλογα με το ποια ημερομηνία είναι προγενέστερη. Η πλήρης μη διαθεσιμότητα μιας υπηρεσίας μετράται από τη χρονική στιγμή που η υπηρεσία είναι πλήρως μη διαθέσιμη στους χρήστες έως τη χρονική στιγμή κατά την οποία οι τακτικές δραστηριότητες ή λειτουργίες έχουν αποκατασταθεί στο επίπεδο της υπηρεσίας που παρεχόταν πριν από το περιστατικό. Σε περίπτωση που μια οικεία οντότητα αδυνατεί να προσδιορίσει πότε άρχισε η πλήρης μη διαθεσιμότητα μιας υπηρεσίας, η μη διαθεσιμότητα μετράται από τη χρονική στιγμή κατά την οποία εντοπίστηκε από την εν λόγω οντότητα.

4. Όσον αφορά το στοιχείο δ) του σημείου 1), περιορισμένη διαθεσιμότητα μιας υπηρεσίας θεωρείται ότι υφίσταται ιδίως όταν μια υπηρεσία είναι σημαντικά βραδύτερη από τον μέσο χρόνο απόκρισης ή όταν δεν είναι διαθέσιμες όλες οι λειτουργίες μιας υπηρεσίας. Όπου είναι δυνατόν, χρησιμοποιούνται αντικειμενικά κριτήρια με βάση τον μέσο χρόνο απόκρισης των υπηρεσιών για την αξιολόγηση των καθυστερήσεων στον χρόνο απόκρισης.

5. Για τον προσδιορισμό των άμεσων οικονομικών ζημιών που προκύπτουν από παραβίαση ή έκθεση σε κίνδυνο που αναφέρεται στο σημείο 1) στοιχείο η), οι οικείες οντότητες θα πρέπει να λαμβάνουν υπόψη όλες τις οικονομικές ζημίες που υπέστησαν ως αποτέλεσμα του περιστατικού, όπως οι δαπάνες αντικατάστασης ή μετεγκατάστασης λογισμικού, υλισμικού ή υποδομής, οι δαπάνες προσωπικού, συμπεριλαμβανομένων των δαπανών που συνδέονται με την αντικατάσταση ή τη μετεγκατάσταση του προσωπικού, την πρόσληψη επιπλέον προσωπικού, τις αμοιβές υπερωριών και την ανάκτηση απολεσθεισών ή υποβαθμισμένων δεξιοτήτων, τα τέλη λόγω μη συμμόρφωσης με τις συμβατικές υποχρεώσεις, τα έξοδα επανόρθωσης και αποζημίωσης των πελατών, οι απώλειες λόγω διαφυγόντων εσόδων, οι δαπάνες που συνδέονται με την εσωτερική και εξωτερική επικοινωνία και οι δαπάνες παροχής συμβουλών, συμπεριλαμβανομένων των δαπανών που συνδέονται με νομικές συμβουλές, εγκληματολογικές υπηρεσίες και υπηρεσίες αποκατάστασης. Οι δαπάνες που είναι αναγκαίες για την καθημερινή λειτουργία της επιχείρησης, όπως οι δαπάνες για τη γενική συντήρηση της υποδομής, του εξοπλισμού, του υλισμικού και του λογισμικού, για τις βελτιώσεις και τις πρωτοβουλίες εκτίμησης κινδύνου, καθώς και για ασφάλιστρα, δεν θεωρούνται οικονομικές ζημίες που προκύπτουν από περιστατικό. Οι οικείες οντότητες υπολογίζουν τα ποσά των οικονομικών ζημιών με βάση τα διαθέσιμα δεδομένα και, όταν τα πραγματικά ποσά των οικονομικών ζημιών δεν μπορούν να προσδιοριστούν, οι εν λόγω οντότητες προβαίνουν σε εκτίμηση των εν λόγω ποσών.