Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/2050

9.10.2025

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/2050 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 1ης Ιουλίου 2025

για τη συμπλήρωση του κανονισμού (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με τον καθορισμό των τεχνικών προϋποθέσεων και διαδικασιών βάσει των οποίων οι πάροχοι πολύ μεγάλων επιγραμμικών πλατφορμών και πολύ μεγάλων επιγραμμικών μηχανών αναζήτησης ανταλλάσσουν δεδομένα με διαπιστευμένους ερευνητές

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Οκτωβρίου 2022, σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της οδηγίας 2000/31/ΕΚ ([1]), και ιδίως το άρθρο 40 παράγραφος 13,

Εκτιμώντας τα ακόλουθα:

(1) Το άρθρο 40 του κανονισμού (ΕΕ) 2022/2065 θεσπίζει κανόνες σχετικά με την πρόσβαση σε δεδομένα που πρέπει να χορηγούν οι πάροχοι πολύ μεγάλων επιγραμμικών πλατφορμών και πολύ μεγάλων επιγραμμικών μηχανών αναζήτησης. Ειδικότερα, δίνει στους ερευνητές που έχουν ολοκληρώσει μια διαδικασία τη δυνατότητα να αποδείξουν ότι πληρούν τις προϋποθέσεις που ορίζονται στην παράγραφο 8 του εν λόγω άρθρου (στο εξής: διαπιστευμένοι ερευνητές) ώστε να τους παρασχεθεί η εν λόγω πρόσβαση.

(2) Σύμφωνα με το άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065, πρέπει να παρέχεται στους διαπιστευμένους ερευνητές πρόσβαση σε δεδομένα που θα τους βοηθούν να μελετούν συστημικούς κινδύνους στην Ένωση και να αξιολογούν την αποτελεσματικότητα των μέτρων για τον περιορισμό των εν λόγω κινδύνων. Τα ευρήματά τους μπορούν να αποτελέσουν πολύτιμη συμβολή για την εφαρμογή του κανονισμού (ΕΕ) 2022/2065 και να ενισχύσουν τη λογοδοσία των παρόχων πολύ μεγάλων επιγραμμικών πλατφορμών και πολύ μεγάλων επιγραμμικών μηχανών αναζήτησης. Σκοπός του παρόντος κανονισμού είναι να καθορίσει τις τεχνικές προϋποθέσεις και τις διαδικασίες που απαιτούνται για να καταστεί δυνατή η εν λόγω πρόσβαση, με ασφαλή και αποτελεσματικό τρόπο που θα είναι συνεπής για όλους τους συντονιστές ψηφιακών υπηρεσιών και με τρόπο που θα διασφαλίζει την ίση μεταχείριση των ερευνητών και των παρόχων δεδομένων.

(3) Για να διασφαλιστεί ότι η διαδικασία πρόσβασης σε δεδομένα είναι συνεπής για όλους τους συντονιστές ψηφιακών υπηρεσιών και για να καταστεί η εν λόγω διαδικασία σαφής και διαφανής για όλους, είναι απαραίτητο να δημιουργηθεί ειδική ψηφιακή υποδομή (στο εξής: πύλη πρόσβασης σε δεδομένα βάσει της DSA). Η πύλη πρόσβασης σε δεδομένα βάσει της DSA θα πρέπει να δίνει στους ερευνητές, στους παρόχους δεδομένων και στους συντονιστές ψηφιακών υπηρεσιών τη δυνατότητα να συμμετέχουν στη διαδικασία πρόσβασης σε δεδομένα, να έχουν πρόσβαση σε σχετικές πληροφορίες, όπως στα στοιχεία των ειδικών σημείων επαφής, και να διαδίδουν τις εν λόγω πληροφορίες, καθώς και να επικοινωνούν μεταξύ τους. Η πύλη πρόσβασης σε δεδομένα βάσει της DSA δεν θα πρέπει να θεωρείται ως μία από τις μεθόδους πρόσβασης προς χρήση για την παροχή πρόσβασης στα δεδομένα κατόπιν αιτιολογημένου αιτήματος.

(4) Οι πάροχοι δεδομένων και οι ερευνητές που επιθυμούν να συμμετάσχουν στη διαδικασία πρόσβασης σε δεδομένα θα πρέπει να δημιουργήσουν λογαριασμό στην πύλη πρόσβασης σε δεδομένα βάσει της DSA για τον σκοπό αυτόν. Για να διασφαλιστεί ότι οι συντονιστές ψηφιακών υπηρεσιών μπορούν να έχουν πρόσβαση σε πληροφορίες που υποβάλλονται μέσω της πύλης πρόσβασης σε δεδομένα βάσει της DSA χωρίς να χρειάζεται να δημιουργήσουν χωριστό λογαριασμό στην πύλη, η πύλη πρόσβασης σε δεδομένα βάσει της DSA θα πρέπει να είναι διαλειτουργική με το σύστημα ανταλλαγής πληροφοριών AGORA που θεσπίστηκε με τον εκτελεστικό κανονισμό (ΕΕ) 2024/607 της Επιτροπής ([2]).

(5) Για να διασφαλιστεί η διαφάνεια της διαδικασίας πρόσβασης σε δεδομένα για όλους τους εμπλεκομένους και για να παρακολουθούνται η αποτελεσματικότητα και η αποδοτικότητα της διαδικασίας πρόσβασης σε δεδομένα και η συμμόρφωση με το άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065 και τον παρόντα κανονισμό, η πύλη πρόσβασης σε δεδομένα βάσει της DSA θα πρέπει να παράγει αυτόματες ειδοποιήσεις σε σχέση με διάφορα στάδια και διάφορες επικαιροποιήσεις της διαδικασίας.

([1]) ΕΕ L 277 της 27.10.2022, σ. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

([2]) Εκτελεστικός κανονισμός (ΕΕ) 2024/607 της Επιτροπής, της 15ης Φεβρουαρίου 2024, σχετικά με τις πρακτικές και επιχειρησιακές ρυθμίσεις για τη λειτουργία του συστήματος ανταλλαγής πληροφοριών σύμφωνα με τον κανονισμό (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (πράξη για τις ψηφιακές υπηρεσίες) (ΕΕ L, 2024/607, 16.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/607/oj).

(6) Προκειμένου να παρέχονται στους ερευνητές συνεπείς πληροφορίες σχετικά με τη διαδικασία πρόσβασης σε δεδομένα, οι συντονιστές ψηφιακών υπηρεσιών θα πρέπει να καθιστούν διαθέσιμες και εύκολα προσβάσιμες στις επιγραμμικές διεπαφές τους πληροφορίες σχετικά με τη διαδικασία πρόσβασης σε δεδομένα, συμπεριλαμβανομένων συνδέσμων προς την πύλη πρόσβασης σε δεδομένα βάσει της DSA. Για να αποφευχθεί η δημιουργία περιττού διοικητικού φόρτου, να αυξηθεί η αποδοτικότητα και να διευκολυνθεί η επικοινωνία μεταξύ όλων των μερών που συμμετέχουν στη διαδικασία πρόσβασης σε δεδομένα, οι συντονιστές ψηφιακών υπηρεσιών παροτρύνονται να διευκολύνουν τη διαχείριση των πληροφοριών που σχετίζονται με τη διαδικασία πρόσβασης σε δεδομένα, μεταξύ άλλων και από γλωσσική άποψη.

(7) Προκειμένου να μπορούν οι ερευνητές να προσδιορίζουν τα σχετικά δεδομένα για τους σκοπούς που ορίζονται στο άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065, οι πάροχοι δεδομένων θα πρέπει να καθιστούν διαθέσιμους καταλόγους δεδομένων βάσει της DSA για τις υπηρεσίες τους. Οι εν λόγω κατάλογοι θα πρέπει να είναι εύκολα ευρέσιμοι και προσβάσιμοι στις επιγραμμικές διεπαφές των παρόχων δεδομένων και θα πρέπει να περιγράφουν τους διαθέσιμους πόρους δεδομένων, τη δομή των δεδομένων τους και τα μεταδεδομένα τους, η πρόσβαση στα οποία μπορεί να ζητηθεί σύμφωνα με το άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065. Κατά τη διάθεση των καταλόγων δεδομένων βάσει της DSA, οι πάροχοι δεδομένων θα πρέπει να λαμβάνουν υπόψη τους κινδύνους για την εμπιστευτικότητα, την ασφάλεια των δεδομένων ή την προστασία των δεδομένων προσωπικού χαρακτήρα που ενδέχεται να προκύψουν από τη δημοσιοποίηση των εν λόγω πληροφοριών.

(8) Για να συμβάλουν στην ανάπτυξη σχετικών ερευνητικών έργων για τους σκοπούς που ορίζονται στο άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065, οι κατάλογοι δεδομένων βάσει της DSA θα πρέπει να περιλαμβάνουν ιδίως δεδομένα που σχετίζονται με τους συστημικούς κινδύνους στην Ένωση που οι πάροχοι δεδομένων έχουν εντοπίσει στις ετήσιες εκτιμήσεις κινδύνων τους σύμφωνα με το άρθρο 34 του εν λόγω κανονισμού, καθώς και δεδομένα σχετικά με τυχόν μέτρα περιορισμού των κινδύνων που αναφέρονται στο άρθρο 35 του εν λόγω κανονισμού. Για να διασφαλιστεί ότι οι κατάλογοι δεδομένων βάσει της DSA θα είναι συναφείς και επίκαιροι, θα πρέπει να επικαιροποιούνται τακτικά, λαμβανομένων δεόντως υπόψη των νέων συστημικών κινδύνων που εντοπίζονται και της εξέλιξής τους. Για παράδειγμα, θα πρέπει να αντικατοπτρίζουν τους αναδυόμενους κινδύνους που εντοπίζονται κατόπιν ειδικής εκτίμησης κινδύνων σύμφωνα με το άρθρο 34 του κανονισμού (ΕΕ) 2022/2065 ή κατόπιν έκθεσης ελέγχου σύμφωνα με το άρθρο 37 του εν λόγω κανονισμού. Για να ελαχιστοποιηθεί ο διαδικαστικός φόρτος για τους παρόχους δεδομένων, κατά περίπτωση, οι εν λόγω κατάλογοι μπορούν να βασίζονται σε υφιστάμενους πόρους τεκμηρίωσης δεδομένων που χρησιμοποιούνται για άλλους σκοπούς και προς άλλο κοινό, όπως για διαφήμιση, δημιουργία περιεχομένου ή ανάπτυξη εφαρμογών τρίτων. Οι κατάλογοι δεδομένων βάσει της DSA δεν απαιτείται να είναι εξαντλητικοί, και ως εκ τούτου δεν θα πρέπει να δεσμεύουν ή να περιορίζουν τους αιτούντες ερευνητές όσον αφορά τις αιτήσεις που υποβάλλουν για την πρόσβαση σε δεδομένα.

(9) Προκειμένου να διευκολυνθεί ο καθορισμός των μεθόδων πρόσβασης από τον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης και να μειωθεί ο συνολικός φόρτος που συνεπάγεται η διαδικασία πρόσβασης σε δεδομένα για όλους τους εμπλεκομένους, οι πάροχοι δεδομένων θα πρέπει να δημοσιεύουν τις προτεινόμενες μεθόδους πρόσβασης για τα δεδομένα που περιγράφονται στους καταλόγους δεδομένων βάσει της DSA. Οι εν λόγω προτεινόμενες μέθοδοι πρόσβασης θα πρέπει να είναι ανάλογες προς τον ευαίσθητο χαρακτήρα των δεδομένων και να περιλαμβάνουν πληροφορίες σχετικά με τις πιθανές τεχνικές, οργανωτικές και νομικές προϋποθέσεις που θεωρούν κατάλληλες οι πάροχοι δεδομένων ώστε να καθίσταται δυνατή η παροχή των δεδομένων. Οι μέθοδοι πρόσβασης που προτείνουν οι πάροχοι δεδομένων δεν θα πρέπει να δεσμεύουν τους συντονιστές ψηφιακών υπηρεσιών της χώρας εγκατάστασης, οι οποίοι θα πρέπει να εξακολουθούν να είναι αρμόδιοι για τον καθορισμό των κατάλληλων μεθόδων πρόσβασης.

(10) Για να διασφαλιστεί ότι οι αιτήσεις πρόσβασης σε δεδομένα αντιμετωπίζονται ισότιμα, ανεξάρτητα από τον συντονιστή ψηφιακών υπηρεσιών στον οποίο υποβάλλεται η αίτηση πρόσβασης σε δεδομένα ή από τον οποίο προέρχεται το αιτιολογημένο αίτημα, θα πρέπει να καθοριστεί το χρονοδιάγραμμα για τη διατύπωση αιτιολογημένων αιτημάτων, ώστε να διασφαλιστεί η συνοχή μεταξύ όλων των συντονιστών ψηφιακών υπηρεσιών. Εάν η διατύπωση του αιτιολογημένου αιτήματος απαιτεί πρόσθετο χρόνο, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να ενημερώσει τον κύριο ερευνητή, αναφέροντας τους λόγους της καθυστέρησης. Στους λόγους αυτούς μπορεί να περιλαμβάνεται η ανάγκη για πρόσθετες επαληθεύσεις από τον συντονιστή ψηφιακών υπηρεσιών του ερευνητικού οργανισμού ή της χώρας εγκατάστασης, για παράδειγμα όταν οι αιτήσεις πρόσβασης σε δεδομένα συνεπάγονται διεθνείς διαβιβάσεις δεδομένων ή όταν ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης έχει εντοπίσει δυνητικούς κινδύνους για την ασφάλεια της Ένωσης σε περίπτωση κοινοποίησης των δεδομένων. Προκειμένου να ευθυγραμμιστούν επίσης τα στάδια της διαδικασίας πρόσβασης σε δεδομένα που προηγούνται της διατύπωσης αιτιολογημένων αιτημάτων, συμπεριλαμβανομένων της αξιολόγησης των αιτήσεων πρόσβασης σε δεδομένα και της χορήγησης καθεστώτος «διαπιστευμένου ερευνητή», οι συντονιστές ψηφιακών υπηρεσιών παροτρύνονται να αναπτύξουν έναν συνεπή και συντονισμένο τρόπο εργασίας, συμπεριλαμβανομένων κοινών επιχειρησιακών κριτηρίων, στο πλαίσιο του ευρωπαϊκού συμβουλίου ψηφιακών υπηρεσιών.

(11) Προκειμένου να εξορθολογιστούν οι διαδικασίες για τη διατύπωση αιτιολογημένων αιτημάτων, όλοι οι συντονιστές ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να υποχρεούνται να επαληθεύουν ότι ορισμένα κοινά στοιχεία της διαδικασίας πρόσβασης σε δεδομένα καλύπτονταν δεόντως στις αιτήσεις πρόσβασης σε δεδομένα. Για τον σκοπό αυτόν, οι συντονιστές ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να επαληθεύουν ότι όλοι οι αιτούντες ερευνητές που αναφέρονται στην αίτηση πρόσβασης σε δεδομένα έχουν αποδείξει τη σύνδεσή τους με ερευνητικό οργανισμό, για παράδειγμα παρέχοντας αποδεικτικά έγγραφα για τις συμβάσεις εργασίας ή οποιαδήποτε άλλη μορφή νομικής σύνδεσης με τον ερευνητικό οργανισμό. Οι συντονιστές ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει επίσης να επαληθεύουν ότι οι αιτούντες ερευνητές έχουν αποδείξει την ανεξαρτησία τους από εμπορικά συμφέροντα, για παράδειγμα, μέσω σχετικής δήλωσης.

(12) Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να επαληθεύει ότι η χρηματοδότηση του ερευνητικού έργου για το οποίο ζητούνται τα δεδομένα γνωστοποιείται στην αίτηση πρόσβασης σε δεδομένα. Οι πληροφορίες που παρέχουν οι αιτούντες ερευνητές θα πρέπει να περιλαμβάνουν λεπτομέρειες σχετικά με τις συνεισφορές, όπως την οντότητα χρηματοδότησης, το ποσό, τη φύση και τη διάρκεια της συνεισφοράς, διευκρινίζοντας, μεταξύ άλλων, αν η χρηματοδότηση έχει ήδη χορηγηθεί ή αν η αίτηση χρηματοδότησης βρίσκεται ακόμη υπό αξιολόγηση, καθώς και, κατά περίπτωση, σχετικές αναφορές σε έργα που χρηματοδοτούνται από την Ένωση. Κατά περίπτωση, η αίτηση πρόσβασης σε δεδομένα θα πρέπει επίσης να περιλαμβάνει τα αποτελέσματα των αξιολογήσεων που διενεργούνται από την οντότητα ή τις οντότητες που παρέχει/-ουν τη χρηματοδότηση.

(13) Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να επαληθεύει ότι η αίτηση πρόσβασης σε δεδομένα περιγράφει τον τρόπο επιλογής των δεδομένων και του μορφότυπου των δεδομένων, με αναφορά στις απαιτήσεις που αφορούν την αναγκαιότητα για τον σκοπό της προβλεπόμενης έρευνας και την αναλογικότητα προς τον σκοπό αυτόν. Όταν τα ζητούμενα δεδομένα είναι διαθέσιμα και από άλλες πηγές, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να αξιολογεί αν το αίτημα για τα εν λόγω δεδομένα που αναφέρεται στην αίτηση πρόσβασης σε δεδομένα είναι δεόντως αιτιολογημένο, λαμβάνοντας υπόψη τις πληροφορίες που περιέχει η αίτηση πρόσβασης σε δεδομένα. Οι πιθανές αιτιολογήσεις μπορεί να περιλαμβάνουν την κακή ποιότητα των αποδεικτικών στοιχείων ή την αναξιοπιστία των εν λόγω δεδομένων που προέρχονται από άλλες πηγές ή την ακαταλληλότητα του μορφότυπου με τον οποίο τα εν λόγω δεδομένα μπορούν να ανακτηθούν από άλλες πηγές για τους σκοπούς του ερευνητικού έργου, κάτι που θα παρεμπόδιζε την εκτέλεση του ερευνητικού έργου. Τα δεδομένα που μπορούν να ζητηθούν για τη μελέτη ή τον περιορισμό των συστημικών κινδύνων στην Ένωση ενδέχεται να εξελιχθούν στο μέλλον. Τρέχοντα παραδείγματα τέτοιου είδους δεδομένων είναι μεταξύ άλλων τα δεδομένα που σχετίζονται με τους χρήστες των υπηρεσιών, όπως οι πληροφορίες προφίλ, τα δίκτυα σχέσεων, η ατομική έκθεση σε περιεχόμενο και το ιστορικό αλληλεπιδράσεων· τα δεδομένα αλληλεπίδρασης, όπως σχόλια ή άλλου είδους συμμετοχές· τα δεδομένα που σχετίζονται με τις συστάσεις περιεχομένου, συμπεριλαμβανομένων των δεδομένων που χρησιμοποιούνται για την εξατομίκευση των συστάσεων· τα δεδομένα που σχετίζονται με τη στόχευση διαφημίσεων και την κατάρτιση προφίλ, συμπεριλαμβανομένου του κόστους ανά κλικ και άλλων μετρήσεων για τις τιμές διαφήμισης· τα δεδομένα που σχετίζονται με τη δοκιμή νέων χαρακτηριστικών πριν από την ανάπτυξή τους, συμπεριλαμβανομένων των αποτελεσμάτων των δοκιμών Α/Β· τα δεδομένα που σχετίζονται με τον έλεγχο και τη διακυβέρνηση περιεχομένου, όπως δεδομένα σχετικά με αλγοριθμικά ή άλλα συστήματα και διαδικασίες ελέγχου περιεχομένου, συμπεριλαμβανομένων καταλόγων αλλαγών, αρχείων ή αποθετηρίων που τεκμηριώνουν ελεγχόμενο περιεχόμενο, συμπεριλαμβανομένων λογαριασμών, καθώς και δεδομένων που σχετίζονται με τις τιμές, τις ποσότητες και τα χαρακτηριστικά αγαθών ή υπηρεσιών που παρέχει ο πάροχος δεδομένων ή για τα/τις οποία/-ες μεσολαβεί ο πάροχος δεδομένων.

(14) Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να επαληθεύει αν η αίτηση πρόσβασης σε δεδομένα προβλέπει την παροχή επαρκών πληροφοριών που αποδεικνύουν ότι ο ερευνητής είναι ικανός να εκπληρώσει τις ειδικές απαιτήσεις εμπιστευτικότητας, ασφάλειας και προστασίας των δεδομένων προσωπικού χαρακτήρα σε σχέση με τα ζητούμενα δεδομένα, να εντοπίζει πιθανούς κινδύνους που απορρέουν από την πρόσβαση στα εν λόγω δεδομένα και την επεξεργασία αυτών για τους σκοπούς της έρευνας, και να τεκμηριώνει τυχόν προτεινόμενες μεθόδους πρόσβασης, συμπεριλαμβανομένων των νομικών, οργανωτικών και τεχνικών προϋποθέσεων που θα τεθούν σε εφαρμογή για την ελαχιστοποίηση των εντοπισθέντων κινδύνων, για παράδειγμα μέσω επιστολής δέσμευσης από τον ερευνητικό οργανισμό που επιβεβαιώνει την πρόσβαση σε μέσα που μπορούν να αποτελέσουν συναφείς διασφαλίσεις, ή άλλα δικαιολογητικά.

(15) Όταν ζητούνται δεδομένα προσωπικού χαρακτήρα, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να επαληθεύει ότι η αίτηση πρόσβασης σε δεδομένα περιλαμβάνει πληροφορίες σχετικά με τη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, κατά περίπτωση, και αν η εν λόγω νομική βάση συνάδει με το άρθρο 6 παράγραφος 1 στοιχεία ε) ή στ) και, κατά περίπτωση, με το άρθρο 9 παράγραφος 2 στοιχεία ζ) ή ι) του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]). Επιπλέον, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να επαληθεύει ότι η αίτηση πρόσβασης σε δεδομένα περιέχει επαρκείς ενδείξεις ότι οι ερευνητές έχουν αξιολογήσει τους κινδύνους για την προστασία των δεδομένων προσωπικού χαρακτήρα. Για παράδειγμα, αυτό θα μπορούσε να αποδειχθεί με εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων κατά την έννοια του άρθρου 35 του εν λόγω κανονισμού. Για να διασφαλιστεί ότι η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα είναι δυνατή σύμφωνα με τον κανονισμό (ΕΕ) 2016/679, οι συντονιστές ψηφιακών υπηρεσιών θα πρέπει να έχουν τη δυνατότητα να ζητούν τη γνώμη των οικείων εποπτικών αρχών που έχουν συσταθεί σύμφωνα με το άρθρο 51 του εν λόγω κανονισμού, οι οποίες παραμένουν αρμόδιες για την αξιολόγηση της συμμόρφωσης με τον κανονισμό (ΕΕ) 2016/679.

([3]) 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).

(16) Για να διευκολυνθεί η διατύπωση του αιτιολογημένου αιτήματος και να διαφυλαχθεί η ακεραιότητα των πληροφοριών που περιλαμβάνονται στην αίτηση πρόσβασης σε δεδομένα, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να επαληθεύει αν η αίτηση πρόσβασης σε δεδομένα περιλαμβάνει περίληψη. Η εν λόγω περίληψη θα πρέπει να περιλαμβάνει επισκόπηση των πληροφοριών που θα αποτελέσουν μέρος του αιτιολογημένου αιτήματος, οι οποίες δημοσιεύονται στην πύλη πρόσβασης σε δεδομένα βάσει της DSA, σε περιπτώσεις στις οποίες η αξιολόγηση της αίτησης πρόσβασης σε δεδομένα οδηγεί στη διατύπωση αιτιολογημένου αιτήματος.

(17) Προκειμένου να διασφαλιστεί ότι οι μέθοδοι πρόσβασης που καθορίζει ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης επαρκούν για την αντιμετώπιση του ευαίσθητου χαρακτήρα των συγκεκριμένων δεδομένων που ζητούνται σε μια αίτηση πρόσβασης σε δεδομένα, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να διενεργεί κατά περίπτωση αξιολόγηση με βάση τις πληροφορίες που παρέχονται στην αίτηση πρόσβασης σε δεδομένα. Οι μέθοδοι πρόσβασης που καθορίζονται στο αιτιολογημένο αίτημα θα πρέπει να είναι κατάλληλες για την εκπλήρωση των απαιτήσεων ασφάλειας των δεδομένων, εμπιστευτικότητας των δεδομένων και προστασίας των δεδομένων προσωπικού χαρακτήρα, και ταυτόχρονα να καθιστούν δυνατή την επίτευξη των ερευνητικών στόχων του ερευνητικού έργου. Η πρόσβαση σε δεδομένα μπορεί να πραγματοποιείται, για παράδειγμα, μέσω διαβίβασης δεδομένων στους διαπιστευμένους ερευνητές με τη χρήση κατάλληλης διεπαφής και κατάλληλης αποθήκευσης δεδομένων, μέσω διαβίβασης και αποθήκευσης των δεδομένων σε ασφαλές περιβάλλον επεξεργασίας το οποίο διαχειρίζεται ο πάροχος δεδομένων ή τρίτος πάροχος στον οποίον έχουν πρόσβαση οι διαπιστευμένοι ερευνητές, αλλά εφόσον δεν πραγματοποιείται διαβίβαση δεδομένων στους διαπιστευμένους ερευνητές, ή μέσω άλλων μεθόδων πρόσβασης που καθορίζονται ή διευκολύνονται από τον πάροχο δεδομένων. Κατά τον καθορισμό των μεθόδων πρόσβασης, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει επίσης να αναφέρει τυχόν νομικές, τεχνικές ή οργανωτικές προϋποθέσεις στις οποίες πρέπει να υπόκειται η πρόσβαση. Σε περιπτώσεις στις οποίες η παροχή πρόσβασης συνεπάγεται διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς κατά την έννοια του κεφαλαίου V του κανονισμού (ΕΕ) 2016/679, οι μέθοδοι πρόσβασης θα πρέπει επίσης να περιλαμβάνουν πληροφορίες σχετικά με την ανάγκη θέσπισης κατάλληλου μηχανισμού διαβίβασης, ώστε να διασφαλίζεται ότι ο πάροχος δεδομένων λαμβάνει τα αναγκαία μέτρα για τη συμμόρφωση με τον εν λόγω κανονισμό.

(18) Για να διασφαλιστεί ότι οι μέθοδοι πρόσβασης στα δεδομένα είναι κατάλληλες προκειμένου να αντιμετωπιστούν συγκεκριμένες ευαισθησίες όσον αφορά την προστασία των δεδομένων, την ασφάλεια των δεδομένων ή την εμπιστευτικότητα, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης, βάσει των πληροφοριών που λαμβάνονται στην αίτηση πρόσβασης σε δεδομένα, θα πρέπει να είναι σε θέση να απαιτήσει την παροχή πρόσβασης στα δεδομένα μέσω ασφαλών περιβαλλόντων επεξεργασίας. Στις περιπτώσεις αυτές, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να διασφαλίζει ότι το επιλεγμένο περιβάλλον λειτουργεί σύμφωνα με την καταλληλότερη τεχνολογία και δίνει στους διαπιστευμένους ερευνητές τη δυνατότητα να επιτύχουν τους στόχους της έρευνάς τους.

(19) Προκειμένου να διασφαλιστεί η συνέπεια των πληροφοριών που διαβιβάζονται από τους συντονιστές ψηφιακών υπηρεσιών της χώρας εγκατάστασης στους παρόχους δεδομένων, είναι απαραίτητο να προσδιοριστεί το περιεχόμενο των αιτιολογημένων αιτημάτων.

(20) Προκειμένου να διασφαλιστούν τα συμφέροντα των παρόχων δεδομένων και να μειωθεί η συχνότητα των αιτημάτων τροποποίησης με την πάροδο του χρόνου και να διευκολυνθεί η διατύπωση σχετικών αιτήσεων πρόσβασης σε δεδομένα από ερευνητές, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης που εξέδωσε τα αντίστοιχα αιτιολογημένα αιτήματα θα πρέπει να δημοσιοποιεί στην πύλη πρόσβασης σε δεδομένα βάσει της DSA επισκόπηση κάθε αιτιολογημένου αιτήματος, συμπεριλαμβανομένων τυχόν τροποποιήσεων και επικαιροποιήσεών του.

(21) Προκειμένου να διασφαλιστεί ότι ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης διαθέτει τις σχετικές πληροφορίες για την αξιολόγηση ενός αιτήματος τροποποίησης και για να διευκολυνθεί η ενιαία προσέγγιση κατά την αξιολόγηση των αιτημάτων τροποποίησης, ο πάροχος δεδομένων θα πρέπει να υποχρεούται να προσδιορίσει τους λόγους του εν λόγω αιτήματος, όπως αναφέρεται στο άρθρο 40 παράγραφος 5 του κανονισμού (ΕΕ) 2022/2065. Ειδικότερα, κατά την αξιολόγηση αιτήματος τροποποίησης που υποβάλλεται λόγω έλλειψης πρόσβασης ενός παρόχου δεδομένων στα δεδομένα, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να είναι σε θέση να εξετάσει αν η εικαζόμενη αδυναμία είναι δεόντως αιτιολογημένη, για παράδειγμα λόγω της μη ύπαρξης των ζητούμενων δεδομένων ή λόγω τεχνικών περιορισμών όπως η κρυπτογράφηση, και θα πρέπει να έχει τις πληροφορίες που χρειάζεται προκειμένου να εξετάσει αν η έλλειψη πρόσβασης είναι μόνιμη ή προσωρινή. Στο πλαίσιο αυτό, θα πρέπει να καταστεί σαφές ότι οι εμπορικοί παράγοντες δεν θα πρέπει να εκλαμβάνονται ως λόγος για την αυτόματη άρνηση παροχής πρόσβασης σε ζητούμενα δεδομένα, αλλά θα πρέπει μάλλον να εκλαμβάνονται ως λόγος για την τροποποίηση των μέσων παροχής πρόσβασης στα δεδομένα, κάτι που μπορεί να οδηγήσει στην επιβολή πρόσθετων απαιτήσεων ασφάλειας και εμπιστευτικότητας των δεδομένων.

(22) Προκειμένου να διασφαλιστεί η αποτελεσματική επίλυση των διαφορών και να προωθηθεί ο προσδιορισμός μιας αμοιβαία αποδεκτής λύσης, κατόπιν αιτήματος τροποποίησης, οι πάροχοι δεδομένων θα πρέπει να είναι σε θέση να ζητούν από τους συντονιστές ψηφιακών υπηρεσιών της χώρας εγκατάστασης να συμμετάσχουν σε διαμεσολάβηση. Η συμμετοχή αυτή θα πρέπει να είναι εθελοντική καθ' όλη τη διάρκεια της διαδικασίας διαμεσολάβησης και δεν θα πρέπει να οδηγεί σε δεσμευτικό αποτέλεσμα για τον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης, ο οποίος παραμένει αρμόδιος για τη λήψη αποφάσεων σχετικά με τα αιτήματα τροποποίησης. Όλα τα μέρη που εμπλέκονται στη διαδικασία διαμεσολάβησης θα πρέπει να συμμετέχουν καλόπιστα και να επιδιώκουν την επίτευξη δίκαιης και αμοιβαία αποδεκτής συμφωνίας.

(23) Προκειμένου να αποφευχθεί η επ' αόριστον παράταση της διαδικασίας πρόσβασης σε δεδομένα εξαιτίας της διαμεσολάβησης, η διαβίβαση του γραπτού αιτήματος διαμεσολάβησης, η επιλογή του διαμεσολαβητή και αυτή καθαυτή η διαδικασία διαμεσολάβησης θα πρέπει να πραγματοποιούνται εντός καθορισμένων χρονικών πλαισίων. Οι συντονιστές ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να ορίζουν προθεσμία για τη διαδικασία διαμεσολάβησης σε σχέση με συγκεκριμένο αιτιολογημένο αίτημα, ενώ ο διαμεσολαβητής θα πρέπει να έχει την εξουσία να τερματίσει τη διαδικασία διαμεσολάβησης υπό συγκεκριμένες περιστάσεις.

