

ΓΑΛΛΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Ο Πρωθυπουργός

Σχέδιο διατάγματος για την προστασία στρατηγικών και ευαίσθητων δεδομένων στην αγορά των υπηρεσιών υπολογιστικού νέφους

Αριθ. αναφοράς:

Ενδιαφερόμενο κοινό: Κρατικές διοικήσεις και φορείς εκμετάλλευσης, ομάδες δημόσιου συμφέροντος

Θέμα: ...

Έναρξη ισχύος: το διάταγμα τίθεται σε ισχύ την επομένη της δημοσίευσής του.

Σημείωση:

Αναφορές: Το διάταγμα εφαρμόζει το άρθρο 31 του νόμου αριθ. 2024-449 της 21ης Μαΐου 2024 για τη διασφάλιση και τη ρύθμιση του ψηφιακού χώρου. Μπορεί να ζητηθεί η γνώμη της στην ιστοσελίδα *Légifrance* (<http://www.legifrance.gouv.fr>).

Η πρωθυπουργός,

Σχετικά με την έκθεση της XX,

έχοντας υπόψη τον κανονισμό (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,

έχοντας υπόψη την οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών,

έχοντας υπόψη τον Αμυντικό Κώδικα, ιδίως το άρθρο D. 3126-2,

έχοντας υπόψη το διάταγμα αριθ. 2005-1516, της 8ης Δεκεμβρίου 2005, σχετικά με τις ηλεκτρονικές ανταλλαγές μεταξύ χρηστών και διοικητικών αρχών και μεταξύ διοικητικών αρχών, και ιδίως το άρθρο 9,

έχοντας υπόψη τον νόμο αριθ. 2016-1321 της 7ης Οκτωβρίου 2016 για τη Ψηφιακή Δημοκρατία, και ιδίως το άρθρο 16,

έχοντας υπόψη τον νόμο αριθ. 2024-449 της 21ης Μαΐου 2024 για τη διασφάλιση και τη ρύθμιση του ψηφιακού χώρου, και ιδίως το άρθρο 31,

έχοντας υπόψη το διάταγμα αριθ. 2014-445 της 30ής Απριλίου 2014 σχετικά με τα καθήκοντα και την οργάνωση της Γενικής Διεύθυνσης Εσωτερικής Ασφάλειας,

έχοντας υπόψη το διάταγμα αριθ. 2015-350 της 27ης Μαρτίου 2015, όπως τροποποιήθηκε, σχετικά με τον χαρακτηρισμό των προϊόντων ασφάλειας και των παρόχων υπηρεσιών εμπιστοσύνης για τις ανάγκες ασφάλειας των συστημάτων πληροφοριών,

έχοντας υπόψη την κοινοποίηση αριθ. XX που στάλθηκε στην Ευρωπαϊκή Επιτροπή στις XXX,

Κατόπιν διαβούλευσης με το Συμβούλιο της Επικρατείας (Τμήμα Διοίκησης),

Αποφασίζεται:

Άρθρο 1

Ο κατάλογος των ομάδων δημόσιου συμφέροντος που αναφέρεται στο άρθρο 31 παράγραφος I του προαναφερθέντος νόμου της 21ης Μαΐου 2024 περιλαμβάνει τις εξής:

- Την ομάδα δημόσιου συμφέροντος με την ονομασία «Οργανισμός Ψηφιακής Υγείας (ANS)»·
- Την ομάδα δημόσιου συμφέροντος με την ονομασία «Εθνική Υπηρεσία Έρευνας για το AIDS (ANRS)»·
- Την ομάδα δημόσιου συμφέροντος με την ονομασία «Οργανισμός για την Προώθηση της Εκπαιδευτικής και Επιστημονικής Κατάρτισης και Ανταλλαγής»·
- Την ομάδα δημόσιου συμφέροντος «Κέντρο Ασφαλούς Πρόσβασης σε Δεδομένα (CASD)»·
- Την ομάδα δημόσιου συμφέροντος «Κέντρο Πόρων για την Πρόληψη της Ριζοσπαστικοποίησης»·
- Την ομάδα δημόσιου συμφέροντος «Εθνική Κτηνιατρική Σχολή»·
- Την ομάδα δημόσιου συμφέροντος «Ομάδα Δημόσιου Συμφέροντος για τις Κλειστές Πηγές Υψηλής Ραδιενέργειας (GIP SOURCES HA)»·
- Την ομάδα δημόσιου συμφέροντος «Εθνικό Σύστημα Καταχώρισης της Ζήτησης Κοινωνικής Στέγασης (GIP SNE)»·
- Την ομάδα δημόσιου συμφέροντος «Εκσυγχρονισμός των Κοινωνικών Δηλώσεων (GIP-MDS)»·
- Την ομάδα δημόσιου συμφέροντος «Παρατηρητήριο Επιστήμης και Τεχνολογίας»·