(24) Προκειμένου να διατηρηθεί η αμοιβαία εμπιστοσύνη μεταξύ των μερών που συμμετέχουν στη διαμεσολάβηση, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θα πρέπει να διασφαλίζει ότι ο προτεινόμενος διαμεσολαβητής πληροί τις απαιτήσεις αμεροληψίας και ανεξαρτησίας και διαθέτει σχετική εμπειρογνωσία στο αντικείμενο της διαμεσολάβησης.

(25) Προκειμένου να διευκολυνθεί η τεκμηριωμένη και αποτελεσματική λήψη αποφάσεων σε σχέση με τη διαδικασία πρόσβασης σε δεδομένα, οι συντονιστές ψηφιακών υπηρεσιών θα πρέπει να έχουν τη δυνατότητα να ζητούν γνωμοδοτήσεις εμπειρογνωμόνων σχετικά με συγκεκριμένα στοιχεία της διαδικασίας πρόσβασης σε δεδομένα, όπως ο καθορισμός των μεθόδων πρόσβασης, συμπεριλαμβανομένων των κατάλληλων διεπαφών, καθώς και η διατύπωση του αιτιολογημένου αιτήματος και τυχόν αιτημάτων τροποποίησης από τον πάροχο δεδομένων. Οι εμπειρογνώμονες των οποίων ζητείται η γνώμη θα πρέπει να διαθέτουν αποδεδειγμένη εμπειρογνωσία στο θέμα για το οποίο ζητείται η γνώμη τους και να είναι ανεξάρτητοι. Ειδικότερα, δεν θα πρέπει να έχουν σύγκρουση συμφερόντων η οποία απορρέει, για παράδειγμα, από τυχόν δεσμούς με τους αιτούντες ερευνητές ή με τον πάροχο των δεδομένων.

(26) Προκειμένου να ενισχυθεί η διαφάνεια και να δοθεί η δυνατότητα στους συντονιστές ψηφιακών υπηρεσιών να αξιοποιήσουν την εμπειρογνωσία που απέκτησαν με την πάροδο του χρόνου, κάθε αίτημα διαβούλευσης με εμπειρογνώμονες και η παρακολούθησή του θα πρέπει να καταχωρίζονται στο σύστημα AGORA.

(27) Προκειμένου να διευκολυνθεί η αποτελεσματική εποπτεία της συμμόρφωσης με τις προϋποθέσεις που καθορίζονται στο αιτιολογημένο αίτημα, ο πάροχος δεδομένων θα πρέπει να ενημερώνει τον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης εντός τριών εργάσιμων ημερών από την ημερομηνία κατά την οποία παρασχέθηκε πρόσβαση στους διαπιστευμένους ερευνητές και από την ημερομηνία τερματισμού της πρόσβασης.

(28) Προκειμένου να μπορούν οι διαπιστευμένοι ερευνητές να χρησιμοποιούν τα ζητούμενα δεδομένα για τους σκοπούς της έρευνας και να παρέχουν σχετικές πληροφορίες πλαισίου, οι πάροχοι δεδομένων θα πρέπει να παρέχουν στους διαπιστευμένους ερευνητές τα σχετικά μεταδεδομένα και τη σχετική τεκμηρίωση όπου περιγράφονται τα διατιθέμενα δεδομένα, όπως εγχειρίδια κωδικοποίησης δεδομένων, κατάλογοι αλλαγών και τεκμηρίωση της υποδομής δεδομένων.

(29) Προκειμένου να διευκολυνθεί η ουσιαστική έρευνα για τους διαπιστευμένους ερευνητές, μεταξύ άλλων καθιστώντας δυνατό τον συνδυασμό των ζητούμενων δεδομένων με δεδομένα διαθέσιμα μέσω άλλων πηγών, οι πάροχοι δεδομένων δεν θα πρέπει να επιβάλλουν περιορισμούς στα εργαλεία ανάλυσης που χρησιμοποιούν οι διαπιστευμένοι ερευνητές, συμπεριλαμβανομένων των σχετικών βιβλιοθηκών λογισμικού, και δεν θα πρέπει να επιβάλλουν απαιτήσεις αρχειοθέτησης, αποθήκευσης, ανανέωσης και διαγραφής, εκτός εάν οι εν λόγω απαιτήσεις ή περιορισμοί αναφέρονται ρητά στις μεθόδους πρόσβασης που προσδιορίζονται στο αιτιολογημένο αίτημα.

(30) Όταν στα δεδομένα που παρέχονται στους διαπιστευμένους ερευνητές περιλαμβάνονται δεδομένα προσωπικού χαρακτήρα κατά την έννοια του άρθρου 4 του κανονισμού (ΕΕ) 2016/679, ο πάροχος δεδομένων θα πρέπει να τηρεί τους κανόνες που ορίζονται στον εν λόγω κανονισμό. Ειδικότερα, με το άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065 θεσπίζεται νομική υποχρέωση κατά την έννοια του άρθρου 6 παράγραφος 1 στοιχείο γ) του κανονισμού (ΕΕ) 2016/679 για κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητη προκειμένου ο πάροχος δεδομένων να παρέχει πρόσβαση στα δεδομένα που προσδιορίζονται στο αιτιολογημένο αίτημα. Σε περιπτώσεις στις οποίες πρόκειται να υποβληθούν σε επεξεργασία ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα κατά την έννοια του άρθρου 9 του κανονισμού (ΕΕ) 2016/679, ο παρών κανονισμός πληροί την απαίτηση του άρθρου 9 παράγραφος 2 σημείο ζ) του κανονισμού (ΕΕ) 2016/679.

(31) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]), η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 4 Δεκεμβρίου 2024.

(32) Αφού ζητήθηκε η γνώμη του ευρωπαϊκού συμβουλίου ψηφιακών υπηρεσιών σύμφωνα με το άρθρο 40 παράγραφος 13 του κανονισμού (ΕΕ) 2022/2065 και ελήφθη η έγκρισή του,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΚΕΦΑΛΑΙΟ I

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο

Ο παρών κανονισμός καθορίζει τις διαδικασίες και τις τεχνικές προϋποθέσεις για την παροχή σε διαπιστευμένους ερευνητές πρόσβασης σε δεδομένα που κατέχουν πάροχοι πολύ μεγάλων επιγραμμικών πλατφορμών και πολύ μεγάλων επιγραμμικών μηχανών αναζήτησης, σύμφωνα με το άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065, πιο συγκεκριμένα:

α) τις τεχνικές προϋποθέσεις για την ανάπτυξη και τη λειτουργία πύλης πρόσβασης σε δεδομένα·

β) τις διαδικασίες και τις τεχνικές προϋποθέσεις για τη διαχείριση της διαδικασίας πρόσβασης σε δεδομένα από τους συντονιστές ψηφιακών υπηρεσιών και τους παρόχους δεδομένων·

γ) τις απαιτήσεις για τη διατύπωση αιτιολογημένων αιτημάτων και την αξιολόγηση των αιτημάτων τροποποίησης·

δ) τις τεχνικές προϋποθέσεις για την παροχή πρόσβασης σε δεδομένα από τους παρόχους δεδομένων.

Άρθρο 2

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ορισμοί που προβλέπονται στο άρθρο 4 του κανονισμού (ΕΕ) 2016/679 και στο άρθρο 3 του κανονισμού (ΕΕ) 2018/1725. Ισχύουν επίσης οι ακόλουθοι ορισμοί:

1) «αίτηση πρόσβασης σε δεδομένα»: οι πληροφορίες και τα σχετικά έγγραφα που υποβάλλουν οι αιτούντες ερευνητές στον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης ή στον συντονιστή ψηφιακών υπηρεσιών του κράτους μέλους του ερευνητικού οργανισμού με τον οποίον συνδέεται ο κύριος ερευνητής, προκειμένου να αποκτήσουν το καθεστώς του «διαπιστευμένου ερευνητή», όπως αναφέρεται στο άρθρο 40 παράγραφος 8 πρώτο εδάφιο του κανονισμού (ΕΕ) 2022/2065, για συγκεκριμένο ερευνητικό έργο που περιλαμβάνει πρόσβαση σε δεδομένα τα οποία παρέχει πάροχος δεδομένων·

2) «διαδικασία πρόσβασης σε δεδομένα»: τα στάδια και οι διαδικασίες που ενδέχεται να οδηγήσουν στην παροχή πρόσβασης στα δεδομένα, όπως αναφέρεται στο άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065·

3) «αιτών ερευνητής»: κάθε φυσικό πρόσωπο που υποβάλλει αίτηση πρόσβασης σε δεδομένα, όπως αναφέρεται στο άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065, είτε ατομικά είτε στο πλαίσιο ομάδας είτε ως μέρος οντότητας·

4) «κύριος ερευνητής»: αιτών ερευνητής που υποβάλλει την αίτηση πρόσβασης σε δεδομένα υπό την ατομική του ιδιότητα ή για λογαριασμό οντότητας ή ομάδας αιτούντων ερευνητών·

5) «πάροχος δεδομένων»: πάροχος πολύ μεγάλης επιγραμμικής πλατφόρμας ή πολύ μεγάλης επιγραμμικής μηχανής αναζήτησης που έχει οριστεί ως τέτοιος σύμφωνα με το άρθρο 33 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065, και στον οποίον μπορεί να υποβληθεί αιτιολογημένο αίτημα·

([4]) 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).

6) «αιτιολογημένο αίτημα»: αιτιολογημένο αίτημα πρόσβασης σε δεδομένα σύμφωνα με το άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065·

7) «αίτημα τροποποίησης»: αίτημα τροποποίησης σύμφωνα με το άρθρο 40 παράγραφος 5 του κανονισμού (ΕΕ) 2022/2065 που υποβάλλεται από τον πάροχο δεδομένων στον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης μετά τη λήψη αιτιολογημένου αιτήματος·

8) «ασφαλές περιβάλλον επεξεργασίας»: ασφαλές περιβάλλον επεξεργασίας όπως ορίζεται στο άρθρο 2 σημείο 20 του κανονισμού (ΕΕ) 2022/868 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]).

ΚΕΦΑΛΑΙΟ II

ΥΠΟΧΡΕΩΣΕΙΣ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΣ

Άρθρο 3

Πύλη πρόσβασης σε δεδομένα βάσει της DSA

1. Η Επιτροπή δημιουργεί και φιλοξενεί πύλη πρόσβασης σε δεδομένα βάσει της DSA.

2. Η πύλη πρόσβασης σε δεδομένα βάσει της DSA έχει τις ακόλουθες λειτουργίες:

α) στηρίζει και εξορθολογίζει τη διαχείριση της διαδικασίας πρόσβασης σε δεδομένα για ερευνητές, παρόχους δεδομένων και συντονιστές ψηφιακών υπηρεσιών·

β) λειτουργεί ως κεντρικό ψηφιακό σημείο ενημέρωσης σχετικά με τη διαδικασία πρόσβασης σε δεδομένα και διευκολύνει τις ανταλλαγές πληροφοριών σύμφωνα με τον παρόντα κανονισμό μεταξύ αιτούντων ερευνητών, διαπιστευμένων ερευνητών, παρόχων δεδομένων και συντονιστών ψηφιακών υπηρεσιών.

3. Η πύλη πρόσβασης σε δεδομένα βάσει της DSA είναι διαλειτουργική με το σύστημα ανταλλαγής πληροφοριών AGORA που δημιουργήθηκε με βάση τον εκτελεστικό κανονισμό (ΕΕ) 2024/607. Οι συντονιστές ψηφιακών υπηρεσιών έχουν πρόσβαση, με τη χρήση του συστήματος AGORA, στις πληροφορίες που υποβάλλονται μέσω της πύλης πρόσβασης σε δεδομένα βάσει της DSA.

4. Οι πάροχοι δεδομένων διαθέτουν λογαριασμό στην πύλη πρόσβασης σε δεδομένα βάσει της DSA.

5. Για να συμμετάσχουν στη διαδικασία πρόσβασης σε δεδομένα, οι αιτούντες ερευνητές διαθέτουν λογαριασμό στην πύλη πρόσβασης σε δεδομένα βάσει της DSA.

Άρθρο 4

Ρόλοι και αρμοδιότητες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στην πύλη πρόσβασης σε δεδομένα βάσει της DSA

1. Οι συντονιστές ψηφιακών υπηρεσιών είναι διακριτοί υπεύθυνοι επεξεργασίας όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα που διενεργούν με στόχο τη διαχείριση της διαδικασίας πρόσβασης σε δεδομένα και για τη δημοσίευση σχετικών πληροφοριών.

2. Η Επιτροπή είναι η εκτελούσα την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία εντός της πύλης πρόσβασης σε δεδομένα βάσει της DSA.

3. Οι αρμοδιότητες της Επιτροπής ως εκτελούσας την επεξεργασία για τις δραστηριότητες επεξεργασίας δεδομένων που πραγματοποιούνται στην πύλη πρόσβασης σε δεδομένα βάσει της DSA καθορίζονται στο παράρτημα.

([5]) Κανονισμός (ΕΕ) 2022/868 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2022, σχετικά με την ευρωπαϊκή διακυβέρνηση δεδομένων και την τροποποίηση του κανονισμού (ΕΕ) 2018/1724 (πράξη για τη διακυβέρνηση δεδομένων) (ΕΕ L 152 της 3.6.2022, σ. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

Άρθρο 5

Επεξεργασία δεδομένων προσωπικού χαρακτήρα στην πύλη πρόσβασης σε δεδομένα βάσει της DSA

1. Όταν δεδομένα προσωπικού χαρακτήρα καταχωρίζονται και ανταλλάσσονται μέσω της πύλης πρόσβασης σε δεδομένα βάσει της DSA, η επεξεργασία πραγματοποιείται μόνο στον βαθμό που είναι αναλογική και αναγκαία για τους σκοπούς της διαδικασίας πρόσβασης σε δεδομένα και της δημοσίευσης σχετικών πληροφοριών.

2. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της πύλης πρόσβασης σε δεδομένα βάσει της DSA πραγματοποιείται μόνο για τις ακόλουθες κατηγορίες υποκειμένων των δεδομένων:

α) φυσικά πρόσωπα που διαθέτουν λογαριασμό στην πύλη πρόσβασης σε δεδομένα βάσει της DSA·

β) φυσικά πρόσωπα των οποίων τα δεδομένα προσωπικού χαρακτήρα περιλαμβάνονται στην πύλη πρόσβασης σε δεδομένα βάσει της DSA ή σε οποιαδήποτε άλλη ανταλλαγή σύμφωνα με τον παρόντα κανονισμό όσον αφορά τη διαδικασία πρόσβασης σε δεδομένα.

3. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της πύλης πρόσβασης σε δεδομένα βάσει της DSA πραγματοποιείται μόνο για τις ακόλουθες κατηγορίες δεδομένων προσωπικού χαρακτήρα:

α) δεδομένα ταυτότητας, όπως όνομα, ταυτότητα χρήστη·

β) στοιχεία επικοινωνίας, όπως διεύθυνση, διεύθυνση ηλεκτρονικού ταχυδρομείου, στοιχεία επικοινωνίας·

γ) δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται στα έγγραφα τα οποία αποδεικνύουν τη σύνδεση με ερευνητικό οργανισμό, καθώς και κάθε άλλη πληροφορία προσωπικού χαρακτήρα που κρίνεται απαραίτητη όσον αφορά τη συμμετοχή στη διαδικασία πρόσβασης σε δεδομένα.

4. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που αναφέρονται στην παράγραφο 1 πραγματοποιείται με τη χρήση υποδομής τεχνολογίας πληροφοριών η οποία βρίσκεται στον Ευρωπαϊκό Οικονομικό Χώρο.

Άρθρο 6

Σημεία επαφής και ενημέρωση του κοινού σχετικά με τη διαδικασία πρόσβασης σε δεδομένα

1. Κάθε συντονιστής ψηφιακών υπηρεσιών και κάθε πάροχος δεδομένων δημιουργεί ειδικό σημείο επαφής, καθήκον του οποίου είναι η παροχή πληροφοριών και υποστήριξης σχετικά με τη διαδικασία πρόσβασης σε δεδομένα.

2. Οι συντονιστές ψηφιακών υπηρεσιών και οι πάροχοι δεδομένων κοινοποιούν τα σημεία επαφής τους στην Επιτροπή, το συντομότερο δυνατόν. Η Επιτροπή δημοσιεύει τα στοιχεία των σημείων επαφής που αναφέρονται στην παράγραφο 1 στη δημόσια διεπαφή της πύλης πρόσβασης σε δεδομένα βάσει της DSA.

3. Κάθε συντονιστής ψηφιακών υπηρεσιών φροντίζει ώστε τα στοιχεία του σημείου επαφής που δημιουργείται σύμφωνα με την παράγραφο 1 να είναι διαθέσιμα και εύκολα ευρέσιμα στην επιγραμμική διεπαφή του, μαζί με σύνδεσμο προς την πύλη πρόσβασης σε δεδομένα βάσει της DSA.

4. Οι πάροχοι δεδομένων φροντίζουν ώστε οι ακόλουθες πληροφορίες να είναι διαθέσιμες και εύκολα ευρέσιμες στις επιγραμμικές διεπαφές τους:

α) τα στοιχεία του σημείου επαφής που έχουν δημιουργήσει σύμφωνα με την παράγραφο 1·

β) σύνδεσμος προς την πύλη πρόσβασης σε δεδομένα βάσει της DSA·

γ) κατάλογος δεδομένων βάσει της DSA, στον οποίον περιγράφονται οι πόροι δεδομένων στους οποίους είναι δυνατή η πρόσβαση για τους σκοπούς που ορίζονται στο άρθρο 40 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2065, καθώς επίσης και η δομή των δεδομένων και τα μεταδεδομένα τους·

δ) προτεινόμενες μέθοδοι πρόσβασης για τα δεδομένα του καταλόγου που αναφέρεται στο στοιχείο γ), οι οποίες είναι κατάλληλες για το επίπεδο ευαισθησίας των διαφόρων πόρων δεδομένων.

5. Οι πληροφορίες που αναφέρονται στην παράγραφο 4 στοιχεία γ) και δ) επικαιροποιούνται τακτικά, ιδίως προκειμένου να αντικατοπτρίζουν τα δεδομένα που σχετίζονται με τις εκτιμήσεις κινδύνων οι οποίες διενεργούνται σύμφωνα με το άρθρο 34 του κανονισμού (ΕΕ) 2022/2065 και τους ελέγχους οι οποίοι διενεργούνται σύμφωνα με το άρθρο 37 του εν λόγω κανονισμού.

ΚΕΦΑΛΑΙΟ III

ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΗ ΔΙΑΤΥΠΩΣΗ ΚΑΙ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΑΙΤΙΟΛΟΓΗΜΕΝΩΝ ΑΙΤΗΜΑΤΩΝ

Άρθρο 7

Διατύπωση αιτιολογημένου αιτήματος

1. Εντός 80 εργάσιμων ημερών από την υποβολή αίτησης πρόσβασης σε δεδομένα, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης, λαμβάνοντας δεόντως υπόψη τις προϋποθέσεις που προβλέπονται στο άρθρο 8 και, κατά περίπτωση, κάθε άλλη αξιολόγηση σχετική με τους σκοπούς αυτούς, αποφασίζει αν μπορεί να διατυπωθεί αιτιολογημένο αίτημα και προβαίνει σε μία από τις ακόλουθες ενέργειες:

α) διατυπώνει αιτιολογημένο αίτημα, το υποβάλλει στον πάροχο δεδομένων και ενημερώνει τον κύριο ερευνητή για την υποβολή του αιτιολογημένου αιτήματος·

β) ενημερώνει τον κύριο ερευνητή για τους λόγους για τους οποίους δεν κατέστη δυνατή η διατύπωση αιτιολογημένου αιτήματος.

2. Όταν, σε δεόντως αιτιολογημένες περιπτώσεις, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης χρειάζεται πρόσθετο χρόνο για να διατυπώσει αιτιολογημένο αίτημα, ενημερώνει τον κύριο ερευνητή το συντομότερο δυνατόν και αναφέρει τους λόγους της καθυστέρησης, και ορίζει επίσης νέα ημερομηνία για την πραγματοποίηση των ενεργειών που αναφέρονται στην παράγραφο 1.

Άρθρο 8

Προϋποθέσεις για τη διατύπωση αιτιολογημένου αιτήματος

Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης αποφασίζει αν μπορεί να διατυπωθεί αιτιολογημένο αίτημα λαμβάνοντας υπόψη τα ακόλουθα στοιχεία:

α) για κάθε αιτούντα ερευνητή:

i) βεβαίωση σύνδεσης με ερευνητικό οργανισμό όπως ορίζεται στο άρθρο 2 σημείο 1) της οδηγίας (ΕΕ) 2019/790 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6])·

ii) δήλωση ανεξαρτησίας από εμπορικά συμφέροντα σχετικά με το συγκεκριμένο έργο για το οποίο ζητούνται τα δεδομένα·

iii) δέσμευση για δωρεάν δημοσιοποίηση των αποτελεσμάτων της έρευνάς τους·

β) πληροφορίες σχετικά με τη χρηματοδότηση που υποστηρίζει το ερευνητικό έργο για το οποίο ζητούνται τα δεδομένα·

γ) περιγραφή των ζητούμενων δεδομένων, συμπεριλαμβανομένων του μορφότυπου, του πεδίου εφαρμογής και, όπου είναι δυνατόν, των ειδικών χαρακτηριστικών, των σχετικών μεταδεδομένων και της τεκμηρίωσης των δεδομένων, λαμβανομένων επίσης υπόψη των πληροφοριών που καθίστανται διαθέσιμα σύμφωνα με το άρθρο 6 παράγραφος 4 του παρόντος κανονισμού·

δ) πληροφορίες σχετικά με την αναγκαιότητα και την αναλογικότητα της πρόσβασης στα δεδομένα και πληροφορίες σχετικά με τα χρονικά πλαίσια της έρευνας για την οποία ζητούνται τα δεδομένα·

ε) πληροφορίες σχετικά με τους εντοπισθέντες κινδύνους όσον αφορά την εμπιστευτικότητα, την ασφάλεια των δεδομένων και την προστασία των δεδομένων προσωπικού χαρακτήρα που σχετίζονται με τα δεδομένα στα οποία θα παρέχεται πρόσβαση, περιγραφή των τεχνικών, νομικών και οργανωτικών μέτρων που θα τεθούν σε εφαρμογή, συμπεριλαμβανομένων, όπου είναι δυνατόν, των προτεινόμενων μεθόδων πρόσβασης, με στόχο τον περιορισμό των εν λόγω κινδύνων κατά την επεξεργασία των ζητούμενων δεδομένων·

στ) περιγραφή των ερευνητικών δραστηριοτήτων που θα πραγματοποιηθούν με τα ζητούμενα δεδομένα·

ζ) περίληψη της αίτησης πρόσβασης σε δεδομένα που περιέχει τα ακόλουθα στοιχεία:

i) το θέμα της έρευνας·

ii) τον πάροχο δεδομένων από τον οποίο ζητούνται τα δεδομένα·

iii) περιγραφή των ζητούμενων δεδομένων, όπως αναφέρεται στο στοιχείο γ).

([6]) Οδηγία (ΕΕ) 2019/790 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, για τα δικαιώματα πνευματικής ιδιοκτησίας και τα συγγενικά δικαιώματα στην ψηφιακή ενιαία αγορά και την τροποποίηση των οδηγιών 96/9/ΕΚ και 2001/29/ΕΚ (ΕΕ L 130 της 17.5.2019, σ. 92, ELI: http://data.europa.eu/eli/dir/2019/790/oj).

Άρθρο 9

Μέθοδοι πρόσβασης

1. Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης καθορίζει τις μεθόδους, συμπεριλαμβανομένων των τεχνικών, νομικών και οργανωτικών μέτρων, που θα χρησιμοποιήσει ο πάροχος δεδομένων προκειμένου να παράσχει στους διαπιστευμένους ερευνητές πρόσβαση στα δεδομένα.

2. Οι συντονιστές ψηφιακών υπηρεσιών έχουν τη δυνατότητα να ζητούν τη γνώμη των σχετικών εποπτικών αρχών που έχουν συσταθεί σύμφωνα με το άρθρο 51 του κανονισμού (ΕΕ) 2016/679.

3. Κατά τον καθορισμό των μεθόδων πρόσβασης, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης λαμβάνει υπόψη τις πληροφορίες που παρέχονται στην αίτηση πρόσβασης σε δεδομένα, ιδίως τις πληροφορίες που αναφέρονται στο άρθρο 8 στοιχείο ε), συνυπολογίζοντας επίσης τα δικαιώματα και τα συμφέροντα των παρόχων δεδομένων και των αποδεκτών της οικείας υπηρεσίας, συμπεριλαμβανομένης της προστασίας των εμπιστευτικών πληροφοριών και των εμπορικών απορρήτων, διατηρώντας παράλληλα την ασφάλεια της υπηρεσίας τους και των πληροφοριών που διατίθενται από τους παρόχους δεδομένων σύμφωνα με το άρθρο 6 παράγραφος 4 στοιχείο δ).

4. Πέραν των στοιχείων που αναφέρονται στην παράγραφο 3, κατά τον καθορισμό των μεθόδων πρόσβασης, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης λαμβάνει υπόψη τα ακόλουθα στοιχεία:

α) όταν η πρόσβαση περιλαμβάνει επεξεργασία δεδομένων προσωπικού χαρακτήρα:

   i. την εκτίμηση των κινδύνων όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως περιγράφεται στο άρθρο 8 στοιχείο ε), συμπεριλαμβανομένων, κατά περίπτωση, των εκτιμήσεων αντικτύπου σχετικά με την προστασία των δεδομένων κατά την έννοια του άρθρου 35 του κανονισμού (ΕΕ) 2016/679·

   ii. τα προβλεπόμενα τεχνικά και οργανωτικά μέτρα που υποβάλλονται σύμφωνα με το άρθρο 8 στοιχείο ε)·

β) τα σχετικά μέτρα ασφάλειας δικτύου, την κρυπτογράφηση, τους μηχανισμούς ελέγχου της πρόσβασης, τις πολιτικές δημιουργίας αντιγράφων ασφαλείας, τους μηχανισμούς διασφάλισης της ακεραιότητας των δεδομένων, τα σχέδια αντιμετώπισης συμβάντων·

γ) κατά περίπτωση, πληροφορίες σχετικά με την προβλεπόμενη περίοδο αποθήκευσης και τα σχετικά σχέδια καταστροφής δεδομένων·

δ) τυχόν οργανωτικά μέτρα, όπως διαδικασίες εσωτερικής επιθεώρησης, περιορισμοί των δικαιωμάτων πρόσβασης και ανταλλαγής πληροφοριών·

ε) τυχόν προτεινόμενες συμβατικές ρήτρες, όπως συμφωνίες εμπιστευτικότητας, συμφωνίες περί δεδομένων και άλλες γραπτές δηλώσεις κάθε είδους, όπου καθορίζονται πιθανές προϋποθέσεις πρόσβασης και επεξεργασίας μεταξύ του κύριου ερευνητή και του παρόχου δεδομένων·

στ) ύπαρξη κατάρτισης σχετικά με την ασφάλεια των δεδομένων και την προστασία των δεδομένων προσωπικού χαρακτήρα που λαμβάνουν οι αιτούντες ερευνητές·

ζ) αν απαιτούνται ασφαλή περιβάλλοντα επεξεργασίας για την επεξεργασία των δεδομένων.

5. Όταν ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης θεωρεί ότι πρόκειται να χρησιμοποιηθεί ασφαλές περιβάλλον επεξεργασίας για την παροχή πρόσβασης στα ζητούμενα δεδομένα, ο εν λόγω συντονιστής απαιτεί έγγραφα τα οποία πιστοποιούν ότι ο φορέας εκμετάλλευσης του εν λόγω περιβάλλοντος:

α) καθορίζει τις προϋποθέσεις πρόσβασης στο ασφαλές περιβάλλον επεξεργασίας προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μη εξουσιοδοτημένης ανάγνωσης, αντιγραφής, τροποποίησης ή αφαίρεσης των δεδομένων που φιλοξενούνται στο εν λόγω περιβάλλον·

β) διασφαλίζει ότι οι διαπιστευμένοι ερευνητές έχουν πρόσβαση μόνο στα δεδομένα που καλύπτονται από το αιτιολογημένο αίτημα, μέσω ατομικών και μοναδικών ταυτοτήτων χρήστη και εμπιστευτικών μεθόδων πρόσβασης·

γ) τηρεί ταυτοποιήσιμα αρχεία καταγραφής της πρόσβασης στο ασφαλές περιβάλλον επεξεργασίας για το χρονικό διάστημα που απαιτείται για την επαλήθευση και τον έλεγχο όλων των πράξεων επεξεργασίας στο εν λόγω περιβάλλον·

δ) διασφαλίζει ότι η υπολογιστική ισχύς που έχουν στη διάθεσή τους οι διαπιστευμένοι ερευνητές είναι κατάλληλη και επαρκής για τους σκοπούς του ερευνητικού έργου·

ε) παρακολουθεί την αποτελεσματικότητα των μέτρων που απαριθμούνται στα στοιχεία α) έως δ).

Άρθρο 10

Περιεχόμενο του αιτιολογημένου αιτήματος

1. Το αιτιολογημένο αίτημα περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία:

α) την ημερομηνία έως την οποία ο πάροχος δεδομένων παρέχει πρόσβαση στα ζητούμενα δεδομένα και την ημερομηνία κατά την οποία τερματίζεται η εν λόγω πρόσβαση·

β) τις μεθόδους πρόσβασης που καθορίζονται σύμφωνα με το άρθρο 9·

γ) την περίληψη της αίτησης πρόσβασης σε δεδομένα που αναφέρεται στο άρθρο 8 στοιχείο ζ).

2. Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης μπορεί να συμπεριλάβει στο αιτιολογημένο αίτημα τα ονόματα και τα στοιχεία επικοινωνίας όλων των διαπιστευμένων ερευνητών που αναφέρονται στην αίτηση πρόσβασης σε δεδομένα όταν αυτό είναι αναγκαίο για να καταστεί δυνατή η πρόσβαση στα ζητούμενα δεδομένα, σύμφωνα με τις μεθόδους πρόσβασης που καθορίζονται στο αιτιολογημένο αίτημα.

3. Εάν η παροχή πρόσβασης συνεπάγεται διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνή οργανισμό κατά την έννοια του κεφαλαίου V του κανονισμού (ΕΕ) 2016/679, το αιτιολογημένο αίτημα περιλαμβάνει πληροφορίες σχετικά με την ανάγκη θέσπισης ή αναφοράς κατάλληλου μηχανισμού διαβίβασης, ώστε να διασφαλίζεται η συμμόρφωση με τον κανονισμό (ΕΕ) 2016/679.

Άρθρο 11

Δημοσίευση επισκόπησης αιτιολογημένου αιτήματος στην πύλη πρόσβασης σε δεδομένα βάσει της DSA

1. Μετά τη διατύπωση αιτιολογημένου αιτήματος, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης δημοσιεύει επισκόπηση του αιτιολογημένου αιτήματος στη δημόσια διεπαφή της πύλης πρόσβασης σε δεδομένα βάσει της DSA. Η επισκόπηση περιλαμβάνει όλα τα εξής:

α) την περίληψη της αίτησης πρόσβασης σε δεδομένα που αναφέρεται στο άρθρο 8 στοιχείο ζ)·

β) τις μεθόδους πρόσβασης που καθορίζονται σύμφωνα με το άρθρο 9.

2. Η επισκόπηση που αναφέρεται στην παράγραφο 1 επικαιροποιείται ώστε να αντικατοπτρίζει τυχόν αλλαγές που προκύπτουν από τροποποίηση ενός ή περισσότερων στοιχείων μετά την εξέταση αιτήματος τροποποίησης ή το αποτέλεσμα διαμεσολάβησης σύμφωνα με το άρθρο 13.

Άρθρο 12

Διαδικασίες εξέτασης αιτημάτων τροποποίησης

1. Μετά την παραλαβή αιτήματος τροποποίησης σύμφωνα με το άρθρο 40 παράγραφος 5 του κανονισμού (ΕΕ) 2022/2065, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης ενημερώνει τον κύριο ενδιαφερόμενο ερευνητή.

2. Κατά τη λήψη απόφασης σχετικά με αίτημα τροποποίησης που υποβάλλεται σύμφωνα με το άρθρο 40 παράγραφος 5 στοιχείο α) του κανονισμού (ΕΕ) 2022/2065, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης λαμβάνει υπόψη τα ακόλουθα στοιχεία:

α) αν οι λόγοι για την εικαζόμενη έλλειψη πρόσβασης στα δεδομένα είναι δεόντως τεκμηριωμένοι·

β) αν η εν λόγω έλλειψη πρόσβασης στα δεδομένα είναι μόνιμη ή προσωρινή.

3. Κατά τη λήψη απόφασης σχετικά με αίτημα τροποποίησης που υποβάλλεται σύμφωνα με το άρθρο 40 παράγραφος 5 στοιχείο α) του κανονισμού (ΕΕ) 2022/2065, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης λαμβάνει υπόψη όλα τα ακόλουθα στοιχεία:

α) αν τα εικαζόμενα τρωτά σημεία και η σημασία τους έχουν τεκμηριωθεί δεόντως·

β) την πιθανότητα και τη σοβαρότητα βλάβης που προκύπτει από τα εν λόγω εικαζόμενα σημαντικά τρωτά σημεία·

γ) τον βαθμό στον οποίον οι μέθοδοι πρόσβασης που καθορίζονται στο αιτιολογημένο αίτημα περιορίζουν αποτελεσματικά τον κίνδυνο πρόκλησης τέτοιου είδους βλάβης.

4. Ανά πάσα στιγμή κατά την αξιολόγηση αιτήματος τροποποίησης, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης μπορεί να ζητήσει από τον πάροχο δεδομένων ή τον κύριο ερευνητή κάθε πρόσθετη πληροφορία που θεωρεί αναγκαία για την ολοκλήρωση της αξιολόγησής του.

5. Το εν λόγω αίτημα παροχής συμπληρωματικών πληροφοριών υποβάλλεται το συντομότερο δυνατόν ώστε να έχει ο πάροχος δεδομένων ή ο κύριος ερευνητής επαρκή χρόνο για να απαντήσει, τηρώντας, σε κάθε περίπτωση, την προθεσμία που ορίζεται στο άρθρο 40 παράγραφος 6 δεύτερο εδάφιο του κανονισμού (ΕΕ) 2022/2065. Εάν ο πάροχος δεδομένων ή ο κύριος ερευνητής δεν παράσχει καν τις ζητούμενες πληροφορίες, ή εάν δεν τις παράσχει εντός της προθεσμίας που έχει ορίσει ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης, ή εάν τις παράσχει εν μέρει, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης λαμβάνει την απόφασή του εντός του χρονικού πλαισίου που ορίζεται στο άρθρο 40 παράγραφος 6 του κανονισμού (ΕΕ) 2022/2065 με βάση τις πληροφορίες που τέθηκαν στη διάθεσή του με εύλογη καθυστέρηση.

Άρθρο 13

Διαμεσολάβηση

1. Εάν ο πάροχος δεδομένων διαφωνεί με την απόφαση του συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης σχετικά με το αίτημα τροποποίησης, ο πάροχος δεδομένων μπορεί, εντός πέντε εργάσιμων ημερών από την κοινοποίηση που απέστειλε ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης σύμφωνα με το άρθρο 40 παράγραφος 6 δεύτερο εδάφιο του κανονισμού (ΕΕ) 2022/2065, να ζητήσει γραπτώς από τον εν λόγω συντονιστή να συμμετάσχει σε διαμεσολάβηση.

2. Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης δεν υποχρεούται να συμμετάσχει στη διαδικασία διαμεσολάβησης.

3. Το γραπτό αίτημα που αναφέρεται στην παράγραφο 1 περιλαμβάνει συνοπτική περιγραφή των ειδικών στοιχείων της απόφασης —την οποία κοινοποιεί ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης σύμφωνα με το άρθρο 40 παράγραφος 6 δεύτερο εδάφιο του κανονισμού (ΕΕ) 2022/2065— με τα οποία έχει αντίρρηση ο πάροχος δεδομένων.

4. Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης και ο πάροχος δεδομένων συμφωνούν σχετικά με τον ορισμό διαμεσολαβητή και δρομολογούν τη διαμεσολάβηση εντός 20 εργάσιμων ημερών από την υποβολή του αιτήματος διαμεσολάβησης σύμφωνα με την παράγραφο 3.

5. Προτού συμφωνήσει για τον διορισμό διαμεσολαβητή, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης επαληθεύει ότι ο διαμεσολαβητής είναι αμερόληπτος και ανεξάρτητος και διαθέτει τη σχετική εμπειρογνωσία που σχετίζεται με το αντικείμενο που περιγράφεται στο γραπτό αίτημα το οποίο αναφέρεται στην παράγραφο 1.

6. Ο πάροχος των δεδομένων αναλαμβάνει όλα τα έξοδα της διαμεσολάβησης.

7. Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης ενημερώνει τον κύριο ερευνητή σχετικά με το αίτημα διαμεσολάβησης που αναφέρεται στην παράγραφο 1 χωρίς αδικαιολόγητη καθυστέρηση και μπορεί να αποφασίσει να καλέσει τον κύριο ερευνητή να λάβει μέρος στη διαμεσολάβηση. Εάν η αίτηση πρόσβασης σε δεδομένα έχει υποβληθεί στον συντονιστή ψηφιακών υπηρεσιών του ερευνητικού οργανισμού, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης μπορεί να καλέσει τον συντονιστή ψηφιακών υπηρεσιών του ερευνητικού οργανισμού να συμμετάσχει στη διαδικασία διαμεσολάβησης. Οποιοδήποτε μέρος που καλείται να συμμετάσχει στη διαμεσολάβηση από τον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης δεν υποχρεούται να συμμετάσχει στη διαδικασία διαμεσολάβησης.

8. Η συμμετοχή σε διαμεσολάβηση δεν θίγει το δικαίωμα των μερών να κινήσουν δικαστική διαδικασία ανά πάσα στιγμή πριν ή μετά τη διαμεσολάβηση ή κατά τη διάρκεια αυτής.

9. Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης ορίζει προθεσμία για τη διαμεσολάβηση, η οποία δεν υπερβαίνει τις 40 εργάσιμες ημέρες από την ημέρα έναρξης της διαμεσολάβησης σύμφωνα με την παράγραφο 4.

10. Ο διαμεσολαβητής μπορεί να τερματίσει τη διαμεσολάβηση νωρίτερα σε μία από τις ακόλουθες περιπτώσεις:

α) όταν ένα από τα μέρη ζητεί ρητά να τερματιστεί η διαμεσολάβηση·

β) όταν καθίσταται σαφές ότι η συμπεριφορά των μερών κατά τη διάρκεια της διαμεσολάβησης, συμπεριλαμβανομένης της μη καλόπιστης συμμετοχής, καθιστά απίθανη την επίτευξη συμφωνίας.

11. Όταν η διαμεσολάβηση καταλήγει σε συμφωνία μεταξύ των μερών, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης λαμβάνει υπόψη την εν λόγω συμφωνία και, κατά περίπτωση, τροποποιεί το αιτιολογημένο αίτημα και ενημερώνει τον κύριο ερευνητή σχετικά με την τροποποίηση.

12. Εάν τα μέρη δεν καταλήξουν σε συμφωνία, ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης ενημερώνει τον πάροχο δεδομένων ότι η απόφαση του συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης σχετικά με το αίτημα τροποποίησης, όπως κοινοποιήθηκε τελευταία σύμφωνα με το άρθρο 40 παράγραφος 6 δεύτερο εδάφιο του κανονισμού (ΕΕ) 2022/2065, θεωρείται έγκυρη και χρησιμεύει ως η σχετική βάση για τα περαιτέρω βήματα της διαδικασίας, και ενημερώνει επίσης τον κύριο ερευνητή.

13. Ο συντονιστής ψηφιακών υπηρεσιών της χώρας εγκατάστασης καταχωρίζει στο σύστημα AGORA συνοπτικό πρακτικό της διαμεσολάβησης, το οποίο καταρτίζει ο διαμεσολαβητής και υπογράφουν όλα τα μέρη. Το πρακτικό περιλαμβάνει τις εξής πληροφορίες:

α) την ημερομηνία του γραπτού αιτήματος διαμεσολάβησης που υπέβαλε ο πάροχος δεδομένων·

β) τα στοιχεία ταυτότητας και τα στοιχεία επικοινωνίας των μερών·

γ) τις ημερομηνίες έναρξης και λήξης της διαμεσολάβησης·

δ) το αποτέλεσμα της διαμεσολάβησης, συμπεριλαμβανομένης/-ου τυχόν συμφωνίας που επιτεύχθηκε ή του λόγου για τον οποίο τερματίστηκε η διαμεσολάβηση.

Άρθρο 14

Διαβούλευση με ανεξάρτητους εμπειρογνώμονες

1. Πριν από τη διατύπωση αιτιολογημένου αιτήματος ή τη λήψη απόφασης σχετικά με αίτημα τροποποίησης, ο συντονιστής ψηφιακών υπηρεσιών μπορεί να αποφασίσει να ζητήσει τη γνώμη εμπειρογνωμόνων.

2. Οι εμπειρογνώμονες είναι ανεξάρτητοι και αμερόληπτοι, έχουν σχετική εμπειρογνωσία και αποδεδειγμένες δεξιότητες, και διαθέτουν την ικανότητα και τους πόρους για την εκτέλεση των προσδιοριζόμενων καθηκόντων χωρίς αδικαιολόγητη καθυστέρηση.

3. Για να πιστοποιήσουν την αμεροληψία τους, οι εμπειρογνώμονες υπογράφουν δήλωση με την οποία βεβαιώνουν ότι:

α) δεν έχουν οικονομικούς ή προσωπικούς δεσμούς με τον πάροχο δεδομένων ή με τους αιτούντες ερευνητές·

β) δεν έχουν συμφέροντα συνδεόμενα με το αποτέλεσμα της διαδικασίας πρόσβασης σε δεδομένα·

γ) δεν εμπλέκονται σε συγκρούσεις συμφερόντων.

4. Ο συντονιστής ψηφιακών υπηρεσιών κωδικοποιεί στο σύστημα AGORA, χωρίς αδικαιολόγητη καθυστέρηση, κάθε διαβούλευση που διενεργείται σύμφωνα με την παράγραφο 1, μαζί με τη γνωμοδότηση των εμπειρογνωμόνων που λαμβάνεται ως απάντηση στη διαβούλευση.

ΚΕΦΑΛΑΙΟ IV

ΠΡΟΫΠΟΘΕΣΕΙΣ ΓΙΑ ΤΗΝ ΠΑΡΟΧΗ ΤΩΝ ΖΗΤΟΥΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΔΙΑΠΙΣΤΕΥΜΕΝΟΥΣ ΕΡΕΥΝΗΤΕΣ

Άρθρο 15

Κοινοποίηση δεδομένων και τεκμηρίωση δεδομένων

1. Οι πάροχοι δεδομένων ενημερώνουν τον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης εντός τριών εργάσιμων ημερών ότι:

α) η πρόσβαση στα ζητούμενα δεδομένα έχει παρασχεθεί στους διαπιστευμένους ερευνητές, σύμφωνα με το αιτιολογημένο αίτημα·

β) η πρόσβαση των διαπιστευμένων ερευνητών έχει διακοπεί.

2. Οι πάροχοι δεδομένων παρέχουν στους διαπιστευμένους ερευνητές κάθε πρόσθετη πληροφορία που απαιτείται για την πρόσβαση στα ζητούμενα δεδομένα και την κατανόηση των δεδομένων αυτών, όπως εγχειρίδια κωδικοποίησης δεδομένων, κατάλογοι αλλαγών και τεκμηρίωση της υποδομής δεδομένων. Σε περιπτώσεις στις οποίες η παροχή των εν λόγω πληροφοριών μπορεί να προκαλέσει σημαντική ευπάθεια στις υπηρεσίες του παρόχου δεδομένων, ο πάροχος δεδομένων ενημερώνει τον συντονιστή ψηφιακών υπηρεσιών της χώρας εγκατάστασης σχετικά τον εν λόγω κίνδυνο και, όπου είναι δυνατόν, προτείνει εναλλακτικές πληροφορίες.

3. Κατά την παροχή πρόσβασης σε δεδομένα, οι πάροχοι δεδομένων δεν επιβάλλουν σε διαπιστευμένους ερευνητές απαιτήσεις διαχείρισης δεδομένων, όπως απαιτήσεις αρχειοθέτησης, αποθήκευσης, ανανέωσης και διαγραφής, ούτε περιορισμούς στη χρήση τυποποιημένων εργαλείων ανάλυσης που ενδέχεται να παρεμποδίζουν την εκτέλεση της σχετικής έρευνας, εκτός εάν οι εν λόγω απαιτήσεις ή περιορισμοί αναφέρονται ρητά στο αιτιολογημένο αίτημα.

4. Κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι πάροχοι δεδομένων δεν επιβάλλουν στους διαπιστευμένους ερευνητές άλλες προϋποθέσεις σε σχέση με την επεξεργασία των κοινοποιούμενων δεδομένων προσωπικού χαρακτήρα πέραν εκείνων που καθορίζονται στο αιτιολογημένο αίτημα.

ΚΕΦΑΛΑΙΟ V

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 16

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.

Βρυξέλλες, 1η Ιουλίου 2025.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ

Αρμοδιότητες της Επιτροπής ως εκτελούσας την επεξεργασία για δραστηριότητες επεξεργασίας δεδομένων που πραγματοποιούνται στο πλαίσιο της πύλης πρόσβασης σε δεδομένα βάσει της DSA

1. Η Επιτροπή δημιουργεί και διασφαλίζει ασφαλή και αξιόπιστη υποδομή ΤΠ, την πύλη πρόσβασης σε δεδομένα βάσει της DSA, για λογαριασμό των συντονιστών ψηφιακών υπηρεσιών, με την οποία υποστηρίζεται και εξορθολογίζεται η διαχείριση της διαδικασίας πρόσβασης σε δεδομένα για ερευνητές, ερευνητικούς οργανισμούς, παρόχους δεδομένων και συντονιστές ψηφιακών υπηρεσιών.

2. Για την εκπλήρωση των υποχρεώσεών της ως εκτελούσας την επεξεργασία για τους συντονιστές ψηφιακών υπηρεσιών, η Επιτροπή μπορεί να χρησιμοποιεί τρίτα μέρη ως υπεργολάβους επεξεργασίας. Σε αυτήν την περίπτωση, οι υπεύθυνοι επεξεργασίας εξουσιοδοτούν την Επιτροπή να χρησιμοποιεί υπεργολάβους επεξεργασίας ή να αντικαθιστά τους υπεργολάβους επεξεργασίας, εφόσον απαιτείται. Η Επιτροπή ενημερώνει τους υπευθύνους επεξεργασίας σχετικά με την εν λόγω χρήση ή αντικατάσταση των υπεργολάβων επεξεργασίας, παρέχοντας έτσι στους υπευθύνους επεξεργασίας τη δυνατότητα να αντιταχθούν σε αυτές τις αλλαγές. Η Επιτροπή μεριμνά ώστε να ισχύουν για τους εν λόγω υπεργολάβους επεξεργασίας οι ίδιες υποχρεώσεις προστασίας δεδομένων που ορίζονται στον παρόντα κανονισμό.

3. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από την Επιτροπή πραγματοποιείται μόνο στον βαθμό που είναι αναγκαίο για:

   α) την επαλήθευση της ταυτότητας και τον έλεγχο της πρόσβασης ως προς όλους τους χρήστες της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

   β) την έγκριση της υλοποίησης αιτημάτων από χρήστες της πύλης πρόσβασης σε δεδομένα βάσει της DSA για τη δημιουργία, την επικαιροποίηση και τη διαγραφή τυχόν πληροφοριών που περιλαμβάνονται στην αίτηση εντός της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

   γ) τη λήψη των δεδομένων προσωπικού χαρακτήρα που αναφέρονται στο άρθρο 5 παράγραφος 3 του παρόντος κανονισμού τα οποία αναφορτώνονται από τους χρήστες της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

   δ) την αποθήκευση δεδομένων προσωπικού χαρακτήρα στην πύλη πρόσβασης σε δεδομένα βάσει της DSA·

   ε) τη διαγραφή των δεδομένων προσωπικού χαρακτήρα κατά την ημερομηνία λήξης τους ή κατόπιν εντολής του υπευθύνου επεξεργασίας·

   στ) μετά το πέρας της παροχής υπηρεσιών που παρέχονται από την πύλη πρόσβασης σε δεδομένα βάσει της DSA, τη διαγραφή τυχόν υπόλοιπων δεδομένων προσωπικού χαρακτήρα, εκτός εάν το δίκαιο της Ένωσης ή των κρατών μελών απαιτεί την αποθήκευση των εν λόγω δεδομένων προσωπικού χαρακτήρα.

4. Η Επιτροπή λαμβάνει όλα τα οργανωτικά, φυσικά και λογικά μέτρα ασφαλείας προηγμένης τεχνολογίας για τη διασφάλιση της λειτουργίας της πύλης πρόσβασης σε δεδομένα βάσει της DSA. Για τον σκοπό αυτόν, η Επιτροπή:

   α) ορίζει μια υπεύθυνη οντότητα για τη διαχείριση της ασφάλειας της πύλης πρόσβασης σε δεδομένα βάσει της DSA, κοινοποιεί στους υπευθύνους επεξεργασίας τα στοιχεία επικοινωνίας μ' αυτήν και εξασφαλίζει ότι η οντότητα αυτή θα είναι διαθέσιμη να αντιδρά σε απειλές κατά της ασφάλειας·

   β) αναλαμβάνει την ευθύνη για την ασφάλεια της πύλης πρόσβασης σε δεδομένα βάσει της DSA, συμπεριλαμβανομένης της τακτικής διενέργειας δοκιμών, αξιολογήσεων και εκτιμήσεων των μέτρων ασφάλειας.

5. Η Επιτροπή λαμβάνει όλα τα αναγκαία μέτρα ασφάλειας ώστε να αποφεύγεται η διασάλευση της ομαλής λειτουργίας της πύλης πρόσβασης σε δεδομένα βάσει της DSA. Στα μέτρα αυτά περιλαμβάνονται:

   α) διαδικασίες αξιολόγησης κινδύνων για τον εντοπισμό και την εκτίμηση πιθανών απειλών κατά της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

   β) διαδικασία ελέγχου και επιθεώρησης με σκοπό:

      i. να ελέγχεται η αντιστοιχία μεταξύ των εφαρμοζόμενων μέτρων ασφάλειας και της πολιτικής ασφάλειας που ακολουθείται·

      ii. να ελέγχονται σε τακτική βάση η ακεραιότητα της πύλης πρόσβασης σε δεδομένα βάσει της DSA, οι παράμετροι ασφαλείας και οι χορηγούμενες άδειες·

      iii. να εντοπίζονται παραβιάσεις της ασφάλειας και εισβολές στην πύλη πρόσβασης σε δεδομένα βάσει της DSA·

iv. να πραγματοποιούνται αλλαγές για τον περιορισμό των υφιστάμενων αδυναμιών στον τομέα της ασφάλειας της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

v. να ορίζονται οι προϋποθέσεις υπό τις οποίες επιτρέπεται η διενέργεια, μεταξύ άλλων κατόπιν αιτήματος των υπευθύνων επεξεργασίας, και η συμβολή στη διενέργεια ανεξάρτητων ελέγχων, συμπεριλαμβανομένων επιθεωρήσεων και αξιολογήσεων των μέτρων ασφαλείας, με την επιφύλαξη προϋποθέσεων που τηρούν το πρωτόκολλο (αριθ. 7) της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης περί των προνομίων και ασυλιών της Ευρωπαϊκής Ένωσης·

γ) αλλαγή της διαδικασίας ελέγχου για την τεκμηρίωση, τη μέτρηση του αντικτύπου μιας αλλαγής πριν από την υλοποίησή της και την ενημέρωση των υπευθύνων επεξεργασίας σχετικά με τυχόν αλλαγές που μπορούν να επηρεάσουν την επικοινωνία με την πύλη πρόσβασης σε δεδομένα βάσει της DSA και/ή την ασφάλεια της πύλης αυτής·

δ) πρόβλεψη διαδικασίας συντήρησης και επισκευής για τον καθορισμό των κανόνων και των προϋποθέσεων που πρέπει να τηρούνται κατά τη συντήρηση και/ή την επισκευή της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

ε) πρόβλεψη διαδικασίας για τα συμβάντα που θέτουν σε κίνδυνο την ασφάλεια με σκοπό τον καθορισμό του συστήματος αναφοράς και κλιμάκωσης, τη χωρίς καθυστέρηση ενημέρωση των υπευθύνων επεξεργασίας που επηρεάζονται, τη χωρίς καθυστέρηση ενημέρωση των υπευθύνων επεξεργασίας προκειμένου με τη σειρά τους να ενημερώσουν τις εθνικές εποπτικές αρχές προστασίας δεδομένων σχετικά με τυχόν παραβίαση δεδομένων προσωπικού χαρακτήρα, και τον καθορισμό πειθαρχικής διαδικασίας για την αντιμετώπιση των παραβιάσεων της ασφάλειας στην πύλη πρόσβασης σε δεδομένα βάσει της DSA.

6. Η Επιτροπή λαμβάνει μέτρα φυσικής και λογικής ασφάλειας προηγμένης τεχνολογίας για τις εγκαταστάσεις που φιλοξενούν την πύλη πρόσβασης σε δεδομένα βάσει της DSA και για τους ελέγχους των δεδομένων και της πρόσβασης ασφαλείας σε αυτά. Για τον σκοπό αυτόν, η Επιτροπή:

α) επιβάλλει φυσική ασφάλεια για να καθιερώσει διακριτές περιμέτρους ασφαλείας και να καταστήσει εφικτό τον εντοπισμό παραβιάσεων στην πύλη πρόσβασης σε δεδομένα βάσει της DSA·

β) ελέγχει την πρόσβαση στις εγκαταστάσεις της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

γ) διασφαλίζει ότι δεν μπορεί να προστεθεί, να αντικατασταθεί ή να αφαιρεθεί εξοπλισμός χωρίς προηγούμενη έγκριση των οριισθέντων αρμόδιων φορέων·

δ) ελέγχει την πρόσβαση από και προς την πύλη πρόσβασης σε δεδομένα βάσει της DSA·

ε) διασφαλίζει την επαλήθευση της ταυτότητας των χρηστών της πύλης πρόσβασης σε δεδομένα βάσει της DSA οι οποίοι αποκτούν πρόσβαση στην εν λόγω πύλη·

στ) ελέγχει τα δικαιώματα εξουσιοδότησης όσον αφορά την πρόσβαση στην πύλη πρόσβασης σε δεδομένα βάσει της DSA σε περίπτωση παραβίασης της ασφάλειας που επηρεάζει την εν λόγω πύλη·

ζ) τηρεί την ακεραιότητα των πληροφοριών που διαβιβάζονται μέσω της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

η) εφαρμόζει τεχνικά και οργανωτικά μέτρα ασφαλείας για την πρόληψη μη εξουσιοδοτημένης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα στην πύλη πρόσβασης σε δεδομένα βάσει της DSA·

θ) εφαρμόζει, όποτε κρίνεται σκόπιμο, μέτρα για την παρεμπόδιση της μη εξουσιοδοτημένης πρόσβασης στην πύλη πρόσβασης σε δεδομένα βάσει της DSA (δηλαδή αποκλεισμός τοποθεσίας/διεύθυνσης IP).

7. Η Επιτροπή:

α) λαμβάνει μέτρα για την προστασία του τομέα της, συμπεριλαμβανομένης της αποκοπής συνδέσεων, σε περίπτωση σημαντικής απόκλισης από τις αρχές και τις έννοιες της ποιότητας και της ασφάλειας·

β) διατηρεί σχέδιο διαχείρισης κινδύνου που αφορά τον τομέα αρμοδιότητάς της·

γ) παρακολουθεί σε πραγματικό χρόνο την απόδοση όλων των στοιχείων των υπηρεσιών της πύλης πρόσβασης σε δεδομένα βάσει της DSA, εκπονεί τακτικές στατιστικές και τηρεί αρχεία·

δ) παρέχει υποστήριξη για την πύλη πρόσβασης σε δεδομένα βάσει της DSA στα αγγλικά στους χρήστες της εν λόγω πύλης·

ε) παρέχει συνδρομή στους υπευθύνους επεξεργασίας με κατάλληλα τεχνικά και οργανωτικά μέτρα για την εκπλήρωση της υποχρέωσης του υπευθύνου επεξεργασίας να απαντά σε αιτήματα για άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων που προβλέπονται στο κεφάλαιο III του κανονισμού (ΕΕ) 2016/679·

στ) υποστηρίζει τους υπευθύνους επεξεργασίας παρέχοντας πληροφορίες σχετικά με την πύλη πρόσβασης σε δεδομένα βάσει της DSA με σκοπό την εκπλήρωση των υποχρεώσεων σύμφωνα με τα άρθρα 32, 33, 34, 35 και 36 του κανονισμού (ΕΕ) 2016/679·

ζ) διασφαλίζει ότι τα δεδομένα που υποβάλλονται σε επεξεργασία στο πλαίσιο της πύλης πρόσβασης σε δεδομένα βάσει της DSA είναι ακατάληπτα για τα πρόσωπα που δεν επιτρέπεται να έχουν πρόσβαση σ' αυτή·

η) λαμβάνει όλα τα σχετικά μέτρα για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται μέσω της πύλης πρόσβασης σε δεδομένα βάσει της DSA·

θ) λαμβάνει μέτρα για να διευκολύνει την επικοινωνία μεταξύ των υπευθύνων επεξεργασίας·

ι) τηρεί αρχείο των δραστηριοτήτων επεξεργασίας που διεξάγονται για λογαριασμό των υπευθύνων επεξεργασίας, σύμφωνα με το άρθρο 31 παράγραφος 2 του κανονισμού (ΕΕ) 2018/1725.

Official Journal
of the European Union

EN
L series

2025/2050

9.10.2025

COMMISSION DELEGATED REGULATION (EU) 2025/2050

of 1 July 2025

supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC ([1]), and in particular Article 40(13) thereof,

Whereas:

(1) Article 40 of Regulation (EU) 2022/2065 lays down rules regarding access to data to be granted by providers of very large online platforms and of very large online search engines. In particular, it enables researchers who have completed a process to demonstrate that they fulfil the conditions laid down in paragraph 8 of that Article ('vetted researchers') to be provided with such access.

(2) Under Article 40(4) of Regulation (EU) 2022/2065, vetted researchers are to be provided with access to data to help them study systemic risks in the Union and assess the effectiveness of measures to mitigate those risks. Their findings can constitute valuable input for the enforcement of Regulation (EU) 2022/2065 and foster accountability of providers of very large online platforms and of very large online search engines. The purpose of this Regulation is to lay down the technical conditions and the procedures necessary to enable such access, in a secure and efficient manner that is consistent across all Digital Services Coordinators, and in a way that ensures equality of treatment for researchers and data providers.

(3) To ensure that the data access process is consistent across all Digital Services Coordinators and to make that process clear and transparent for everyone, it is necessary to create a dedicated digital infrastructure ('the DSA data access portal'). The DSA data access portal should allow researchers, data providers, and Digital Services Coordinators to participate in the data access process, have access to and disseminate relevant information, such as the details of the dedicated points of contact, and communicate with one another. The DSA data access portal should not be considered as one of the access modalities to be used for the provision of access to the data pursuant to a reasoned request.

(4) Data providers, and researchers wishing to participate in the data access process, should create an account on the DSA data access portal for that purpose. To ensure that Digital Services Coordinators can access information submitted via the DSA data access portal without needing to create a separate account on the portal, the DSA data access portal should be interoperable with the information sharing system AGORA established in Commission Implementing Regulation (EU) 2024/607 ([2]).

(5) To ensure transparency of the data access process for all the parties involved and to monitor the effectiveness and efficiency of the data access process and compliance with Article 40(4) of Regulation (EU) 2022/2065 and this Regulation, the DSA data access portal should generate automatic notifications in relation to different steps and updates of the process.

([1]) OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

([2]) Commission Implementing Regulation (EU) 2024/607 of 15 February 2024 on the practical and operational arrangements for the functioning of the information sharing system pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act) (OJ L, 2024/607, 16.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/607/oj).

(6) In order to provide researchers with consistent information about the data access process, Digital Services Coordinators should make available and easily accessible on their online interfaces information concerning the data access process, including links to the DSA data access portal. To avoid creating unnecessary administrative burden, increase efficiency and facilitate communication among all parties involved in the data access process, Digital Services Coordinators are encouraged to facilitate the management of information related to the data access process, also from a linguistic perspective.

(7) In order to allow researchers to identify the relevant data for the purposes set out in Article 40(4) of Regulation (EU) 2022/2065, data providers should make available DSA data catalogues for their services. Such catalogues should be easily findable and accessible on the online interfaces of data providers, and should describe the available data assets, their data structure and metadata, access to which may be requested pursuant to Article 40(4) of Regulation (EU) 2022/2065. When making available the DSA data catalogues, data providers should have regard to risks to confidentiality, data security or personal data protection potentially deriving from such information being made public.

(8) To contribute to the development of relevant research projects for the purposes set out in Article 40(4) of Regulation (EU) 2022/2065, the DSA data catalogues should include in particular data related to the systemic risks in the Union that data providers have identified in their annual risk assessments pursuant to Article 34 of that Regulation, as well as data related to any risk mitigation measures referred to in Article 35 of that Regulation. To ensure the relevance and timeliness of the DSA data catalogues, those catalogues should be updated regularly with due consideration to newly identified systemic risks and the evolution of systemic risks. For example, they should reflect emerging risks identified following an ad hoc risk assessment pursuant to Article 34 of Regulation (EU) 2022/2065 or following an audit report pursuant to Article 37 of that Regulation. To minimise the procedural burden on the data providers, where appropriate, such catalogues may rely on existing data documentation resources used for other purposes and audiences, such as advertising, content creation, or third-party app development. The DSA data catalogues should not be required to be exhaustive and therefore should not bind or limit applicant researchers in their data access applications.

(9) In order to facilitate the determination of the access modalities by the Digital Services Coordinator of establishment and reduce the overall burden of the data access process on all actors involved, data providers should publish their suggested access modalities for the data described in the DSA data catalogues. These suggested access modalities should be proportionate to the sensitivity of the data and include information on the possible technical, organisational and legal conditions considered by the data providers as appropriate to enable the provision of the data. The access modalities suggested by data providers should not bind Digital Services Coordinators of establishment, who should remain competent to determine the appropriate access modalities.

(10) To ensure that data access applications are treated equally, independently of the Digital Services Coordinator to which the data access application is submitted or from which the reasoned request originates, the timeframe for the formulation of reasoned requests should be specified to ensure consistency across all Digital Services Coordinators. If the formulation of the reasoned request requires additional time, the Digital Services Coordinator of establishment should notify the principal researcher, giving reasons for the delay. Such reasons may include the need for additional verifications by the Digital Services Coordinator of the research organisation or of establishment, for example where data access applications imply international data transfers, or where the Digital Services Coordinator of establishment has identified potential risks to the security of the Union if the data were to be shared. With a view to aligning also the steps in the data access process preceding the formulation of reasoned requests, including the assessment of data access applications and granting of vetted researcher status, Digital Services Coordinators are encouraged to develop a consistent and coordinated way of working, including common operational criteria, within the framework of the European Board for Digital Services.