Άρθρο 2

I — Για την εφαρμογή του άρθρου 31 του προαναφερθέντος νόμου της 21ης Μαΐου 2024, ο ιδιώτης πάροχος υπηρεσιών οφείλει να εφαρμόζει τα ακόλουθα κριτήρια ασφάλειας και προστασίας δεδομένων:

- τεκμηριωμένη πολιτική ασφάλειας πληροφοριών και διαχείρισης κινδύνων που ενσωματώνει την αλυσίδα υπεργολαβίας·
- ασφαλές σύστημα διαχείρισης ανθρώπινων πόρων για το προσωπικό που συμμετέχει στην παροχή της υπηρεσίας·
- εργαλεία και διαδικασίες για την ασφαλή διαχείριση του εξοπλισμού που υλοποιεί την υπηρεσία και τα συστήματα πληροφοριών·
- μέτρα φυσικής, περιβαλλοντικής και λογικής ασφάλειας, όπως η χρήση μηχανισμών κρυπτογράφησης, ο έλεγχος πρόσβασης και η διαχείριση ταυτότητας χρήστη·
- διαδικασίες διαχείρισης συμβάντων ασφάλειας πληροφοριών και μέτρα επιχειρησιακής συνέχειας·
- μέτρα για την τήρηση των ισχυουσών στη Γαλλία νομικών διατάξεων και των μέτρων προστασίας των δεδομένων, ιδίως των συμβατικών, για επεξεργασμένα ή αποθηκευμένα δεδομένα έναντι οποιασδήποτε πρόσβασης δημόσιων αρχών τρίτων χωρών που δεν επιτρέπεται από το δίκαιο της Ευρωπαϊκής Ένωσης ή το δίκαιο κράτους μέλους, συμπεριλαμβανομένων ιδίως των όρων που διέπουν την κατοχή κεφαλαίου και δικαιωμάτων ψήφου στην εταιρεία του παρόχου υπηρεσιών και την εγκατάσταση του παρόχου υπηρεσιών και τυχόν υπεργολάβων.

Ένα πλαίσιο που αναπτύχθηκε από τον γαλλικό Οργανισμό για την Ασφάλεια στον Κυβερνοχώρο υπό τους όρους του προαναφερθέντος διατάγματος της 27ης Μαρτίου 2015, καθορίζει τις απαιτήσεις σχετικά με τα εν λόγω κριτήρια. Η αναγκαία διαβούλευση για τη δημιουργία και ανάπτυξη του παρόντος πλαισίου αναφοράς του κρατικού πληροφοριακού συστήματος πραγματοποιείται σε συνεργασία με τη Διυπουργική Διεύθυνση Ψηφιακής Τεχνολογίας.

II — Προκειμένου να πληρούνται οι απαιτήσεις προστασίας και ασφάλειας των δεδομένων που ορίζονται στο άρθρο 31 παράγραφος I του προαναφερθέντος νόμου της 21ης Μαΐου 2024, οι ενδιαφερόμενες διοικήσεις προσφεύγουν σε υπηρεσίες υπολογιστικού νέφους παρεχόμενες από ειδικευμένο ιδιωτικό φορέα παροχής υπηρεσιών, οι οποίες χορηγούνται υπό τους όρους του κεφαλαίου III του προαναφερθέντος διατάγματος της 27ης Μαρτίου 2015 και πληρούν τα κριτήρια που αναφέρονται στην παράγραφο I του παρόντος άρθρου, ή ευρωπαϊκής πιστοποίησης τουλάχιστον ισοδύναμου επιπέδου.