(11) In order to streamline the procedures for the formulation of reasoned requests, all Digital Services Coordinators of establishment should be required to verify that certain common elements of the data access process were duly covered in the data access applications. To that end, the Digital Services Coordinators of establishment should verify that all applicant researchers who are mentioned in the data access application demonstrated their affiliation to a research organisation, for example by providing documentary evidence of employment contracts or any other form of legal association with the research organisation. The Digital Services Coordinators of establishment should also verify that the applicant researchers demonstrated their independence from commercial interests, for example, by means of a declaration to that effect.

(12) The Digital Services Coordinator of establishment should verify that the funding of the research project for which the data are requested is disclosed in the data access application. The information provided by the applicant researchers should include details of the contributions, such as the funding entity, the amount, the nature and duration of the contribution, including whether the funding has already been awarded or whether an application for funding is still under evaluation, as well as, where applicable, relevant references to Union funded projects. Where available, the data access application should also include the outcomes of evaluations conducted by the entity or entities providing the funding.

(13) The Digital Services Coordinator of establishment should verify that the data access application describes how the data and data format are selected, with reference to the requirements of necessity for, and proportionality to, the purpose of the envisaged research. Where the requested data are also available through other sources, the Digital Services Coordinator of establishment should assess whether the request for such data in the data access application is duly justified, having regard to the information in the data access application. Possible justifications may include evidence of poor quality or unreliability of such data deriving from other sources or the unsuitability of the format in which such data may be retrieved from other sources for the purposes of the research project, which would hinder the performance of the research project. Data that can be requested in order to study systemic risks or their mitigation in the Union may evolve in the future. Current examples of such data include data related to users of the services, such as profile information, relationship networks, individual-level content exposure and engagement histories; interaction data such as comments or other engagements; data related to content recommendations, including data used to personalise recommendations; data related to the targeting of advertisements and profiling, including cost per click data and other measures of advertising prices; data related to the testing of new features prior to their deployment, including the results of A/B tests; data related to content moderation and governance, such as data on algorithmic or other content moderation systems and processes, including changelogs, archives or repositories documenting moderated content, including accounts as well as data related to prices, quantities and characteristics of goods or services provided or intermediated by the data provider.

(14) The Digital Services Coordinator of establishment should verify whether the data access application provides for sufficient information that demonstrate that the researcher is capable of fulfilling the specific requirements of confidentiality, security and protection of personal data with respect to the requested data, identifies possible risks deriving from accessing and processing of such data for the purposes of the research, and documents any access modalities proposed, including the legal, organisational and technical conditions that will be put in place to minimise identified risks, for instance by means of a commitment letter from the research organisation confirming access to means that can constitute relevant safeguards, or other supporting documents.

(15) Where personal data are requested, the Digital Services Coordinator of establishment should verify that the data access application includes information on the legal basis for the processing of personal data, including special categories of personal data, where applicable, and whether such legal basis is in line with Article 6(1), point (e) or (f), and where applicable Article 9(2), point (g) or (j), of Regulation (EU) 2016/679 of the European Parliament and of the Council ([3]). In addition, the Digital Services Coordinator of establishment should verify that the data access application contains sufficient indication that the researchers have assessed risks to personal data protection. For example, this could be demonstrated by a data protection impact assessment within the meaning of Article 35 of that Regulation. To ensure that personal data can be accessed in compliance with Regulation (EU) 2016/679, Digital Services Coordinators should be allowed to consult the relevant supervisory authorities established pursuant to Article 51 of that Regulation, which remain competent to assess compliance with Regulation (EU) 2016/679.

([3]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(16) To facilitate the formulation of the reasoned request and preserve the integrity of the information included in the data access application the Digital Services Coordinator of establishment should verify whether the data access application includes a summary. Such summary should contain an overview of the information that will be part of the reasoned request, published in the DSA data access portal, in cases where the assessment of the data access application leads to the formulation of a reasoned request.

(17) In order to ensure that the access modalities the Digital Services Coordinator of establishment determines are adequate to address the sensitivity of the specific data requested in a data access application, the Digital Services Coordinator of establishment should perform a case-by-case assessment, based on the information provided in the data access application. The access modalities established in the reasoned request should be appropriate to fulfil the requirements of data security, data confidentiality and protection of personal data and, at the same time, enable the attainment of the research objectives of the research project. Access to data may take place for example through data transmission to the vetted researchers via an appropriate interface and appropriate data storage; transmission of the data to, and storage in, a secure processing environment operated by the data provider or by a third party provider to which vetted researchers have access but where no data transmission to the vetted researchers takes place, or other access modalities to be set up or facilitated by the data provider. When specifying the access modalities, the Digital Services Coordinator of establishment should also list any legal, technical or organisational conditions to which access is to be subject. In cases where providing access involves a transfer of personal data to third countries or international organisations within the meaning of Chapter V of Regulation (EU) 2016/679, the access modalities should also include information on the need to put in place an appropriate transfer mechanism, to ensure that the data provider takes the necessary action to comply with that Regulation.

(18) To ensure that the data access modalities are appropriate to address specific sensitivities in terms of data protection, of data security or of confidentiality, the Digital Services Coordinator of establishment, on the basis of the information received in the data access application, should be able to require, that access to data be provided via secure processing environments. In such cases, the Digital Services Coordinator of establishment should ensure that the chosen environment operates in line with the most appropriate technology and it allows the vetted researchers to attain the objectives of their research.

(19) In order to ensure consistency of the information transmitted by the Digital Services Coordinators of establishment to the data providers, it is necessary to specify the content of the reasoned requests.

(20) In order to safeguard the interests of data providers and to reduce the frequency of amendment requests over time and facilitate the formulation of relevant data access applications by researchers, an overview of each reasoned request, including any amendments and updates to it, should be made publicly available in the DSA data access portal by the Digital Services Coordinator of establishment who issued the respective reasoned requests.

(21) In order to ensure that the Digital Services Coordinator of establishment has the relevant information to evaluate an amendment request and to facilitate a uniform approach in the evaluation of amendment requests, the data provider should be required to specify the reasons for such request, as referred to in Article 40(5) of Regulation (EU) 2022/2065. More specifically, when assessing an amendment request submitted on the basis of a data provider's lack of access to the data, the Digital Service Coordinator of establishment should be in a position to examine whether the alleged impossibility is duly justified, for example by the non-existence of the requested data, or by technical restrictions such as encryption and it should have the information necessary to consider whether the lack of access is permanent or temporary. It should be clear, in this respect, that commercial considerations should not be considered as a ground to automatically refuse access to requested data but rather as a ground to modify the means of providing access to the data, which may result in imposing additional data security and confidentiality requirements.

(22) In order to ensure an efficient resolution of disputes and to encourage the identification of a mutually acceptable solution, following an amendment request, data providers should be able to ask the Digital Services Coordinators of establishment to participate in mediation. Such participation should be voluntary throughout the entire mediation process and should not result in any binding outcome for the Digital Services Coordinator of establishment, which remain competent to decide on the amendment requests. All parties involved in the mediation process should engage in good faith and strive to reach a fair and mutually acceptable agreement.

(23) In order to prevent that mediation indefinitely prolong the data access process, the transmission of the written request for mediation, the selection of the mediator and the mediation process itself should take place within specified timeframes. The Digital Services Coordinators of establishment should set a time limit for the mediation process in relation to a given reasoned request and the mediator should have the authority to terminate the mediation process in specific circumstances.

(24) In order to maintain mutual trust among the parties involved in the mediation, the Digital Services Coordinator of establishment should ensure that the proposed mediator meet the requirements of impartiality, independence and possess relevant expertise on the subject matter of the mediation.

(25) For the purposes of facilitating informed and effective decision-making in relation to the data access process, Digital Services Coordinators should have the possibility to request expert opinions on specific elements of the data access process, such as the determination of the access modalities, including appropriate interfaces, the formulation of the reasoned request and any amendment requests by the data provider. The experts consulted should possess proven expertise in the matter on which their opinion is sought and should be independent. In particular, they should not have any conflict of interests, deriving for example from any ties with the applicant researchers or with the data provider.

(26) In order to increase transparency and allow Digital Services Coordinators to build on their expertise acquired over time, each expert consultation request and the follow-up generated by it should be registered in AGORA.

(27) In order to facilitate the effective supervision of compliance with the conditions set out in the reasoned request, the data provider should notify the Digital Services Coordinator of establishment within three working days of the date on which access has been provided to the vetted researchers and of the date of the access its termination.

(28) In order to enable the vetted researchers to use the requested data for the purposes of the research and to provide relevant context information, data providers should provide vetted researchers with the relevant metadata and documentation describing the data made available, such as codebooks, changelogs and architectural documentation.

(29) In order to facilitate meaningful research by the vetted researchers, also by enabling the combination of the data requested with data available through other sources, data providers should not impose any restrictions on the analytical tools employed by vetted researchers, including relevant software libraries, and should not impose archiving, storage, refresh and deletion requirements, unless they are explicitly mentioned in the access modalities identified in the reasoned request.

(30) Where the data provided to the vetted researchers include personal data within the meaning of Article 4 of Regulation (EU) 2016/679, the data provider should observe the rules laid down in that Regulation. In particular, Article 40(4) of Regulation (EU) 2022/2065 creates a legal obligation within the meaning of Article 6(1), point (c) of Regulation (EU) 2016/679 for any processing of personal data necessary for the data provider to provide access to the data specified in the reasoned request. Where special categories of personal data within the meaning of Article 9 of Regulation (EU) 2016/679 are to be processed, this Regulation meets the requirement of Article 9(2), point (g) of Regulation (EU) 2016/679.

(31) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([4]) and delivered an opinion on 4 December 2024.

(32) After consulting the European Board for Digital Services in accordance with Article 40(13) of Regulation (EU) 2022/2065 and following its endorsement,

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

This Regulation lays down procedures and technical conditions for providing vetted researchers with access to data held by providers of very large online platforms and of very large online search engines, pursuant to Article 40(4) of Regulation (EU) 2022/2065, in particular:

(a) the technical conditions for the development and functioning of a data access portal;

(b) the procedures and technical conditions for the management of the data access process by Digital Services Coordinators and data providers;

(c) the requirements for the formulation of reasoned requests and the assessment of amendment requests;

(d) the technical conditions for the provision of access to data by the data providers.

Article 2

Definitions

For the purposes of this Regulation, the definitions in Article 4 of Regulation (EU) 2016/679 and Article 3 of Regulation (EU) 2018/1725 shall apply. The following definitions shall also apply:

(1) 'data access application' means the information and relevant documentation submitted by applicant researchers to the Digital Services Coordinator of establishment or the Digital Services Coordinator of the Member State of the research organisation, to which the principal researcher is affiliated, to obtain the status of 'vetted researcher' as referred to in Article 40(8), first subparagraph, of Regulation (EU) 2022/2065, for a specific research project involving access to data from a data provider;

(2) 'data access process' means the steps and procedures that may lead to the provision of access to the data as referred to in Article 40(4) of Regulation (EU) 2022/2065;

(3) 'applicant researcher' means any natural person applying for access to data as referred to in Article 40(4) of Regulation (EU) 2022/2065, either individually, in a group or as part of an entity;

(4) 'principal researcher' means the applicant researcher who submits the data access application in their individual capacity or on behalf of an entity or a group of applicant researchers;

(5) 'data provider' means a provider of a very large online platform or of a very large online search engine designated as such in accordance with Article 33(4) of Regulation (EU) 2022/2065, to which a reasoned request might be addressed;

([4]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(6) 'reasoned request' means a reasoned request for data access pursuant to Article 40(4) of Regulation (EU) 2022/2065;

(7) 'amendment request' means a request for amendment pursuant to Article 40(5) of Regulation (EU) 2022/2065 submitted by the data provider to the Digital Services Coordinator of establishment following the receipt of a reasoned request;

(8) 'secure processing environment' means secure processing environment as defined in Article 2, point (20), of Regulation (EU) 2022/868 of the European Parliament and of the Council ([5]).

CHAPTER II

INFORMATION AND CONTACT OBLIGATIONS

Article 3

DSA data access portal

1. The Commission shall establish and host a DSA data access portal.

2. The DSA data access portal shall have the following functions:

(a) support and streamline the management of the data access process for researchers, data providers and Digital Services Coordinators;

(b) serve as the central digital point for information on the data access process and facilitate the information exchanges pursuant to this Regulation among applicant researchers, vetted researchers, data providers and Digital Services Coordinators.

3. The DSA data access portal shall be interoperable with the information sharing system AGORA established by Implementing Regulation (EU) 2024/607. The Digital Services Coordinators shall have access in AGORA to the information submitted through the DSA data access portal.

4. Data providers shall have an account on the DSA data access portal.

5. To participate in the data access process, applicant researchers shall have an account on the DSA data access portal.

Article 4

Roles and responsibilities for processing personal data in the DSA data access portal

1. Digital Services Coordinators shall be separate controllers with respect to the processing of personal data they carry out to manage the data access process and for publication of relevant information.

2. The Commission shall be a processor of personal data processed within the DSA data access portal.

3. The responsibilities of the Commission as processor for data processing activities conducted in the DSA data access portal shall be as set out in the Annex.

([5]) Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

Article 5

Processing of personal data in the DSA data access portal

1. Where personal data are registered in and exchanged via the DSA data access portal, the processing shall take place only in so far as it is proportionate and necessary for the purpose of the data access process and publication of relevant information.

2. The processing of personal data shall take place in the DSA data access portal only in respect of the following categories of data subjects:

(a) natural persons having an account on the DSA data access portal;

(b) natural persons whose personal data is contained in the DSA data access portal or in any other exchange pursuant to this Regulation concerning the data access process.

3. The processing of personal data shall take place in the DSA data access portal only in respect of the following categories of personal data:

(a) identity data, such as name, user ID;

(b) contact information such as address, email address, contact details;

(c) personal data contained in the documentation demonstrating the affiliation to a research organisation, and any other personal information deemed necessary for the purpose of participating in the data access process.

4. The processing of personal data referred to in paragraph 1 shall be performed using information technology infrastructure located in the European Economic Area.

Article 6

Points of contact and public information on the data access process

1. Each Digital Services Coordinator and each data provider shall establish a dedicated point of contact, whose task shall be to provide information and support on the data access process.

2. The Digital Services Coordinators and data providers shall communicate their points of contact to the Commission, as soon as possible. The Commission shall publish the details of the points of contact referred to in paragraph 1 in the public interface of the DSA data access portal.

3. Each Digital Services Coordinator shall make available and easily findable on its online interface, the details of the point of contact established pursuant to paragraph 1 together with a link to the DSA data access portal.

4. Data providers shall make the following information available and easily findable on their online interfaces:

(a) the details of the point of contact established by them pursuant to paragraph 1;

(b) a link to the DSA data access portal;

(c) a DSA data catalogue, which describes the data assets, that may be accessed for the purposes set out in Article 40(4) of Regulation EU 2022/2065, as well as their data structure and metadata;

(d) suggested access modalities for the data in the catalogue pursuant to point (c), adequate to the level of sensitivity of the different data assets.

5. The information referred to in paragraph 4, points (c) and (d), shall be regularly updated, in particular to reflect data related to the risk assessments carried out pursuant to Article 34 of Regulation (EU) 2022/2065 and the audits carried out pursuant to Article 37 of that Regulation.

CHAPTER III

REQUIREMENTS FOR FORMULATING AND PROCESSING OF REASONED REQUESTS

Article 7

Formulation of reasoned request

1. Within 80 working days from the submission of a data access application, the Digital Services Coordinator of establishment, taking due account of the prerequisites set out in Article 8 and, where applicable, any other assessment relevant for these purposes, shall decide whether a reasoned request can be formulated and shall undertake one of the following actions:

(a) formulate a reasoned request, submit it to the data provider and notify the principal researcher of the submission of the reasoned request;

(b) inform the principal researcher of the reasons why the reasoned request could not be formulated.

2. Where, in duly justified cases, the Digital Services Coordinator of establishment needs additional time to formulate a reasoned request, it shall notify the principal researcher as soon as possible and shall indicate the reasons for the delay as well as a new date for undertaking the actions referred to in paragraph 1.

Article 8

Prerequisites for formulating a reasoned request

The Digital Services Coordinator of establishment shall decide whether a reasoned request can be formulated taking into account the following elements:

(a) for each applicant researcher:

  (i) a confirmation of affiliation to a research organisation as defined in Article 2, point (1), of Directive (EU) 2019/790 of the European Parliament and of the Council ([6]);

  (ii) a declaration of independence from commercial interests relevant to the specific project for which the data are requested;

  (iii) a commitment to making their research results publicly available free of charge;

(b) information about funding supporting the research project for which the data are requested;

(c) a description of the data requested, including format, scope and, where possible, the specific attributes, relevant metadata and data documentation, also considering the information made available pursuant to Article 6(4) of this Regulation;

(d) information on the necessity and proportionality of the access to the data and the information on the time frames of the research for which the data are requested;

(e) information on the identified risks in terms of confidentiality, data security and personal data protection related to the data that would be accessed, a description of the technical, legal and organisational measures that will be put in place, including, where possible, suggested access modalities, to mitigate such risks when processing the requested data;

(f) a description of the research activities to be conducted with the requested data;

(g) a summary of the data access application containing the following elements:

  (i) the research topic;

  (ii) the data provider from which data are requested;

  (iii) a description of the data requested, as referred to in point (c).

([6]) Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92, ELI: http://data.europa.eu/eli/dir/2019/790/oj).

Article 9

Access modalities

1. The Digital Services Coordinator of establishment shall determine the modalities, including the technical, legal and organisational measures, that the data provider is to use for providing access to the data to the vetted researchers.

2. The Digital Services Coordinators shall be allowed to consult the relevant supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679.

3. When determining the access modalities, the Digital Services Coordinator of establishment shall take into account the information provided in the data access application, in particular the information referred to in Article 8, point (e), considering also the rights and interests of the data providers and the recipients of the service concerned, including the protection of confidential information, trade secrets, and maintaining the security of their service and the information made available by the data providers pursuant to Article 6(4), point (d).

4. In addition to the elements referred to in paragraph 3, the Digital Services Coordinator of establishment shall, when determining access modalities, take into account the following elements:

(a) where the access involves the processing of personal data:

  (i) the assessment of the risks concerning processing of personal data as described in Article 8(e), including, where applicable, data protection impact assessments within the meaning of Article 35 of Regulation (EU) 2016/679;

  (ii) envisaged technical and organisational measures as submitted pursuant to Article 8(e);

(b) relevant network security measures, encryption, access control mechanisms, backup policies, data integrity mechanisms, incident response plans;

(c) where applicable, information on the intended storage period and the relevant data destruction plans;

(d) any organisational measures such as internal review processes, restrictions of access rights and information sharing;

(e) any proposed contractual clauses, such as non-disclosure agreements, data agreements and any other type of written statements, laying down possible conditions of access and processing between the principal researcher and the data provider;

(f) existence of training on data security and protection of personal data received by the applicant researchers;

(g) whether secure processing environments is necessary to process the data.

5. Where the Digital Services Coordinator of establishment considers that a secure processing environment is to be used to provide access to the data requested, the Digital Services Coordinator of establishment shall require documentation attesting that the operator of that environment:

(a) specifies access conditions to the secure processing environment in order to minimise the risk of the unauthorised reading, copying, modification or removal of the data hosted in the secure processing environment;

(b) ensures that vetted researchers have access only to data covered by the reasoned request, by means of individual and unique user identities and confidential access modes;

(c) keeps identifiable logs of access to the secure processing environment for the period necessary to verify and audit all processing operations in that environment;

(d) ensures that the computing power at the disposal of the vetted researchers is appropriate and sufficient for the purposes of the research project;

(e) monitors the effectiveness of the measures listed in points (a) to (d).

Article 10

Content of a reasoned request

1. A reasoned request shall contain at least the following elements:

(a) the date by which the data provider shall give access to the data requested and the date on which such access shall be terminated;

(b) the access modalities determined pursuant to Article 9;

(c) the summary of the data access application referred to in Article 8 point (g).

2. The Digital Services Coordinator of establishment may include in the reasoned request the names and contact details of all vetted researchers mentioned in the data access application where this is necessary to enable access to the requested data, in accordance with the access modalities specified in the reasoned request.

3. If providing access involves a transfer of personal data to a third country or international organisation within the meaning of Chapter V of Regulation (EU) 2016/679, the reasoned request shall include information on the need to put in place or refer to an appropriate transfer mechanism to ensure compliance with Regulation (EU) 2016/679.

Article 11

Publication of an overview of a reasoned request in the DSA data access portal

1. Upon formulation of a reasoned request, the Digital Services Coordinator of establishment shall publish an overview of the reasoned request in the public interface of the DSA data access portal. The overview shall contain all the following:

(a) the summary of the data access application referred to in Article 8 point (g);

(b) the access modalities determined pursuant to Article 9.

2. The overview referred to in paragraph 1 shall be updated to reflect any changes resulting from a modification of one or more elements following the examination of an amendment request or the outcome of a mediation in accordance with Article 13.

Article 12

Procedures for examining amendment requests

1. Upon the receipt of an amendment request pursuant to Article 40(5) of Regulation (EU) 2022/2065, the Digital Services Coordinator of establishment shall inform the principal researcher concerned.

2. When deciding on an amendment request made pursuant to Article 40(5), point (a), of Regulation (EU) 2022/2065, the Digital Services Coordinator of establishment shall take into account the following:

(a) whether the reasons for the alleged lack of access to data are duly substantiated;

(b) whether that lack of access to data is permanent or temporary.

3. When deciding on an amendment request made pursuant to Article 40(5), point (b), of Regulation (EU) 2022/2065, the Digital Services Coordinator of establishment shall take into account all the following:

(a) whether the alleged vulnerabilities and their significance are duly substantiated;

(b) the likelihood and severity of harm resulting from these alleged significant vulnerabilities;

(c) the extent to which the access modalities set out in the reasoned request effectively mitigate the risk of such harm occurring.

4. At any time during the assessment of an amendment request, the Digital Services Coordinator of establishment may ask the data provider or the principal researcher for any additional information that it considers necessary to complete its assessment.

5. Such request for additional information shall be made as soon as possible to allow the data provider or the principal researcher sufficient time to respond and, in any event, shall not affect the deadline set in Article 40(6), second subparagraph of Regulation (EU) 2022/2065. Where the data provider or the principal researcher fails to provide the requested information at all or within a period specified by the Digital Services Coordinator of establishment or provides partial information, the Digital Services Coordinator of establishment shall make its decision within the timeframe laid down in Article 40(6) of Regulation (EU) 2022/2065, based on the information that was made available to it within a reasonable delay.

Article 13

Mediation

1. If the data provider disagrees with the decision of the Digital Services Coordinator of establishment on the amendment request, the data provider may, within a period of five working days from the communication by the Digital Services Coordinator of establishment pursuant to Article 40(6), second subparagraph of Regulation (EU) 2022/2065, request in writing the Digital Services Coordinator of establishment to participate in mediation.

2. The Digital Services Coordinator of establishment shall not be obliged to participate in the mediation process.

3. The written request referred to in paragraph 1, shall include a concise description of the specific elements of the decision, as communicated by the Digital Services Coordinator of establishment pursuant to Article 40(6), second subparagraph of Regulation (EU) 2022/2065, to which the data provider objects.

4. The Digital Services Coordinator of establishment and the data provider shall agree on the appointment of a mediator and initiate the mediation within 20 working days from the submission of the mediation request pursuant to paragraph 3.

5. Before agreeing to the appointment of a mediator, the Digital Services Coordinator of establishment shall verify that the mediator is impartial and independent and possesses the relevant expertise related to the subject matter as described in the written request referred to in paragraph 1.

6. The data provider shall bear all costs of the mediation.

7. The Digital Services Coordinator of establishment shall inform the principal researcher of the mediation request referred to in paragraph 1 without undue delay and may decide to invite the principal researcher to join the mediation as a party. Where the data access application has been submitted to the Digital Services Coordinator of the research organisation, the Digital Services Coordinator of establishment may invite the Digital Services Coordinator of the research organisation to participate in the mediation process. Any party invited to join the mediation by the Digital Services Coordinator of establishment shall not be obliged to participate in the mediation process.

8. Participation in mediation shall not affect the right of the parties to initiate judicial proceedings at any time before, during or after the mediation.

9. The Digital Services Coordinator of establishment shall set a time limit for the mediation, which shall not exceed 40 working days starting on the day of the initiation of the mediation pursuant to paragraph 4.

10. The mediator may terminate the mediation earlier in one of the following cases:

(a) one of the parties requests explicitly to terminate the mediation;

(b) it becomes clear that the conduct of the parties during the mediation, including a failure to engage in good faith, makes it unlikely that an agreement will be reached.

11. Where the mediation results in an agreement between the parties, the Digital Services Coordinator of establishment shall take such agreement into account and, where appropriate, modify the reasoned request and inform the principal researcher of the modification.

12. Where the parties fail to reach an agreement, the Digital Services Coordinator of establishment shall notify the data provider that the decision of the Digital Services Coordinator of establishment on the amendment request, as last communicated pursuant to Article 40(6), second subparagraph of Regulation (EU) 2022/2065, shall be considered valid and shall serve as the relevant basis for further steps in the process and inform the principal researcher.

13. The Digital Services Coordinator of establishment shall register in AGORA a summary record of the mediation, prepared by the mediator and signed by all parties. The record shall include the following information:

(a) the date of the written request for mediation by the data provider;

(b) the identities and contact details of the parties;

(c) the start and end dates of the mediation;

(d) the outcome of the mediation, including any agreement reached or the reason for termination of the mediation.

Article 14

Independent expert consultation

1. Before formulating a reasoned request, or taking a decision on an amendment request, the Digital Services Coordinator may decide to consult experts.

2. The experts shall be independent and impartial and possess relevant expertise and proven skills and have the capacity and resources to perform the identified task, without incurring undue delay.

3. To attest impartiality, the experts shall sign a declaration confirming that they:

(a) have no financial or personal ties to the data provider or the applicant researchers;

(b) have no interest in the outcome of the data access process;

(c) are free from any conflicts of interest.

4. The Digital Services Coordinator shall encode any consultation carried out pursuant to paragraph 1, along with the expert opinion received in response to the consultation, without undue delay in AGORA.

CHAPTER IV

CONDITIONS FOR PROVIDING THE DATA REQUESTED TO VETTED RESEARCHERS

Article 15

Data sharing and data documentation

1. Data providers shall notify the Digital Services Coordinator of establishment within three working days of the fact:

(a) that access to the requested data has been provided to vetted researchers, in accordance with the reasoned request;

(b) that the access for the vetted researchers has been terminated.

2. Data providers shall provide vetted researchers with any additional information needed to access and understand the requested data, such as codebooks, changelogs and architectural documentation. In cases where the provision of such information may result in a significant vulnerability of the data provider's services, the data provider shall notify the Digital Services Coordinator of establishment of that risk and, where possible, propose alternative information.

3. When providing access to data, data providers shall not impose on vetted researchers data management requirements such as archiving, storage, refresh and deletion requirements, or limitations to the use of standard analytical tools, that may hinder the performance of the relevant research, unless such requirements or limitations are explicitly mentioned in the reasoned request.

4. Where personal data are processed, data providers shall not impose on vetted researchers any conditions in relation to the processing of the shared personal data other than those specified in the reasoned request.

CHAPTER V

FINAL PROVISIONS

Article 16

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 1 July 2025.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

Responsibilities of the Commission as processor for data processing activities conducted in the context of the DSA data access portal

1. The Commission shall set up and ensure a secure and reliable IT infrastructure, the DSA data access portal, on behalf of the Digital Services Coordinators, that supports and streamlines the management of the data access process for researchers, research organisations, data providers and Digital Services Coordinators.

2. To fulfil its obligations as processor for the Digital Services Coordinators, the Commission may use third parties as sub-processors. If it is the case, the controllers shall authorise the Commission to use sub-processors or replace sub-processors where necessary. The Commission shall inform the controllers of said use or replacement of sub-processors, thereby giving the controllers the opportunity to object to any such changes. The Commission shall ensure that the same data protection obligations as set out in this Regulation apply to these sub-processors.

3. The processing by the Commission shall process personal data only insofar as necessary for the:

   (a) authentication and access control with regard to all DSA data access portal users;

   (b) authorisation implementation of requests by DSA data access portal users to create, update and delete any information contained in the application within the DSA data access portal;

   (c) reception of the personal data referred to in Article 5(3) of this Regulation uploaded by DSA data access portal users;

   (d) storage of the personal data in the DSA data access portal;

   (e) deletion of the personal data at their expiration date or upon instruction of the controller;

   (f) after the end of the provision of services provided by the DSA data access portal, deletion of any remaining personal data unless Union or Member State laws require storage of such personal data.

4. The Commission shall take all state of the art organisational, physical, and logical security measures to ensure the DSA data access portal functioning. To this end, the Commission shall:

   (a) designate a responsible entity for the security management of the DSA data access portal, communicate to the controllers its contact information and ensure its availability to react to security threats;

   (b) assume the responsibility for the security of the DSA data access portal, including regularly carrying out tests, evaluations and assessments of the security measures.

5. The Commission shall take all necessary security measures to avoid compromising the smooth operational functioning of the DSA data access portal. This shall include:

   (a) risk assessment procedures to identify and estimate potential threats to the DSA data access portal;

   (b) audit and review procedure to:

      (i) check the correspondence between the implemented security measures and the applicable security policy;

      (ii) control on a regular basis the integrity of the DSA data access portal, security parameters and granted authorisations;

      (iii) detect security breaches and intrusions into the DSA data access portal;

(iv) implement changes to mitigate existing security weaknesses in the DSA data access portal;

(v) define the conditions under which to authorise, including at the request of controllers, and contribute to, the performance of independent audits, including inspections, and reviews on security measures subject to conditions that respect Protocol (No 7) to the Treaty on the Functioning of the European Union on the Privileges and Immunities of the European Union;

(c) changing the control procedure to document, measure the impact of a change before its implementation, and keep the controllers informed of any changes that can affect the communication with and/or the security of the DSA data access portal;

(d) laying down a maintenance and repair procedure to specify the rules and conditions to be respected when maintenance and/or repair of the DSA data access portal is to be performed;

(e) laying down a security incident procedure to define the reporting and escalation scheme, inform without delay the controllers affected, inform without delay the controllers for them to notify the national data protection supervisory authorities of any personal data breach and define a disciplinary process to deal with security breaches in the DSA data access portal.

6. The Commission shall take state of the art physical and logical security measures for the facilities hosting the DSA data access portal and for the controls of data and security access thereto. To this end, the Commission shall:

(a) enforce physical security to establish distinct security perimeters and allowing detection of breaches in the DSA data access portal;

(b) control access to the DSA data access portal facilities;

(c) ensure that equipment cannot be added, replaced or removed without prior authorisation from the designated responsible bodies;

(d) control access from and to the DSA data access portal;

(e) ensure that the DSA data access portal users who access the DSA data access portal are authenticated;

(f) review the authorisation rights related to the access to the DSA data access portal in case of a security breach affecting the DSA data access portal;

(g) keep the integrity of the information transmitted through the DSA data access portal;

(h) implement technical and organisational security measures to prevent unauthorised access to personal data in the DSA data access portal;

(i) implement, whenever necessary, measures to block unauthorised access to the DSA data access portal (i.e. block a location/IP address).

7. The Commission shall:

(a) take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality and security;

(b) maintain a risk management plan related to its area of responsibility;

(c) monitor, in real time, the performance of all the service components of the DSA data access portal, produce regular statistics and keep records;

(d) provide support for the DSA data access portal in English to the DSA data access portal users;

(e) assist the controllers by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of Regulation (EU) 2016/679;

(f) support the controllers by providing information concerning the DSA data access portal to implement the obligations pursuant to Articles 32, 33, 34, 35 and 36 of Regulation (EU) 2016/679;

(g) ensure that data processed within the DSA data access portal is unintelligible to any person who is not authorised to access it;

(h) take all relevant measures to prevent unauthorised access to transmitted personal data via the DSA data access portal;

(i) take measures in order to facilitate communication between the controllers;

(j) maintain a record of processing activities carried out on behalf of the controllers in accordance with Article 31(2) of Regulation (EU) 2018/1725.