III — Επιχειρησιακά συστήματα πληροφοριών και συστήματα επικοινωνίας, συστήματα επιστημονικών και τεχνικών πληροφοριών, και τα συστήματα πληροφοριών που περιλαμβάνουν, απαιτούν ή περιέχουν διαβαθμισμένα μέσα ή πληροφορίες που περιλαμβάνουν το αμυντικό σύστημα πληροφοριών και επικοινωνίας, καθώς και τα συστήματα πληροφοριών και επικοινωνιών που λειτουργούν από τις υπηρεσίες που αναφέρονται στο άρθρο D. 3126-2 του Αμυντικού Κώδικα και στο άρθρο 1 του ανωτέρω διατάγματος της 30ής Απριλίου 2014, εξαιρούνται από το πεδίο εφαρμογής του παρόντος άρθρου.

Άρθρο 3

I — Όταν μια διοίκηση έχει ήδη δρομολογήσει, κατά την ημερομηνία έναρξης ισχύος του άρθρου 31 του προαναφερθέντος νόμου της 21ης Μαΐου 2024, έργο που πληροί τις προϋποθέσεις του ως άνω άρθρου και χρησιμοποιεί υπηρεσία υπολογιστικού νέφους που παρέχεται από ιδιωτικό πάροχο υπηρεσιών που δεν εφαρμόζει τα κριτήρια ασφάλειας και προστασίας των δεδομένων που ορίζονται στο άρθρο 2 του παρόντος διατάγματος, μπορεί να ζητήσει, σύμφωνα με τις διαδικασίες που καθορίζονται με απόφαση του πρωθυπουργού, παρέκκλιση από τις υποχρεώσεις που ορίζονται στο ίδιο άρθρο.

Η παρέκκλιση αυτή δεν μπορεί να υπερβαίνει τους 18 μήνες όταν υπάρχει αποδεκτή προσφορά υπηρεσιών υπολογιστικού νέφους, κατά την έννοια της παραγράφου II του παρόντος άρθρου, που είναι διαθέσιμη στη Γαλλία. Όταν δεν υπάρχει αποδεκτή προσφορά υπολογιστικού νέφους στη Γαλλία κατά την ημερομηνία υποβολής του αιτήματος παρέκκλισης, η παρέκκλιση δεν μπορεί να υπερβαίνει το ένα έτος πριν από την ενδεχόμενη υποβολή νέας αίτησης.

Η παρέκκλιση αυτή χορηγείται με αιτιολογημένη απόφαση του αρμόδιου για το έργο υπουργού και επικυρώνεται από τον πρωθυπουργό.

Δημοσιοποιείται υπό τους όρους που καθορίζονται στο βιβλίο III του Κώδικα Σχέσεων μεταξύ Διοικουμένων και Διοίκησης.

II — Η εκτίμηση του αποδεκτού χαρακτήρα, κατά την έννοια του άρθρου 31 παράγραφος III του προαναφερθέντος νόμου της 21ης Μαΐου 2024, μιας προσφοράς υπηρεσιών υπολογιστικού νέφους βασίζεται στα ακόλουθα κριτήρια:

- τη λειτουργική ανάγκη που μπορεί να καλύψει η προσφορά, λαμβανομένων υπόψη των καθηκόντων της οικείας διοίκησης·
- τους χρηματοδοτικούς όρους·
- τους επιχειρησιακούς και τεχνικούς όρους ασφάλειας και προστασίας των δεδομένων που υποβάλλονται σε επεξεργασία από τον πάροχο της προσφοράς σύμφωνα με τις απαιτήσεις του άρθρου 2 του παρόντος διατάγματος·
- τους όρους λήξης της σύμβασης και τις εγγυήσεις αναστρεψιμότητας·
- οι όροι ελέγχου, βιωσιμότητας και ανεξαρτησίας κατά την έννοια του άρθρου 16 του προαναφερθέντος νόμου της 7ης Οκτωβρίου 2016.

Εκδόθηκε στις

Από τον Πρωθυπουργό: