Κατευθυντήριες γραμμές 1/2018 σχετικά με την πιστοποίηση και τον προσδιορισμό κριτηρίων πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 του κανονισμού 2016/679

Έκδοση 3.0

4 Ιουνίου 2019

Ιστορικό εκδόσεων

Έκδοση 3.0	4 Ιουνίου 2019	Συμπερίληψη του παραρτήματος 2 (έκδοση 2.0 του παραρτήματος 2, που εγκρίθηκε στις 4 Ιουνίου 2019 μετά τη δημόσια διαβούλευση)
Έκδοση 2.1	9 Απριλίου 2019	Έγκριση διορθωτικού των κατευθυντήριων γραμμών (παράγραφος 45)
Έκδοση 2.0	23 Ιανουαρίου 2019	Έγκριση των κατευθυντήριων γραμμών μετά τη δημόσια διαβούλευση — Την ίδια ημερομηνία εγκρίθηκε το παράρτημα 2 (έκδοση 1.0) για δημόσια διαβούλευση
Έκδοση 1.0	25 Μαΐου 2018	Έγκριση των κατευθυντήριων γραμμών για δημόσια διαβούλευση

Πίνακας περιεχομένων

1.1 Πεδίο εφαρμογής των κατευθυντήριων γραμμών 5
1.2 Ο σκοπός της πιστοποίησης σύμφωνα με τον ΓΚΠΔ 6
1.3 Βασικές έννοιες 7
1.3.1 Ερμηνεία της «πιστοποίησης» 7
1.3.2 Μηχανισμοί πιστοποίησης, σφραγίδες και σήματα 8
2 Ο ρόλος των εποπτικών αρχών 9
2.1 Εποπτική αρχή ως φορέας πιστοποίησης 9
2.2 Περαιτέρω καθήκοντα της εποπτικής αρχής σχετικά με την πιστοποίηση 10
3 Ο ρόλος του φορέα πιστοποίησης 11
4 Η έγκριση των κριτηρίων πιστοποίησης 12
4.1 Έγκριση κριτηρίων από την αρμόδια εποπτική αρχή 12
4.2 Έγκριση κριτηρίων από το ΕΣΠΔ για την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων 13
4.2.1 Αίτηση έγκρισης 13
4.2.2 Κριτήρια για την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων 13
4.2.3 Ο ρόλος της διαπίστευσης 15
5 Η θέσπιση κριτηρίων πιστοποίησης 15
5.1 Τι μπορεί να πιστοποιηθεί σύμφωνα με τον ΓΚΠΔ; 16
5.2 Καθορισμός του αντικειμένου της πιστοποίησης 17
5.3 Μέθοδοι αξιολόγησης και μεθοδολογία της αξιολόγησης 19
5.4 Τεκμηρίωση της αξιολόγησης 20
5.5 Τεκμηρίωση των αποτελεσμάτων 21
6 Καθοδήγηση για τον ορισμό κριτηρίων πιστοποίησης 21
6.1 Υφιστάμενα πρότυπα 22
6.2 Καθορισμός κριτηρίων 22
6.3 Διάρκεια ζωής των κριτηρίων πιστοποίησης 23

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 70 παράγραφος 1 στοιχείο ε) του κανονισμού (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 (εφεξής «ΓΚΠΔ»),

Έχοντας υπόψη τη συμφωνία για τον ΕΟΧ, και ιδίως το παράρτημα XI και το πρωτόκολλο 37, όπως αυτά τροποποιήθηκαν με την απόφαση αριθ. 154/2018 της Μεικτής Επιτροπής του ΕΟΧ, της 6ης Ιουλίου 2018,

Έχοντας υπόψη τα άρθρα 12 και 22 του εσωτερικού κανονισμού του, της 25ης Μαΐου 2018,

Έχοντας λάβει υπόψη τα αποτελέσματα της δημόσιας διαβούλευσης που έλαβε χώρα από τις 30 Μαΐου 2018 έως τις 12 Ιουλίου 2018, σύμφωνα με το άρθρο 70 παράγραφος 4 του ΓΚΠΔ,

ΕΝΕΚΡΙΝΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ:

1. ΕΙΣΑΓΩΓΗ

1. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (κανονισμός 2016/279, «ο ΓΚΠΔ» ή «ο κανονισμός»), παρέχει ένα εκσυγχρονισμένο πλαίσιο για τη συμμόρφωση με τη λογοδοσία και τα θεμελιώδη δικαιώματα για την προστασία δεδομένων στην Ευρώπη. Διάφορα μέτρα που διευκολύνουν τη συμμόρφωση με τις διατάξεις του ΓΚΠΔ έχουν κεντρική σημασία σε αυτό το νέο πλαίσιο. Αυτά περιλαμβάνουν υποχρεωτικές απαιτήσεις σε ειδικές συνθήκες (περιλαμβανομένου του διορισμού υπευθύνων προστασίας δεδομένων και της διενέργειας εκτιμήσεων επιπτώσεων σχετικά με την προστασία των δεδομένων) και εθελοντικά μέτρα όπως κώδικες δεοντολογίας και μηχανισμούς πιστοποίησης.

2. Πριν από την έγκριση του ΓΚΠΔ, η ομάδα εργασίας του άρθρου 29 έκρινε ότι η πιστοποίηση θα μπορούσε να παίξει σημαντικό ρόλο στο πλαίσιο της λογοδοσίας για την προστασία δεδομένων.1 Προκειμένου η πιστοποίηση να παρέχει αξιόπιστες αποδείξεις της συμμόρφωσης με την προστασία δεδομένων, θα πρέπει να θεσπιστούν σαφείς κανόνες οι οποίοι να καθορίζουν απαιτήσεις για τη χορήγηση πιστοποίησης.2 Το άρθρο 42 του ΓΚΠΔ παρέχει τη νομική βάση για την κατάρτιση τέτοιων κανόνων.

3. Το άρθρο 42 παράγραφος 1 του ΓΚΠΔ ορίζει ότι:

   «Τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή παροτρύνουν, ιδίως σε ενωσιακό επίπεδο, τη θέσπιση μηχανισμών πιστοποίησης προστασίας

[1] Ομάδα εργασίας του άρθρου 29, γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας, WP173, 13 Ιουλίου 2010, παράγραφοι 69-71.
[2] Ομάδα εργασίας του άρθρου 29, γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας (WP173), παράγραφος 69.

δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Λαμβάνονται υπόψη οι ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων».

4. Οι μηχανισμοί πιστοποίησης3 μπορούν να βελτιώσουν τη διαφάνεια για τα υποκείμενα των δεδομένων, αλλά επίσης και τις σχέσεις μεταξύ επιχειρήσεων, για παράδειγμα μεταξύ υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία. Η αιτιολογική σκέψη 100 του ΓΚΠΔ αναφέρει ότι η θέσπιση μηχανισμών πιστοποίησης μπορεί να βελτιώσει τη διαφάνεια και τη συμμόρφωση προς τον κανονισμό και να επιτρέψει στα υποκείμενα των δεδομένων να αξιολογούν ταχέως το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων και υπηρεσιών.4

5. Ο ΓΚΠΔ δεν εισάγει δικαίωμα ή υποχρέωση πιστοποίησης για τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία· σύμφωνα με το άρθρο 42 παράγραφος 3, η πιστοποίηση είναι εθελοντική διαδικασία με σκοπό να βοηθήσει την απόδειξη της συμμόρφωσης με τον ΓΚΠΔ. Τα κράτη μέλη και οι εποπτικές αρχές καλούνται να παροτρύνουν τη θέσπιση μηχανισμών πιστοποίησης και θα καθορίσουν τη συμμετοχή των ενδιαφερομένων στη διαδικασία και στον κύκλο ζωής της πιστοποίησης.

6. Επιπλέον, η τήρηση εγκεκριμένων μηχανισμών πιστοποίησης είναι ένας παράγοντας που θα πρέπει να λαμβάνουν υπόψη οι εποπτικές αρχές ως επιβαρυντικό ή ελαφρυντικό στοιχείο όταν αποφασίζουν να επιβάλουν διοικητικό πρόστιμο και όταν ορίζουν το ύψος του προστίμου [άρθρο 83 παράγραφος 2 στοιχείο ι)].5

1.1 Πεδίο εφαρμογής των κατευθυντήριων γραμμών

7. Οι παρούσες κατευθυντήριες γραμμές είναι περιορισμένης εμβέλειας· δεν είναι εγχειρίδιο διαδικασίας για την πιστοποίηση σύμφωνα με τον ΓΚΠΔ. Πρωταρχικός στόχος των εν λόγω κατευθυντήριων γραμμών είναι ο καθορισμός βασικών απαιτήσεων και κριτηρίων που μπορεί να αφορούν όλους τους τύπους μηχανισμών πιστοποίησης που εφαρμόζονται σύμφωνα με τα άρθρα 42 και 43 του ΓΚΠΔ. Για τον σκοπό αυτό, οι κατευθυντήριες γραμμές:

    - διερευνούν τη λογική της πιστοποίησης ως εργαλείου λογοδοσίας·
    - εξηγούν τις βασικές έννοιες των διατάξεων περί πιστοποίησης στα άρθρα 42 και 43· και
    - εξηγούν το πεδίο εφαρμογής του τι μπορεί να πιστοποιηθεί σύμφωνα με τα άρθρα 42 και 43 και τον σκοπό της πιστοποίησης·

[3] Οι παρούσες κατευθυντήριες γραμμές θα αναφέρονται στους μηχανισμούς πιστοποίησης και τις σφραγίδες και τα σήματα προστασίας δεδομένων συνολικά με τον όρο «μηχανισμοί πιστοποίησης», βλέπε τμήμα 1.3.2.
[4] Η αιτιολογική σκέψη 100 του ΓΚΠΔ αναφέρει ότι θα πρέπει να παροτρύνεται η θέσπιση μηχανισμών πιστοποίησης για τη «βελτίωση της διαφάνειας και της συμμόρφωσης προς τον κανονισμό επιτρέποντας στα υποκείμενα των δεδομένων να αξιολογούν ταχέως το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων και υπηρεσιών».
[5] Βλέπε ομάδα εργασίας του άρθρου 29, κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679 (WP 253).

- βοηθούν ώστε το αποτέλεσμα της πιστοποίησης να είναι ουσιαστικό, σαφές, όσο πιο αναπαραγώγιμο γίνεται και συγκρίσιμο ανεξαρτήτως του φορέα πιστοποίησης (συγκρισιμότητα).

8. Ο ΓΚΠΔ δίνει στα κράτη μέλη και στις εποπτικές αρχές τη δυνατότητα να εφαρμόσουν τα άρθρα 42 και 43 με διάφορους τρόπους. Οι κατευθυντήριες γραμμές παρέχουν συμβουλές σχετικά με την ερμηνεία και την εφαρμογή των διατάξεων στα άρθρα 42 και 43 και θα βοηθήσουν τα κράτη μέλη, τις εποπτικές αρχές και τους εθνικούς οργανισμούς διαπίστευσης να θεσπίσουν μια πιο συνεκτική και εναρμονισμένη προσέγγιση για την εφαρμογή μηχανισμών πιστοποίησης σύμφωνα με τον ΓΚΠΔ.

9. Οι συμβουλές που περιέχονται στις κατευθυντήριες γραμμές θα αφορούν:

    - τις αρμόδιες εποπτικές αρχές και το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων («το ΕΣΠΔ») όταν εγκρίνουν κριτήρια πιστοποίησης σύμφωνα με το άρθρο 42 παράγραφος 5, το άρθρο 58 παράγραφος 3 στοιχείο στ) και το άρθρο 70 παράγραφος 1 στοιχείο ιε)·

    - τους φορείς πιστοποίησης όταν σχεδιάζουν και αναθεωρούν τα κριτήρια πιστοποίησης πριν από την υποβολή στην αρμόδια εποπτική αρχή για έγκριση σύμφωνα με το άρθρο 42 παράγραφος 5·

    - το ΕΣΠΔ όταν εγκρίνει την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων σύμφωνα με το άρθρο 42 παράγραφος 5 και το άρθρο 70 παράγραφος 1 στοιχείο ιε)·

    - τις εποπτικές αρχές, όταν σχεδιάζουν τα δικά τους κριτήρια πιστοποίησης·

    - την Ευρωπαϊκή Επιτροπή, η οποία διαθέτει την εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων με σκοπό τον προσδιορισμό των απαιτήσεων που πρέπει να ληφθούν υπόψη για τους μηχανισμούς πιστοποίησης σύμφωνα με το άρθρο 43 παράγραφος 8·

    - το ΕΣΠΔ όταν γνωμοδοτεί στην Ευρωπαϊκή Επιτροπή σχετικά με τις απαιτήσεις πιστοποίησης σύμφωνα με το άρθρο 70 παράγραφος 1 στοιχείο ιη) και το άρθρο 43 παράγραφος 8·

    - τους εθνικούς οργανισμούς διαπίστευσης, οι οποίοι θα χρειαστεί να λάβουν υπόψη κριτήρια πιστοποίησης ενόψει της διαπίστευσης φορέων πιστοποίησης σύμφωνα με το πρότυπο EN-ISO/IEC 17065/2012 και τις πρόσθετες απαιτήσεις σύμφωνα με το άρθρο 43· και

    - τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία όταν ορίζουν τη δική τους στρατηγική συμμόρφωσης με τον ΓΚΠΔ και εξετάζουν την πιστοποίηση ως μέσο απόδειξης της συμμόρφωσης.

10. Το ΕΣΠΔ θα δημοσιεύσει χωριστές κατευθυντήριες γραμμές για να προσδιορίσει τα κριτήρια έγκρισης των μηχανισμών πιστοποίησης ως εργαλείων διαβίβασης σε τρίτες χώρες ή διεθνείς οργανισμούς σύμφωνα με το άρθρο 42 παράγραφος 2.

1.2 Ο σκοπός της πιστοποίησης σύμφωνα με τον ΓΚΠΔ

11. Το άρθρο 42 παράγραφος 1 προβλέπει ότι μηχανισμοί πιστοποίησης θεσπίζονται «με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία».

12. Ο ΓΚΠΔ παρουσιάζει χαρακτηριστικά το πλαίσιο στο οποίο μπορούν να χρησιμοποιηθούν εγκεκριμένοι μηχανισμοί πιστοποίησης ως στοιχείο που αποδεικνύει τη συμμόρφωση με τις υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία σχετικά με:

    - την εφαρμογή και την απόδειξη κατάλληλων τεχνικών και οργανωτικών μέτρων όπως αναφέρεται στο άρθρο 24 παράγραφοι 1 και 3, στο άρθρο 25 και στο άρθρο 32 παράγραφοι 1 και 3·
    - τις επαρκείς διαβεβαιώσεις που αναφέρονται στο άρθρο 28 παράγραφος 1 (ο εκτελών την επεξεργασία στον υπεύθυνο επεξεργασίας) και παράγραφος 4 (ο άλλος εκτελών την επεξεργασία στον εκτελούντα την επεξεργασία).

13. Καθώς η πιστοποίηση αυτή καθαυτή δεν αποδεικνύει συμμόρφωση, αλλά μάλλον αποτελεί ένα στοιχείο που μπορεί να χρησιμοποιηθεί προς απόδειξη συμμόρφωσης, θα πρέπει να καταρτίζεται με διαφάνεια. Η απόδειξη της συμμόρφωσης απαιτεί δικαιολογητικά έγγραφα, ειδικότερα γραπτές εκθέσεις που όχι μόνο επαναλαμβάνουν, αλλά περιγράφουν πώς πληρούνται τα κριτήρια και, αν δεν πληρούνταν αρχικά, περιγράφουν τις διορθώσεις, τις διορθωτικές δράσεις και την καταλληλότητά τους, παρέχοντας έτσι τους λόγους χορήγησης και διατήρησης της πιστοποίησης. Αυτό περιλαμβάνει την περιγραφή κάθε απόφασης χορήγησης, ανανέωσης ή ανάκλησης πιστοποιητικού. Θα πρέπει να παρέχει τους λόγους, τα επιχειρήματα και τις αποδείξεις που προκύπτουν από την εφαρμογή των κριτηρίων, καθώς και τα συμπεράσματα, τις αποφάσεις ή τα συμπερασματικά στοιχεία από πραγματικά περιστατικά ή παραδοχές που συγκεντρώθηκαν κατά τη διάρκεια της πιστοποίησης.

1.3 Βασικές έννοιες

14. Το παρακάτω τμήμα διερευνά τις βασικές έννοιες στα άρθρα 42 και 43. Η ανάλυση αυτή συμβάλλει στην κατανόηση των βασικών όρων και του πεδίου εφαρμογής της πιστοποίησης σύμφωνα με τον ΓΚΠΔ.

1.3.1 Ερμηνεία της «πιστοποίησης»

15. Ο ΓΚΠΔ δεν ορίζει την «πιστοποίηση». Ο Διεθνής Οργανισμός Τυποποίησης (ISO) παρέχει έναν καθολικά αποδεκτό ορισμό της πιστοποίησης: «η παροχή από ανεξάρτητο φορέα γραπτής διαβεβαίωσης (πιστοποιητικού) ότι το υπό εξέταση προϊόν, η υπηρεσία ή το σύστημα πληροί συγκεκριμένες απαιτήσεις.» Η πιστοποίηση είναι γνωστή και ως «αξιολόγηση της συμμόρφωσης από τρίτο μέρος» και οι φορείς πιστοποίησης μπορούν να αναφέρονται και ως «φορείς αξιολόγησης της συμμόρφωσης» (ΦΑΣ). Στο πρότυπο EN-ISO/IEC 17000:2004 - Αξιολόγηση συμμόρφωσης -- Λεξιλόγιο και γενικές αρχές (στα οποία αναφέρεται το πρότυπο ISO17065) - η πιστοποίηση ορίζεται ως εξής: «επιβεβαίωση τρίτου μέρους… αναφορικά με προϊόντα, διεργασίες και υπηρεσίες».

16. Η επιβεβαίωση συνιστά «έκδοση δήλωσης, βάσει απόφασης κατόπιν ελέγχου, ότι η εκπλήρωση συγκεκριμένων απαιτήσεων έχει τεκμηριωθεί» (τμήμα 5.2, πρότυπο ISO 17000:2004).

17. Στο πλαίσιο της πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 του ΓΚΠΔ, η πιστοποίηση αναφέρεται στην επιβεβαίωση τρίτου μέρους αναφορικά με πράξεις επεξεργασίας υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία.

1.3.2 Μηχανισμοί πιστοποίησης, σφραγίδες και σήματα

18. Ο ΓΚΠΔ δεν ορίζει τους «μηχανισμούς πιστοποίησης, τις σφραγίδες ή τα σήματα» και χρησιμοποιεί τους όρους συλλογικά. Το πιστοποιητικό είναι μια δήλωση συμμόρφωσης. Η σφραγίδα ή το σήμα μπορούν να χρησιμοποιηθούν για να σημάνουν την επιτυχή ολοκλήρωση της διαδικασίας πιστοποίησης. Η σφραγίδα ή το σήμα αναφέρονται συνήθως στον λογότυπο ή στο σύμβολο του οποίου η παρουσία (επιπλέον του πιστοποιητικού) υποδεικνύει ότι το αντικείμενο της πιστοποίησης έχει αξιολογηθεί ανεξάρτητα στο πλαίσιο διαδικασίας πιστοποίησης και συμμορφώνεται με συγκεκριμένες απαιτήσεις που αναφέρονται σε κανονιστικά έγγραφα όπως κανονισμούς, πρότυπα ή τεχνικές προδιαγραφές. Οι απαιτήσεις αυτές στο πλαίσιο της πιστοποίησης σύμφωνα με τον ΓΚΠΔ περιέχονται στις πρόσθετες απαιτήσεις που συμπληρώνουν τους κανόνες διαπίστευσης των φορέων πιστοποίησης στο πρότυπο EN-ISO/IEC 17065/2012 και τα κριτήρια πιστοποίησης που έχει εγκρίνει η αρμόδια εποπτική αρχή ή το Συμβούλιο Προστασίας Δεδομένων. Πιστοποιητικό, σφραγίδα ή σήμα σύμφωνα με τον ΓΚΠΔ μπορεί να χορηγηθεί μόνο κατόπιν της ανεξάρτητης αξιολόγησης των αποδείξεων από διαπιστευμένο φορέα πιστοποίησης ή αρμόδια εποπτική αρχή, που θα αναφέρει ότι τα κριτήρια πιστοποίησης έχουν εκπληρωθεί.

19. Ο πίνακας παρέχει ένα γενικό παράδειγμα διαδικασίας πιστοποίησης.

Υποβολή αίτησης από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία	Επίσημος έλεγχος από ΦΠ	Αξιολόγηση Προαξιολόγηση	Αξιολόγηση Αξιολόγηση του ToE	Αξιολόγηση Επικύρωση αποτελεσμάτων	Πληροφορίες προς την ΑΕΑ	Πιστοποίηση	Παρακολούθηση	Ανανέωση της πιστοποίησης
Είναι η περιγραφή του αντικειμένου της αξιολόγησης (ToE) σαφής και πλήρης περιλαμβανομένων των διεπαφών;	Μπορεί να γίνει αποδεκτή η περιγραφή του ToE;	Ποια είναι τα ισχύοντα κριτήρια;	Πληροί το ToE τα κριτήρια;	Αντανακλούν όλα τα σχετικά κριτήρια που προσδιορίζονται το ToE;	Έχει αιτιολογηθεί η χορήγηση ή η απόσυρση της πιστοποίησης;	Μπορεί να δοθεί το πιστοποιητικό;	Εξακολουθεί το ToE να πληροί τα κριτήρια;	Εξακολουθεί η επεξεργασία να πληροί τα κριτήρια πιστοποίησης;
Μπορεί να χορηγηθεί πρόσβαση στις δραστηριότητες επεξεργασίας του ToE;	Είναι όλα τα έγγραφα πλήρη και επικαιροποιημένα;	Ποιες είναι οι ισχύουσες μέθοδοι αξιολόγησης;	Είναι ορθή η τεκμηρίωση του ToE;	Έχει τεκμηριωθεί επαρκώς η αξιολόγηση;		Είναι οι εκθέσεις έτοιμες για δημοσίευση;	Χρησιμοποιείται ορθά το πιστοποιητικό /η σφραγίδα /το σήμα αξιοπιστίας;	Έχουν αντιμετωπιστεί ικανοποιητικά οι τομείς ανάπτυξης;
Άρθρο 42 παράγραφος 6	Άρθρο 43 παράγραφος 4	Άρθρο 43 παράγραφος 4	Άρθρο 42 παράγραφος 5, άρθρο 43	Άρθρο 43 παράγραφος 4	Άρθρο 43 παράγραφος 1, άρθρο 43 παράγραφος 5	Άρθρο 43 παράγραφος 1, άρθρο 42 παράγραφος 7	Άρθρο 42 παράγραφος 7	Άρθρο 42 παράγραφος 7

2 Ο ΡΟΛΟΣ ΤΩΝ ΕΠΟΠΤΙΚΩΝ ΑΡΧΩΝ

20. Το άρθρο 42 παράγραφος 5 προβλέπει ότι η πιστοποίηση χορηγείται από διαπιστευμένο φορέα πιστοποίησης ή από αρμόδια εποπτική αρχή. Ο ΓΚΠΔ δεν καθιστά τη χορήγηση πιστοποιήσεων υποχρεωτικό καθήκον των εποπτικών αρχών. Αντίθετα, ο ΓΚΠΔ δίνει δυνατότητα για διάφορα μοντέλα. Για παράδειγμα, η εποπτική αρχή δύναται να αποφασίσει να επιλέξει ένα ή περισσότερα από τα παρακάτω:

    - να χορηγήσει πιστοποίηση η ίδια, με βάση το δικό της σύστημα πιστοποίησης·
    - να χορηγήσει πιστοποίηση η ίδια, με βάση το δικό της σύστημα πιστοποίησης, αλλά να αναθέσει το σύνολο ή μέρος της διαδικασίας αξιολόγησης σε τρίτα μέρη·
    - να δημιουργήσει το δικό της σύστημα πιστοποίησης και να αναθέσει σε φορείς πιστοποίησης τη διαδικασία πιστοποίησης και τη χορήγηση πιστοποίησης· και
    - να παροτρύνει την αγορά να αναπτύξει μηχανισμούς πιστοποίησης.

21. Η εποπτική αρχή θα πρέπει επίσης να εξετάζει τον ρόλο της με βάση τις αποφάσεις που λαμβάνονται σε εθνικό επίπεδο αναφορικά με τους μηχανισμούς διαπίστευσης —ιδίως αν η διαπίστευση φορέων πιστοποίησης είναι αρμοδιότητα της ίδιας της εποπτικής αρχής σύμφωνα με το άρθρο 43 παράγραφος 1 του ΓΚΠΔ. Συνεπώς, κάθε εποπτική αρχή θα καθορίσει ποια προσέγγιση θα υιοθετήσει προκειμένου να επιδιώξει τον ευρύ στόχο πιστοποίησης σύμφωνα με τον ΓΚΠΔ. Η προσέγγιση αυτή θα καθοριστεί στο πλαίσιο όχι μόνο των καθηκόντων και των εξουσιών σύμφωνα με τα άρθρα 57 και 58, αλλά και του γεγονότος ότι η πιστοποίηση πρέπει να θεωρείται ως παράγοντας που συνεκτιμάται για τον καθορισμό διοικητικών προστίμων, και γενικότερα ως μέσο απόδειξης συμμόρφωσης.

2.1 Εποπτική αρχή ως φορέας πιστοποίησης

22. Στις περιπτώσεις όπου η εποπτική αρχή επιλέγει να διενεργήσει πιστοποίηση, θα πρέπει να αξιολογήσει προσεκτικά τον ρόλο της αναφορικά με τα καθήκοντα που της έχουν ανατεθεί σύμφωνα με τον ΓΚΠΔ. Ο ρόλος της θα πρέπει να είναι διαφανής κατά την άσκηση των αρμοδιοτήτων της. Θα χρειαστεί να προσέξει ειδικότερα τη διάκριση εξουσιών που αφορούν τις έρευνες και την επιβολή προκειμένου να αποφύγει οποιεσδήποτε πιθανές συγκρούσεις συμφερόντων.

23. Όταν ενεργεί ως φορέας πιστοποίησης, η εποπτική αρχή θα πρέπει να διασφαλίσει την κατάλληλη δημιουργία ενός μηχανισμού πιστοποίησης και να αναπτύξει δικά της κριτήρια πιστοποίησης ή να υιοθετήσει άλλα. Επιπλέον, κάθε εποπτική αρχή η οποία εκδίδει πιστοποιήσεις έχει το καθήκον να τις επανεξετάζει περιοδικά [άρθρο 57 παράγραφος 1 στοιχείο ιε)] και την εξουσία να τις αποσύρει εφόσον οι απαιτήσεις πιστοποίησης δεν πληρούνται ή δεν πληρούνται πλέον [άρθρο 58 παράγραφος 2 στοιχείο η)]. Για την εκπλήρωση αυτών των απαιτήσεων, είναι χρήσιμο να δημιουργηθούν μια διαδικασία πιστοποίησης και απαιτήσεις της διαδικασίας αυτής, και, αν δεν ορίζεται διαφορετικά π.χ. από την εθνική νομοθεσία, να τεθεί σε εφαρμογή μια νομικά εκτελεστή σύμβαση με κάθε αιτούντα οργανισμό για την παροχή δραστηριοτήτων πιστοποίησης. Θα πρέπει να διασφαλιστεί ότι η εν λόγω σύμβαση πιστοποίησης απαιτεί από τον αιτούντα να

συμμορφώνεται τουλάχιστον με τα κριτήρια πιστοποίησης, περιλαμβανομένων των απαραίτητων ρυθμίσεων για τη διενέργεια της αξιολόγησης, την παρακολούθηση της τήρησης των κριτηρίων και την περιοδική επανεξέταση, περιλαμβανομένης της πρόσβασης σε πληροφορίες και/ή εγκαταστάσεις, της τεκμηρίωσης και της δημοσίευσης εκθέσεων και αποτελεσμάτων, και της διερεύνησης καταγγελιών. Επιπλέον, αναμένεται ότι η εποπτική αρχή θα τηρήσει τις απαιτήσεις στις κατευθυντήριες γραμμές για τη διαπίστευση των φορέων πιστοποίησης επιπλέον των απαιτήσεων σύμφωνα με το άρθρο 43 παράγραφος 2.

2.2 Περαιτέρω καθήκοντα της εποπτικής αρχής σχετικά με την πιστοποίηση

24. Στα κράτη μέλη όπου αρχίζουν να δραστηριοποιούνται φορείς πιστοποίησης, η εποπτική αρχή έχει την εξουσία και το καθήκον, ανεξαρτήτως των δικών της δραστηριοτήτων:

    - να αξιολογεί τα κριτήρια του συστήματος πιστοποίησης και να συντάσσει σχέδιο απόφασης (άρθρο 42 παράγραφος 5)·
    - να ανακοινώνει στο Συμβούλιο Προστασίας Δεδομένων το σχέδιο απόφασης όταν προτίθεται να εγκρίνει τα κριτήρια πιστοποίησης [άρθρο 64 παράγραφος 1 στοιχείο γ), άρθρο 64 παράγραφος 7] και να λαμβάνει υπόψη τη γνώμη του Συμβουλίου Προστασίας Δεδομένων [άρθρο 64 παράγραφος 1 στοιχείο γ) και άρθρο 70 παράγραφος 1 στοιχείο κ)]·
    - να εγκρίνει τα κριτήρια πιστοποίησης [άρθρο 58 παράγραφος 3 στοιχείο στ)] προκειμένου να είναι δυνατό να πραγματοποιηθούν η διαπίστευση και η πιστοποίηση [άρθρο 42 παράγραφος 5 και άρθρο 43 παράγραφος 2 στοιχείο β)]·
    - να δημοσιεύει τα κριτήρια πιστοποίησης (άρθρο 43 παράγραφος 6)·
    - να ενεργεί ως αρμόδια αρχή για τα συστήματα πιστοποίησης σε όλη την ΕΕ, το οποίο μπορεί να οδηγήσει στην εγκεκριμένη από το ΕΣΠΔ Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων [άρθρο 42 παράγραφος 5 και άρθρο 70 παράγραφος 1 στοιχείο ιε)]· και
    - να διατάξει τον φορέα πιστοποίησης α) να μην εκδώσει πιστοποίηση ή β) να αποσύρει την πιστοποίηση εφόσον οι απαιτήσεις πιστοποίησης (διαδικασίες ή κριτήρια πιστοποίησης) δεν πληρούνται ή δεν πληρούνται πλέον [άρθρο 58 παράγραφος 2 στοιχείο η)].

25. Ο ΓΚΠΔ αναθέτει στην εποπτική αρχή την έγκριση κριτηρίων πιστοποίησης, αλλά όχι τη θέσπιση κριτηρίων. Προκειμένου να εγκρίνει κριτήρια πιστοποίησης σύμφωνα με το άρθρο 42 παράγραφος 5, η εποπτική αρχή θα πρέπει να αντιλαμβάνεται σαφώς τι να αναμένει, ειδικότερα ως προς το πεδίο εφαρμογής και το περιεχόμενο της απόδειξης συμμόρφωσης με τον ΓΚΠΔ και αναφορικά με το καθήκον της να παρακολουθεί και να επιβάλλει την εφαρμογή του κανονισμού. Το παράρτημα παρέχει καθοδήγηση για να εξασφαλιστεί μια εναρμονισμένη προσέγγιση κατά την αξιολόγηση κριτηρίων για τον σκοπό της έγκρισης.

26. Το άρθρο 43 παράγραφος 1 υποχρεώνει τους φορείς πιστοποίησης να ενημερώνουν την εποπτική τους αρχή πριν χορηγήσουν ή ανανεώσουν πιστοποιήσεις προκειμένου να μπορέσει η αρμόδια εποπτική αρχή να ασκήσει τις διορθωτικές εξουσίες της σύμφωνα με το άρθρο 58 παράγραφος 2 στοιχείο η). Επιπλέον, το άρθρο 43 παράγραφος 5 υποχρεώνει τους φορείς πιστοποίησης να παρέχουν στην αρμόδια εποπτική αρχή τους λόγους χορήγησης ή ανάκλησης της αιτηθείσας πιστοποίησης. Παρόλο που ο ΓΚΠΔ δίνει τη δυνατότητα στις εποπτικές αρχές να καθορίσουν τον τρόπο λήψης, επιβεβαίωσης, επανεξέτασης και διαχείρισης αυτών των πληροφοριών σε επιχειρησιακό επίπεδο (για παράδειγμα, αυτό θα μπορούσε να περιλαμβάνει τεχνολογικές λύσεις για την υποβολή εκθέσεων από τους φορείς πιστοποίησης), ο φορέας πιστοποίησης μπορεί να θέσει σε εφαρμογή μια διαδικασία και κριτήρια επεξεργασίας των πληροφοριών και των εκθέσεων που υποβάλλονται σε κάθε επιτυχές έργο πιστοποίησης σύμφωνα με το άρθρο 43 παράγραφος 1. Βάσει αυτών των πληροφοριών, η εποπτική αρχή μπορεί να ασκεί την εξουσία της να διατάσσει τον φορέα πιστοποίησης να αποσύρει ή να μην εκδώσει πιστοποίηση [άρθρο 58 παράγραφος 2 στοιχείο η)] και να παρακολουθεί και να επιβάλλει την εφαρμογή των απαιτήσεων και των κριτηρίων πιστοποίησης σύμφωνα με τον ΓΚΠΔ [άρθρο 57 παράγραφος 1 στοιχείο α) και άρθρο 58 παράγραφος 2 στοιχείο η)]. Έτσι θα στηριχθεί η εναρμονισμένη προσέγγιση και η συγκρισιμότητα στην πιστοποίηση από διαφορετικούς φορείς πιστοποίησης, καθώς και η γνώση εκ μέρους των εποπτικών αρχών των πληροφοριών για την κατάσταση πιστοποίησης ενός οργανισμού.

3 Ο ΡΟΛΟΣ ΤΟΥ ΦΟΡΕΑ ΠΙΣΤΟΠΟΙΗΣΗΣ

27. Ο ρόλος του φορέα πιστοποίησης είναι να εκδίδει, να επανεξετάζει, να ανανεώνει και να ανακαλεί πιστοποιήσεις (άρθρο 42 παράγραφοι 5 και 7) βάσει ενός μηχανισμού πιστοποίησης και εγκεκριμένων κριτηρίων (άρθρο 43 παράγραφος 1). Αυτό απαιτεί από τον φορέα πιστοποίησης ή τον ιδιοκτήτη του συστήματος πιστοποίησης να δημιουργήσει και να καθορίσει κριτήρια πιστοποίησης και διαδικασίες πιστοποίησης, περιλαμβανομένων διαδικασιών για την παρακολούθηση της τήρησης, την επανεξέταση, τη διαχείριση καταγγελιών και την ανάκληση. Τα κριτήρια πιστοποίησης επανεξετάζονται στο πλαίσιο της διαδικασίας διαπίστευσης, η οποία λαμβάνει υπόψη τους κανόνες και τις διαδικασίες με βάση τις οποίες εκδίδονται πιστοποιήσεις, σφραγίδες ή σήματα [άρθρο 43 παράγραφος 2 στοιχείο γ)].

28. Η ύπαρξη μηχανισμού πιστοποίησης και κριτηρίων πιστοποίησης είναι απαραίτητη για να επιτύχει ο φορέας πιστοποίησης τη διαπίστευση σύμφωνα με το άρθρο 43. Σημαντικό αντίκτυπο στις ενέργειες του φορέα πιστοποίησης έχει το πεδίο εφαρμογής και το είδος των κριτηρίων πιστοποίησης που έχουν αντίκτυπο στις διαδικασίες πιστοποίησης και αντίστροφα. Συγκεκριμένα κριτήρια μπορεί, για παράδειγμα, να απαιτούν συγκεκριμένες μεθόδους αξιολόγησης, όπως επιτόπιες επιθεωρήσεις και επανεξέταση του κώδικα. Οι διαδικασίες αυτές είναι υποχρεωτικές για τη διαπίστευση και εξηγούνται περαιτέρω στις κατευθυντήριες γραμμές σχετικά με τη διαπίστευση.

29. Ο ΓΚΠΔ υποχρεώνει τον φορέα πιστοποίησης να παρέχει στις εποπτικές αρχές πληροφορίες, ειδικά σχετικά με μεμονωμένες πιστοποιήσεις, κάτι το οποίο είναι απαραίτητο για την

παρακολούθηση της εφαρμογής του μηχανισμού πιστοποίησης [άρθρο 42 παράγραφος 7, άρθρο 43 παράγραφος 5 και άρθρο 58 παράγραφος 2 στοιχείο η)].

4 Η ΕΓΚΡΙΣΗ ΤΩΝ ΚΡΙΤΗΡΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

30. Τα κριτήρια πιστοποίησης αποτελούν αναπόσπαστο μέρος κάθε μηχανισμού πιστοποίησης. Συνεπώς, ο ΓΚΠΔ απαιτεί την έγκριση των κριτηρίων πιστοποίησης κάθε μηχανισμού πιστοποίησης από την αρμόδια εποπτική αρχή [άρθρο 42 παράγραφος 5 και άρθρο 43 παράγραφος 2 στοιχείο β)]. Διαφορετικά, στην περίπτωση της Ευρωπαϊκής Σφραγίδας Προστασίας των Δεδομένων, τα κριτήρια πιστοποίησης εγκρίνονται από το ΕΣΠΔ [άρθρο 42 παράγραφος 5 και άρθρο 70 παράγραφος 1 στοιχείο ιε)]. Και οι δύο οδοί έγκρισης κριτηρίων πιστοποίησης εξηγούνται στη συνέχεια.

31. Το ΕΣΠΔ αναγνωρίζει τους παρακάτω σκοπούς για την έγκριση κριτηρίων πιστοποίησης:

    - να αντανακλούν ορθά τις απαιτήσεις και τις αρχές σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που προβλέπονται στον κανονισμό (ΕΕ) 2016/679· και
    - να συμβάλλουν στη συνεκτική εφαρμογή του ΓΚΠΔ.

32. Η έγκριση χορηγείται με βάση την απαίτηση του ΓΚΠΔ σύμφωνα με την οποία ο μηχανισμός πιστοποίησης παρέχει στους υπευθύνους επεξεργασίας και στους εκτελούντες την επεξεργασία τη δυνατότητα να αποδείξουν ότι τα κριτήρια πιστοποίησης τηρούν πλήρως τον ΓΚΠΔ.

4.1 Έγκριση κριτηρίων από την αρμόδια εποπτική αρχή

33. Τα κριτήρια πιστοποίησης πρέπει να εγκριθούν από την αρμόδια εποπτική αρχή πριν από ή κατά τη διάρκεια της διαδικασίας διαπίστευσης του φορέα πιστοποίησης. Έγκριση απαιτείται επίσης για επικαιροποιημένα ή πρόσθετα συστήματα ή σύνολα κριτηρίων σύμφωνα με το πρότυπο ISO 17065 από τον ίδιο φορέα πιστοποίησης πριν από τη χρήση των τροποποιημένων μηχανισμών πιστοποίησης [άρθρο 42 παράγραφος 5 και άρθρο 43 παράγραφος 2 στοιχείο β)]. Οι εποπτικές αρχές αντιμετωπίζουν όλα τα αιτήματα έγκρισης κριτηρίων πιστοποίησης με δίκαιο τρόπο και χωρίς διακρίσεις, σύμφωνα με μια δημόσια διαθέσιμη διαδικασία η οποία προσδιορίζει τις γενικές προϋποθέσεις που πρέπει να πληρούνται και περιγράφει τη διαδικασία έγκρισης.

34. Ο φορέας πιστοποίησης μπορεί να χορηγήσει πιστοποίηση σε ένα συγκεκριμένο κράτος μέλος μόνο σύμφωνα με τα κριτήρια που έχει εγκρίνει η εποπτική αρχή στο συγκεκριμένο κράτος μέλος. Με άλλα λόγια, τα κριτήρια πιστοποίησης πρέπει να εγκριθούν από την αρμόδια εποπτική αρχή εκεί όπου ο φορέας πιστοποίησης στοχεύει να προσφέρει πιστοποίηση και αποκτά διαπίστευση. Βλέπε το παρακάτω τμήμα για συστήματα πιστοποίησης σε όλη την Ευρώπη.

4.2 Έγκριση κριτηρίων από το ΕΣΠΔ για την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων

35. Ο φορέας πιστοποίησης μπορεί επίσης να εκδώσει πιστοποίηση σύμφωνα με κριτήρια που έχει εγκρίνει το ΕΣΠΔ για την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων. Τα κριτήρια πιστοποίησης που έχει εγκρίνει το ΕΣΠΔ σύμφωνα με το άρθρο 63 μπορεί να οδηγήσουν στην Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων (άρθρο 42 παράγραφος 5). Με βάση τις υφιστάμενες συμβάσεις πιστοποίησης και διαπίστευσης, το ΕΣΠΔ αναγνωρίζει ότι είναι επιθυμητό να αποφευχθεί ο κατακερματισμός της αγοράς πιστοποίησης της προστασίας των δεδομένων. Σημειώνει ότι το άρθρο 42 παράγραφος 1 προβλέπει ότι τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή ενθαρρύνουν τη θέσπιση μηχανισμών πιστοποίησης, ιδίως σε ενωσιακό επίπεδο.

4.2.1 Αίτηση έγκρισης

36. Η αίτηση έγκρισης κριτηρίων από το ΕΣΠΔ σύμφωνα με το άρθρο 42 παράγραφος 5 και το άρθρο 70 παράγραφος 1 στοιχείο ιε) πρέπει να υποβληθεί μέσω αρμόδιας εποπτικής αρχής και θα πρέπει να αναφέρει την πρόθεση του ιδιοκτήτη του συστήματος, του υποψηφίου ή του διαπιστευμένου φορέα πιστοποίησης να προσφέρει τα κριτήρια σε έναν μηχανισμό πιστοποίησης που απευθύνεται σε υπευθύνους επεξεργασίας και εκτελούντες επεξεργασία σε όλα τα κράτη μέλη. Η αρμόδια εποπτική αρχή θα υποβάλει στο ΕΣΠΔ σχέδιο όταν κρίνει ότι τα κριτήρια μπορούν να εγκριθούν από το ΕΣΠΔ.

37. Ο τόπος υποβολής της αίτησης έγκρισης κριτηρίων επιλέγεται με βάση τους ιδιοκτήτες του συστήματος πιστοποίησης ή τα κεντρικά γραφεία των φορέων πιστοποίησης.

38. Αν ένας φορέας πιστοποίησης υποβάλει αίτηση, η υποβολή αυτή κατά κανόνα πραγματοποιείται στο πλαίσιο αίτησης διαπίστευσης ή ο φορέας είναι ήδη διαπιστευμένος είτε από την αρμόδια εποπτική αρχή είτε από τον εθνικό οργανισμό διαπίστευσης του κράτους μέλους του. Αν ο φορέας πιστοποίησης είναι ήδη διαπιστευμένος για μηχανισμό πιστοποίησης σύμφωνα με τον ΓΚΠΔ, αυτό μπορεί να βοηθήσει στη βελτίωση της διαδικασίας εγκρίσεων.

4.2.2 Κριτήρια για την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων

39. Το ΕΣΠΔ θα συντονίσει τη διαδικασία αξιολόγησης και θα εγκρίνει τα κριτήρια για την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων σύμφωνα με τις απαιτήσεις. Η αξιολόγηση θα αφορά τομείς όπως: το πεδίο εφαρμογής των κριτηρίων και την καταλληλότητά τους να χρησιμεύσουν ως κοινή πιστοποίηση. Αν τα κριτήρια εγκριθούν από το ΕΣΠΔ, η αρμόδια εποπτική αρχή για τα κεντρικά γραφεία του φορέα πιστοποίησης στην ΕΕ αναμένεται να διαχειρίζεται καταγγελίες σχετικά με τον ίδιο τον μηχανισμό και να ενημερώνει τις άλλες εποπτικές αρχές. Η εν λόγω εποπτική αρχή είναι επίσης αρμόδια για τη λήψη μέτρων κατά του φορέα πιστοποίησης. Ανάλογα με την περίπτωση, η αρμόδια εποπτική αρχή θα ενημερώνει τις άλλες εποπτικές αρχές και το ΕΣΠΔ.

40. Τα κριτήρια πιστοποίησης που στοχεύουν στην κοινή πιστοποίηση υπόκεινται σε απαιτήσεις σε επίπεδο ΕΕ και θα πρέπει να παρέχουν έναν συγκεκριμένο μηχανισμό για την αντιμετώπιση αυτών των απαιτήσεων. Οι ευρωπαϊκοί μηχανισμοί πιστοποίησης πρέπει να προορίζονται για χρήση σε όλα τα κράτη μέλη. Βάσει του άρθρου 42 παράγραφος 5, ο μηχανισμός της Ευρωπαϊκής Σφραγίδας Προστασίας των Δεδομένων, καθώς και τα κριτήριά του πρέπει να είναι δυνατό να προσαρμόζονται κατάλληλα ώστε να λαμβάνουν υπόψη εθνικούς τομεακούς κανονισμούς κατά περίπτωση, π.χ. για την επεξεργασία δεδομένων στα σχολεία, και να είναι δυνατό να εφαρμοστούν σε όλη την Ευρώπη.

41. Παράδειγμα: Ένα διεθνές σχολείο που προσφέρει εκπαίδευση σε υποκείμενα δεδομένων στην Ένωση είναι εγκατεστημένο στο κράτος μέλος «Α». Το σχολείο επιθυμεί να πιστοποιήσει τη διαδικτυακή διαδικασία αιτήσεών του με ένα σύστημα πιστοποίησης που εφαρμόζεται σε όλη την ΕΕ για να αποκτήσει την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων. Το εν λόγω σχολείο στοχεύει να υποβάλει αίτηση για πιστοποίηση των πράξεων επεξεργασίας που εκτελούνται από φορέα πιστοποίησης εγκατεστημένο στο κράτος μέλος «Β» βάσει Ευρωπαϊκής Σφραγίδας Προστασίας των Δεδομένων. Τα κριτήρια της σφραγίδας που έχουν σχεδιαστεί και τεκμηριωθεί στον σχετικό μηχανισμό πρέπει να μπορούν να λάβουν υπόψη τους κανονισμούς για τα σχολεία που ισχύουν στο κράτος μέλος «Α». Τα κριτήρια θα πρέπει επίσης να απαιτούν η διαδικτυακή διαδικασία αιτήσεων του σχολείου να παρέχει πληροφορίες και να λαμβάνει υπόψη τις ισχύουσες απαιτήσεις του κράτους μέλους για την προστασία δεδομένων, οι οποίες μπορεί να είναι διαφορετικές σε άλλα κράτη μέλη. Για παράδειγμα, σύνολα προσωπικών δεδομένων προς υποβολή για σκοπούς αίτησης, π.χ. βαθμοί νηπιαγωγείου ή αποτελέσματα εξετάσεων, διαφορές ως προς τις περιόδους διατήρησης, τη συλλογή ή την επεξεργασία οικονομικών ή βιομετρικών δεδομένων, περαιτέρω περιορισμοί επεξεργασίας.

- Τα κριτήρια υψηλού επιπέδου για έγκριση μηχανισμού Ευρωπαϊκής Σφραγίδας Προστασίας των Δεδομένων περιλαμβάνουν:
    - τα κριτήρια που έχει εγκρίνει το Συμβούλιο Προστασίας Δεδομένων·
    - την εφαρμογή σε δικαιοδοσίες που αντανακλούν κατά περίπτωση εθνικές νομικές απαιτήσεις και τομεακούς κανονισμούς·
    -
- εναρμονισμένα κριτήρια που μπορούν να προσαρμοστούν για να αντανακλούν εθνικές απαιτήσεις·
    - περιγραφή του συγκεκριμένου μηχανισμού πιστοποίησης, όπου προσδιορίζονται:
    - οι συμβάσεις πιστοποίησης, αναγνωρίζοντας απαιτήσεις για ολόκληρη την Ευρώπη·
    - οι διαδικασίες διασφάλισης και παροχής λύσεων για εθνικές αποκλίσεις και διασφάλισης ότι η σφραγίδα βοηθά στην απόδειξη της συμμόρφωσης με τον ΓΚΠΔ· και
    - η γλώσσα των εκθέσεων που απευθύνονται σε όλες τις σχετικές εποπτικές αρχές.

42. Το παράρτημα περιέχει επίσης συμβουλές σχετικά με τα κριτήρια για την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων.

4.2.3 Ο ρόλος της διαπίστευσης

43. Όπως σημειώνεται στο τμήμα 4.2.1, όταν τα κριτήρια χαρακτηρίζονται ως κατάλληλα για κοινή πιστοποίηση και έχουν εγκριθεί ως τέτοια από το Συμβούλιο Προστασίας Δεδομένων σύμφωνα με το άρθρο 42 παράγραφος 5, τότε οι φορείς πιστοποίησης μπορούν να διαπιστευτούν για τη διενέργεια πιστοποίησης με βάση αυτά τα κριτήρια σε ενωσιακό επίπεδο.

44. Τα συστήματα που προορίζονται για να προσφέρονται μόνο σε συγκεκριμένα κράτη μέλη δεν θα είναι υποψήφια για τη σφραγίδα της ΕΕ. Για τη διαπίστευση για το πεδίο εφαρμογής της Ευρωπαϊκής Σφραγίδας Προστασίας των Δεδομένων θα απαιτείται διαπίστευση στο κράτος μέλος στο οποίο βρίσκονται τα κεντρικά γραφεία του φορέα πιστοποίησης που προτίθεται να χρησιμοποιήσει το σύστημα, δηλαδή που είναι υπεύθυνος για την έκδοση πιστοποιήσεων και τη διαχείριση των δραστηριοτήτων πιστοποίησης των οντοτήτων του και των θυγατρικών του σε άλλα κράτη μέλη. Σε περίπτωση που άλλες εγκαταστάσεις ή γραφεία διαχειρίζονται και εκτελούν πιστοποιήσεις αυτόνομα, καθεμία από αυτές τις εγκαταστάσεις ή τα γραφεία θα πρέπει να έχει χωριστή διαπίστευση στο κράτος μέλος όπου είναι εγκατεστημένη/-ο. Με άλλα λόγια, η διαπίστευση είναι απαραίτητη μόνο στο κράτος μέλος στο οποίο βρίσκονται τα κεντρικά γραφεία του φορέα πιστοποίησης μόνο σε περίπτωση που τα κεντρικά γραφεία εκδίδουν τα πιστοποιητικά. Αντιθέτως, όταν και άλλες εγκαταστάσεις του φορέα πιστοποίησης εκδίδουν πιστοποιητικά, αυτές οι εγκαταστάσεις πρέπει επίσης να είναι διαπιστευμένες.

45. Συνεπώς, αν ένας φορέας πιστοποίησης δεν έχει διαπιστευτεί για τη διενέργεια πιστοποίησης σύμφωνα με την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων, τα κριτήρια που έχουν εγκριθεί από το ΕΣΠΔ δεν μπορούν να χρησιμοποιηθούν και δεν είναι δυνατόν να χορηγηθεί η σφραγίδα.

5 Η ΘΕΣΠΙΣΗ ΚΡΙΤΗΡΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

46. Ο ΓΚΠΔ διαμόρφωσε το πλαίσιο για τη θέσπιση κριτηρίων πιστοποίησης. Ενώ οι βασικές απαιτήσεις σχετικά με τη διαδικασία της πιστοποίησης αναφέρονται στα άρθρα 42 και 43 παρέχοντας ταυτόχρονα βασικά κριτήρια για τις διαδικασίες πιστοποίησης, η βάση για τα κριτήρια πιστοποίησης πρέπει να προέρχεται από τις αρχές και τους κανόνες του ΓΚΠΔ και να βοηθά στην παροχή βεβαιότητας ότι τα κριτήρια αυτά πληρούνται.

47. Η θέσπιση κριτηρίων πιστοποίησης θα πρέπει να εστιάζει στην επαληθευσιμότητα, στη βαρύτητα και στην καταλληλότητα των κριτηρίων πιστοποίησης για την απόδειξη της συμμόρφωσης με τον κανονισμό. Τα κριτήρια πιστοποίησης θα πρέπει να διατυπώνονται κατά τρόπο ώστε να είναι σαφή και κατανοητά και να είναι δυνατή η πρακτική εφαρμογή τους.

48. Κατά τον σχεδιασμό των κριτηρίων πιστοποίησης, λαμβάνονται υπόψη, μεταξύ άλλων και κατά περίπτωση, οι παρακάτω πτυχές συμμόρφωσης για την υποστήριξη της αξιολόγησης της πράξης επεξεργασίας:

    - η νομιμότητα της επεξεργασίας σύμφωνα με το άρθρο 6,
    - οι αρχές της επεξεργασίας δεδομένων σύμφωνα με το άρθρο 5,
    - τα δικαιώματα των υποκειμένων των δεδομένων σύμφωνα με τα άρθρα 12-23,
    - η υποχρέωση γνωστοποίησης παραβίασης δεδομένων σύμφωνα με το άρθρο 33,
    - η υποχρέωση προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού σύμφωνα με το άρθρο 25,
    - το κατά πόσον έχει διενεργηθεί εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων, σύμφωνα με το άρθρο 35 παράγραφος 7 στοιχείο δ), κατά περίπτωση, και
    - τα τεχνικά και οργανωτικά μέτρα που έχουν τεθεί σε εφαρμογή σύμφωνα με το άρθρο 32.

49. Ο βαθμός στον οποίο αυτές οι πτυχές αντανακλώνται στα κριτήρια ενδέχεται να διαφέρει ανάλογα με το πεδίο εφαρμογής της πιστοποίησης, που μπορεί να περιλαμβάνει το είδος της πράξης ή των πράξεων επεξεργασίας και τον τομέα (π.χ. τομέας υγείας) της πιστοποίησης.

5.1 Τι μπορεί να πιστοποιηθεί σύμφωνα με τον ΓΚΠΔ;

50. Το ΕΣΠΔ λαμβάνει υπόψη το γεγονός ότι ο ΓΚΠΔ προβλέπει ευρύ πεδίο ως προς το τι μπορεί να πιστοποιηθεί σύμφωνα με τον ΓΚΠΔ, εφόσον δίνεται έμφαση στη βοήθεια για απόδειξη της συμμόρφωσης με τον εν λόγω κανονισμό των πράξεων επεξεργασίας που εκτελούν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία (άρθρο 42 παράγραφος 1).

51. Κατά την αξιολόγηση μιας πράξης επεξεργασίας, πρέπει να λαμβάνονται υπόψη τα παρακάτω τρία βασικά στοιχεία, κατά περίπτωση:

    1. τα προσωπικά δεδομένα (καθ' ύλην πεδίο εφαρμογής του ΓΚΠΔ)·
    2. τα τεχνικά συστήματα - οι υποδομές, όπως το υλισμικό και το λογισμικό, που χρησιμοποιούνται για την επεξεργασία των προσωπικών δεδομένων· και
    3. οι διαδικασίες που σχετίζονται με την πράξη ή τις πράξεις επεξεργασίας.

52. Κάθε στοιχείο που χρησιμοποιείται στις πράξεις επεξεργασίας πρέπει να υπόκειται σε αξιολόγηση έναντι των κριτηρίων που έχουν οριστεί. Τουλάχιστον τέσσερις διαφορετικοί σημαντικοί παράγοντες μπορεί να έχουν επίδραση: 1) η οργάνωση και το νομικό πλαίσιο του υπευθύνου επεξεργασίας ή του εκτελούντα την επεξεργασία· 2) το τμήμα, το περιβάλλον και τα πρόσωπα που εμπλέκονται στην πράξη ή τις πράξεις επεξεργασίας· 3) η τεχνική περιγραφή των στοιχείων προς αξιολόγηση· και τέλος 4) οι υποδομές ΤΠ που υποστηρίζουν την πράξη επεξεργασίας, περιλαμβανομένων λειτουργικών συστημάτων, εικονικών συστημάτων,

βάσεων δεδομένων, συστημάτων ελέγχου ταυτότητας και εξουσιοδότησης, δρομολογητών και τειχών προστασίας, συστημάτων αποθήκευσης, υποδομών επικοινωνίας ή πρόσβασης στο διαδίκτυο και σχετικών τεχνικών μέτρων.

53. Και τα τρία βασικά στοιχεία είναι σημαντικά για τον σχεδιασμό των διαδικασιών και των κριτηρίων πιστοποίησης. Ανάλογα με το αντικείμενο της πιστοποίησης, ο βαθμός στον οποίο λαμβάνονται υπόψη μπορεί να διαφέρει. Για παράδειγμα, σε ορισμένες περιπτώσεις, ορισμένα στοιχεία μπορούν να παραβλεφθούν αν κριθεί ότι δεν αφορούν το αντικείμενο της πιστοποίησης.

54. Για να προσδιορίσει περαιτέρω τι μπορεί να πιστοποιηθεί σύμφωνα με τον ΓΚΠΔ, ο ΓΚΠΔ περιέχει πρόσθετη καθοδήγηση. Από το άρθρο 42 παράγραφος 7 προκύπτει ότι οι πιστοποιήσεις σύμφωνα με τον ΓΚΠΔ χορηγούνται μόνο σε υπευθύνους επεξεργασίας δεδομένων και εκτελούντες επεξεργασία δεδομένων, με αποτέλεσμα να αποκλείεται, για παράδειγμα, η πιστοποίηση υπευθύνων προστασίας δεδομένων. Το άρθρο 43 παράγραφος 1 στοιχείο β) αναφέρει το πρότυπο ISO 17065 το οποίο προβλέπει τη διαπίστευση φορέων πιστοποίησης που αξιολογούν τη συμμόρφωση προϊόντων, υπηρεσιών και διαδικασιών. Μια πράξη ή μια σειρά πράξεων επεξεργασίας μπορεί να θέσει ένα προϊόν ή μια υπηρεσία εντός της ορολογίας του προτύπου ISO 17065 με συνέπεια το προϊόν ή η υπηρεσία να υπόκειται σε πιστοποίηση. Για παράδειγμα, η επεξεργασία δεδομένων υπαλλήλων για τον σκοπό της καταβολής μισθού ή της διαχείρισης της άδειας αποτελεί ένα σύνολο πράξεων κατά την έννοια του ΓΚΠΔ και μπορεί να θέσει ένα προϊόν, μια διαδικασία ή μια υπηρεσία εντός της ορολογίας του προτύπου ISO.

55. Με βάση αυτές τις παρατηρήσεις, το ΕΣΠΔ λαμβάνει υπόψη ότι το πεδίο εφαρμογής της πιστοποίησης σύμφωνα με τον ΓΚΠΔ στοχεύει σε πράξεις ή σειρές πράξεων επεξεργασίας. Σε αυτές μπορούν να συγκαταλέγονται διαδικασίες διακυβέρνησης ως οργανωτικά μέτρα, συνεπώς ως αναπόσπαστα μέρη μιας πράξης επεξεργασίας (π.χ. η διαδικασία διακυβέρνησης που έχει θεσπιστεί για τη διαχείριση καταγγελιών στο πλαίσιο της επεξεργασίας δεδομένων υπαλλήλων για τον σκοπό της καταβολής μισθού).

56. Προκειμένου να αξιολογηθεί η συμμόρφωση της πράξης επεξεργασίας με τα κριτήρια πιστοποίησης, πρέπει να δοθεί μια περίπτωση χρήσης. Για παράδειγμα, η συμμόρφωση της χρήσης τεχνικών υποδομών που αναπτύχθηκαν σε μια πράξη επεξεργασίας εξαρτάται από τις κατηγορίες δεδομένων που είναι σχεδιασμένες να επεξεργαστούν. Τα οργανωτικά μέτρα εξαρτώνται από τις κατηγορίες και την ποσότητα των δεδομένων και από τις τεχνικές υποδομές που χρησιμοποιούνται για την επεξεργασία, λαμβανομένων υπόψη της φύσης, του πεδίου εφαρμογής, του περιεχομένου και των σκοπών της επεξεργασίας, καθώς και των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

57. Επιπλέον, πρέπει να λαμβάνεται υπόψη ότι οι εφαρμογές ΤΠ μπορούν να διαφέρουν σημαντικά ακόμη και αν υπηρετούν τους ίδιους σκοπούς επεξεργασίας. Ως εκ τούτου, αυτό θα πρέπει να συνεκτιμάται κατά τον ορισμό του πεδίου εφαρμογής των μηχανισμών πιστοποίησης και κατά την κατάρτιση των κριτηρίων πιστοποίησης, δηλαδή το πεδίο εφαρμογής της πιστοποίησης και τα κριτήρια δεν θα πρέπει να είναι τόσο στενά ώστε να αποκλείουν εφαρμογές ΤΠ που έχουν σχεδιαστεί διαφορετικά.

5.2 Καθορισμός του αντικειμένου της πιστοποίησης

58. Το πεδίο εφαρμογής του μηχανισμού πιστοποίησης πρέπει να διακρίνεται από το αντικείμενο —που αποκαλείται και αντικείμενο αξιολόγησης— σε κάθε έργο πιστοποίησης που εκτελείται στο πλαίσιο μηχανισμού πιστοποίησης. Ο μηχανισμός πιστοποίησης μπορεί να ορίσει το πεδίο εφαρμογής του είτε γενικά είτε σε σχέση με ένα συγκεκριμένο είδος ή τομέα πράξεων επεξεργασίας και ως εκ τούτου μπορεί ήδη να προσδιορίσει τα αντικείμενα της πιστοποίησης που εμπίπτουν στο πεδίο εφαρμογής του μηχανισμού πιστοποίησης (π.χ. ασφαλής αποθήκευση και προστασία των προσωπικών δεδομένων που περιέχονται σε ψηφιακό θησαυροφυλάκιο). Σε κάθε περίπτωση, αξιόπιστη και ουσιαστική αξιολόγηση συμμόρφωσης μπορεί να γίνει μόνο αν κάθε αντικείμενο ενός έργου πιστοποίησης περιγραφεί με ακρίβεια. Πρέπει να περιγραφεί με σαφήνεια ποιες πράξεις επεξεργασίας περιλαμβάνονται στο αντικείμενο της πιστοποίησης και έπειτα να περιγραφούν τα βασικά στοιχεία, δηλαδή ποια δεδομένα, διαδικασίες και τεχνικές υποδομές θα αξιολογηθούν και ποια όχι. Σε αυτό το πλαίσιο, οι διεπαφές προς άλλες διαδικασίες πρέπει πάντα να λαμβάνονται υπόψη καθώς και να περιγράφονται. Είναι σαφές πως ό,τι δεν είναι γνωστό δεν μπορεί να αποτελεί μέρος της αξιολόγησης και ως εκ τούτου δεν μπορεί να πιστοποιηθεί. Σε κάθε περίπτωση, το επιμέρους αντικείμενο της πιστοποίησης πρέπει να είναι κατανοητό ως προς το μήνυμα ή τους ισχυρισμούς που διατυπώνεται/-νται στην/από την πιστοποίηση και δεν θα πρέπει να παραπλανά τον χρήστη, τον πελάτη ή τον καταναλωτή.

59. [Παράδειγμα 1]

Μια τράπεζα προσφέρει στους πελάτες της έναν ιστότοπο για τραπεζικές συναλλαγές μέσω διαδικτύου. Στο πλαίσιο αυτής της υπηρεσίας, υπάρχει η δυνατότητα εκτέλεσης εμβασμάτων, αγοράς μετοχών, εκτέλεσης πάγιων εντολών και διαχείρισης του λογαριασμού. Η τράπεζα επιθυμεί να πιστοποιήσει τα παρακάτω σύμφωνα με έναν μηχανισμό πιστοποίησης προστασίας δεδομένων με γενικό πεδίο εφαρμογής βάσει γενικών κριτηρίων:

α) Ασφαλής σύνδεση

Η ασφαλής σύνδεση είναι μια πράξη επεξεργασίας η οποία είναι κατανοητή στον τελικό χρήση και έχει σημασία από την άποψη της προστασίας δεδομένων καθώς παίζει σημαντικό ρόλο στη διασφάλιση της ασφάλειας των σχετικών προσωπικών δεδομένων. Ως εκ τούτου, αυτή η πράξη επεξεργασίας είναι απαραίτητη για την ασφαλή σύνδεση και μπορεί επομένως να αποτελεί εύλογο αντικείμενο αξιολόγησης αν το πιστοποιητικό αναφέρει σαφώς ότι πιστοποιείται μόνο η πράξη επεξεργασίας της σύνδεσης.

β) Κώδικας web front-end

Ενώ ο κώδικας web front-end μπορεί να έχει σημασία από την άποψη της προστασίας δεδομένων, δεν είναι κατανοητός από τον τελικό χρήστη και επομένως δεν μπορεί να αποτελεί εύλογο αντικείμενο αξιολόγησης. Επιπλέον, δεν είναι σαφές στον χρήστη ποιες υπηρεσίες στον ιστότοπο και επομένως ποιες πράξεις επεξεργασίας καλύπτονται από την πιστοποίηση.

γ) Τραπεζικές συναλλαγές μέσω διαδικτύου

Ο κώδικας web front-end μαζί με τον κώδικα back-end επεξεργάζονται πράξεις που προβλέπονται στο πλαίσιο της υπηρεσίας τραπεζικών συναλλαγών μέσω διαδικτύου και οι οποίες μπορούν να έχουν σημασία για τον χρήστη. Σε αυτό το πλαίσιο, και τα

δύο πρέπει να περιληφθούν στο αντικείμενο αξιολόγησης. Αντίθετα, πράξεις επεξεργασίας οι οποίες δεν συνδέονται άμεσα με την παροχή της υπηρεσίας τραπεζικών συναλλαγών μέσω διαδικτύου, όπως πράξεις επεξεργασίας για τον σκοπό της πρόληψης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, μπορούν να αποκλειστούν από το αντικείμενο της αξιολόγησης.

Παρ' όλα αυτά, οι υπηρεσίες τραπεζικών συναλλαγών μέσω διαδικτύου που προσφέρει η τράπεζα μέσω του ιστότοπού της μπορούν να περιλαμβάνουν και άλλες υπηρεσίες οι οποίες με τη σειρά τους να απαιτούν τις δικές τους πράξεις επεξεργασίας. Σε αυτό το πλαίσιο, στις άλλες υπηρεσίες μπορεί να περιλαμβάνεται, για παράδειγμα, η προσφορά ενός ασφαλιστικού προϊόντος. Επειδή αυτή η πρόσθετη υπηρεσία δεν συνδέεται άμεσα με τον σκοπό της παροχής υπηρεσιών τραπεζικών συναλλαγών μέσω διαδικτύου, μπορεί να αποκλειστεί από το αντικείμενο αξιολόγησης. Αν αυτή η πρόσθετη υπηρεσία (ασφάλεια) αποκλειστεί από το αντικείμενο αξιολόγησης, οι διεπαφές για αυτή την υπηρεσία που είναι ενσωματωμένες στον ιστότοπο αποτελούν μέρος του αντικειμένου αξιολόγησης και πρέπει επομένως να περιγραφούν προκειμένου να υπάρχει σαφής διάκριση των υπηρεσιών. Η περιγραφή αυτή είναι απαραίτητη προκειμένου να προσδιοριστούν και να αξιολογηθούν πιθανές ροές δεδομένων μεταξύ των δύο υπηρεσιών.

60. [Παράδειγμα 2]

Μια τράπεζα προσφέρει στους πελάτες της μια υπηρεσία που τους δίνει τη δυνατότητα να συγκεντρώσουν πληροφορίες που αφορούν διαφορετικούς λογαριασμούς και πιστωτικές κάρτες από διάφορες τράπεζες (συνολικοί λογαριασμοί). Η τράπεζα επιθυμεί να πιστοποιήσει την υπηρεσία της σύμφωνα με τον ΓΚΠΔ. Η αρμόδια εποπτική αρχή έχει εγκρίνει ένα συγκεκριμένο σύνολο κριτηρίων πιστοποίησης που εστιάζει σε αυτό το είδος δραστηριότητας. Το πεδίο εφαρμογής του μηχανισμού πιστοποίησης περιλαμβάνει μόνο τις παρακάτω πτυχές συμμόρφωσης:

- επαλήθευση ταυτότητας χρήστη· και
- αποδεκτοί τρόποι απόκτησης των δεδομένων προς συγκέντρωση από άλλες τράπεζες/υπηρεσίες.

Επειδή το ίδιο το πεδίο εφαρμογής του συγκεκριμένου μηχανισμού πιστοποίησης ορίζει το αντικείμενο αξιολόγησης, δεν είναι δυνατό να περιοριστεί ουσιαστικά το αντικείμενο αξιολόγησης σύμφωνα με το προτεινόμενο πεδίο εφαρμογής και να πιστοποιηθούν συγκεκριμένα μόνο χαρακτηριστικά ή μία δραστηριότητα επεξεργασίας. Σε αυτό το σενάριο, το αντικείμενο αξιολόγησης πρέπει να ταυτίζεται με το συγκεκριμένο πεδίο εφαρμογής.

5.3 Μέθοδοι αξιολόγησης και μεθοδολογία της αξιολόγησης

61. Η αξιολόγηση συμμόρφωσης που θα βοηθήσει στην απόδειξη της συμμόρφωσης πράξεων επεξεργασίας απαιτεί να προσδιοριστούν και να καθοριστούν οι μέθοδοι αξιολόγησης και η μεθοδολογία της αξιολόγησης. Έχει σημασία αν οι πληροφορίες για την αξιολόγηση συλλέγονται μόνο από έγγραφα (το οποίο δεν θα ήταν αρκετό από μόνο του) ή αν συλλέγονται ενεργά επιτόπου και με άμεση ή έμμεση πρόσβαση. Ο τρόπος με τον οποίο

συλλέγονται οι πληροφορίες έχει συνέπειες για τη σημασία της πιστοποίησης και θα πρέπει επομένως να ορίζεται και να περιγράφεται.

Οι διαδικασίες για την έκδοση και την περιοδική επανεξέταση των πιστοποιήσεων θα πρέπει να περιλαμβάνουν προδιαγραφές για τον προσδιορισμό του κατάλληλου επιπέδου αξιολόγησης (βάθος και βαθμός λεπτομέρειας δεδομένων) για την εκπλήρωση των κριτηρίων πιστοποίησης και θα πρέπει να παρέχουν τα παρακάτω στοιχεία:

- πληροφορίες και λεπτομέρειες για τις μεθόδους αξιολόγησης που εφαρμόστηκαν και τα συμπεράσματα που συλλέχθηκαν π.χ. κατά τη διάρκεια επιτόπιων ελέγχων ή από έγγραφα,
- τις μεθόδους αξιολόγησης που εστιάζουν στις πράξεις επεξεργασίας (δεδομένα, συστήματα, διαδικασίες) και στον σκοπό της επεξεργασίας,
- προσδιορισμό των κατηγοριών δεδομένων, των αναγκών προστασίας και της πιθανής εμπλοκής εκτελούντων επεξεργασία ή τρίτων μερών,
- προσδιορισμό των ρόλων και ύπαρξη μηχανισμού ελέγχου της πρόσβασης που καθορίζει ρόλους και αρμοδιότητες.

62. Το βάθος της αξιολόγησης έχει αντίκτυπο στη σημασία και στην αξία της πιστοποίησης. Η μείωση του βάθους της αξιολόγησης για πρακτικούς σκοπούς ή για περιορισμό του κόστους θα μειώσει τη σημασία της πιστοποίησης της προστασίας δεδομένων. Οι αποφάσεις για τον βαθμό λεπτομέρειας των δεδομένων της αξιολόγησης, από την άλλη πλευρά, μπορεί να υπερβούν τις οικονομικές δυνατότητες του αιτούντα και συχνά τις δυνατότητες και των αξιολογητών και των ελεγκτών. Για τους σκοπούς της απόδειξης της συμμόρφωσης ίσως να μην είναι πάντα καθοριστικής σημασίας να επιτευχθεί πολύ λεπτομερής ανάλυση των συστημάτων ΤΠ που χρησιμοποιούνται, έτσι ώστε να διατηρηθεί η ουσία.

5.4 Τεκμηρίωση της αξιολόγησης

63. Η τεκμηρίωση της πιστοποίησης θα πρέπει να είναι διεξοδική και πλήρης. Έλλειψη τεκμηρίωσης σημαίνει ότι δεν μπορεί να πραγματοποιηθεί σωστή αξιολόγηση. Η ουσιαστική λειτουργία της τεκμηρίωσης της πιστοποίησης είναι η παροχή διαφάνειας στη διαδικασία αξιολόγησης σύμφωνα με τον μηχανισμό πιστοποίησης. Η τεκμηρίωση δίνει απαντήσεις σε ερωτήσεις που αφορούν τις απαιτήσεις που ορίζει η νομοθεσία. Οι μηχανισμοί πιστοποίησης θα πρέπει να προβλέπουν μια τυποποιημένη μεθοδολογία τεκμηρίωσης. Η μετέπειτα αξιολόγηση θα δώσει δυνατότητα σύγκρισης της τεκμηρίωσης της πιστοποίησης με την πραγματική κατάσταση επιτόπου και έναντι των κριτηρίων πιστοποίησης.

64. Η πλήρης τεκμηρίωση του τι έχει πιστοποιηθεί και της μεθοδολογίας που χρησιμοποιήθηκε βελτιώνει τη διαφάνεια. Σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο γ), οι μηχανισμοί πιστοποίησης θα πρέπει να θεσπίζουν διαδικασίες που δίνουν τη δυνατότητα επανεξέτασης των πιστοποιήσεων. Προκειμένου να μπορεί η εποπτική αρχή να αξιολογεί αν και σε ποιο βαθμό μπορεί να αναγνωριστεί η πιστοποίηση σε επίσημες έρευνες, η λεπτομερής τεκμηρίωση ίσως είναι το πιο κατάλληλο μέσο επικοινωνίας. Επομένως, η τεκμηρίωση που παράγεται κατά τη διάρκεια της αξιολόγησης θα πρέπει να εστιάζει σε τρεις κύριες πτυχές:

- στη συνεκτικότητα και στη συνοχή των μεθόδων αξιολόγησης που εφαρμόζονται·

- στις μεθόδους αξιολόγησης που στοχεύουν στην απόδειξη της συμμόρφωσης του αντικειμένου της αξιολόγησης με τα κριτήρια πιστοποίησης και ως εκ τούτου με τον κανονισμό· και
- στο ότι τα αποτελέσματα της αξιολόγησης έχουν επικυρωθεί από ανεξάρτητο και αμερόληπτο φορέα πιστοποίησης.

5.5 Τεκμηρίωση των αποτελεσμάτων

65. Η αιτιολογική σκέψη 100 παρέχει πληροφορίες για τους στόχους που επιδιώκονται με την εισαγωγή της πιστοποίησης.

«Για τη βελτίωση της διαφάνειας και της συμμόρφωσης προς τον παρόντα κανονισμό, θα πρέπει να ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης και σφραγίδων και σημάτων προστασίας των δεδομένων, επιτρέποντας στα υποκείμενα των δεδομένων να αξιολογούν ταχέως το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων και υπηρεσιών.»

66. Η τεκμηρίωση και η ανακοίνωση των αποτελεσμάτων παίζουν σημαντικό ρόλο στη βελτίωση της διαφάνειας. Οι φορείς πιστοποίησης που χρησιμοποιούν μηχανισμούς πιστοποίησης, σφραγίδες ή σήματα που στοχεύουν στα υποκείμενα των δεδομένων (με την ιδιότητά τους ως καταναλωτών ή πελατών) θα πρέπει να παρέχουν ευχερώς προσβάσιμες, κατανοητές και ουσιαστικές πληροφορίες σχετικά με την πιστοποιημένη πράξη ή τις πράξεις επεξεργασίας. Οι εν λόγω δημόσιες πληροφορίες θα πρέπει να περιλαμβάνουν τουλάχιστον τα εξής:
    - περιγραφή του αντικειμένου αξιολόγησης·
    - αναφορά στα εγκεκριμένα κριτήρια που εφαρμόστηκαν στο συγκεκριμένο αντικείμενο αξιολόγησης·
    - μεθοδολογία για την αξιολόγηση των κριτηρίων (επιτόπου αξιολόγηση, τεκμηρίωση, κ.λπ.)· και
    - διάρκεια ισχύος του πιστοποιητικού· και
    - θα πρέπει να δίνουν στις εποπτικές αρχές και στο κοινό δυνατότητα σύγκρισης των αποτελεσμάτων.

6 ΚΑΘΟΔΗΓΗΣΗ ΓΙΑ ΤΟΝ ΟΡΙΣΜΟ ΚΡΙΤΗΡΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

67. Τα κριτήρια πιστοποίησης αποτελούν αναπόσπαστο μέρος του μηχανισμού πιστοποίησης. Η διαδικασία πιστοποίησης περιλαμβάνει τις απαιτήσεις ως προς το πώς, από ποιον, σε ποιον βαθμό και με ποιον βαθμό λεπτομέρειας των δεδομένων διενεργείται η αξιολόγηση των επιμέρους έργων πιστοποίησης σχετικά με ένα συγκεκριμένο αντικείμενο ή αντικείμενο αξιολόγησης. Τα κριτήρια πιστοποίησης παρέχουν τις ονομαστικές απαιτήσεις έναντι των οποίων αξιολογείται η πραγματική πράξη επεξεργασίας που ορίζεται στο αντικείμενο

αξιολόγησης. Οι παρούσες κατευθυντήριες γραμμές για τον ορισμό των κριτηρίων πιστοποίησης παρέχουν γενικές συμβουλές που θα διευκολύνουν την αξιολόγηση των κριτηρίων πιστοποίησης για τον σκοπό της έγκρισης.

- Κατά την έγκριση ή τον ορισμό κριτηρίων πιστοποίησης θα πρέπει να λαμβάνονται υπόψη οι παρακάτω γενικές πτυχές. Τα κριτήρια πιστοποίησης θα πρέπει:
- να είναι ομοιόμορφα και επαληθεύσιμα·
- να είναι ελέγξιμα, προκειμένου να διευκολυνθεί η αξιολόγηση των πράξεων επεξεργασίας σύμφωνα με τον ΓΚΠΔ, προσδιορίζοντας, συγκεκριμένα, τους στόχους και τις κατευθυντήριες γραμμές εφαρμογής για την επίτευξη αυτών των στόχων·
- να είναι σχετικά με το στοχευόμενο κοινό (π.χ. μεταξύ επιχειρήσεων και από επιχείρηση προς καταναλωτή)·
- να λαμβάνουν υπόψη και κατά περίπτωση να είναι διαλειτουργικά με άλλα πρότυπα (όπως πρότυπα ISO, πρότυπα που ισχύουν σε εθνικό επίπεδο)· και
- να είναι ευέλικτα και κλιμακούμενα ώστε να εφαρμόζονται σε διαφορετικά είδη και μεγέθη οργανισμών, περιλαμβανομένων πολύ μικρών, μικρών και μεσαίων επιχειρήσεων σύμφωνα με το άρθρο 42 παράγραφος 1 και να αντικατοπτρίζουν την προσέγγιση προσδιορισμού του κινδύνου σύμφωνα με την αιτιολογική σκέψη 77.

68. Μια μικρή τοπική εταιρεία, όπως μια επιχείρηση λιανικού εμπορίου, θα πραγματοποιεί συνήθως λιγότερο περίπλοκες πράξεις επεξεργασίας από μια μεγάλη πολυεθνική επιχείρηση λιανικού εμπορίου. Ενώ οι απαιτήσεις για τη νομιμότητα των πράξεων επεξεργασίας είναι οι ίδιες, πρέπει να ληφθούν υπόψη το πεδίο εφαρμογής της επεξεργασίας των δεδομένων και η περιπλοκότητά του· συνεπώς υπάρχει ανάγκη για μηχανισμούς πιστοποίησης με κλιμακούμενα κριτήρια ανάλογα με την υπό εξέταση δραστηριότητα επεξεργασίας.

6.1 Υφιστάμενα πρότυπα

69. Οι φορείς πιστοποίησης θα χρειαστεί να εξετάσουν πώς συγκεκριμένα κριτήρια λαμβάνουν υπόψη τα υφιστάμενα σχετικά μέσα, όπως κώδικες δεοντολογίας, τεχνικά πρότυπα ή εθνικές κανονιστικές και νομοθετικές πρωτοβουλίες. Ιδανικά, τα κριτήρια θα είναι διαλειτουργικά με τα υφιστάμενα πρότυπα που μπορούν να βοηθήσουν τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία να εκπληρώσουν τις υποχρεώσεις τους σύμφωνα με τον ΓΚΠΔ. Ωστόσο, ενώ τα βιομηχανικά πρότυπα εστιάζουν συχνά στην προστασία και στην ασφάλεια του οργανισμού έναντι απειλών, ο ΓΚΠΔ στοχεύει στην προστασία των θεμελιωδών δικαιωμάτων των φυσικών προσώπων. Αυτή η διαφορετική οπτική πρέπει να ληφθεί υπόψη κατά τον σχεδιασμό κριτηρίων ή την έγκριση κριτηρίων ή μηχανισμών πιστοποίησης βάσει βιομηχανικών προτύπων.

6.2 Καθορισμός κριτηρίων

70. Τα κριτήρια πιστοποίησης πρέπει να αντιστοιχούν στη δήλωση πιστοποίησης (μήνυμα ή ισχυρισμό) του μηχανισμού ή του συστήματος πιστοποίησης και να ανταποκρίνονται στις προσδοκίες που εγείρουν. Το όνομα του μηχανισμού πιστοποίησης μπορεί να προσδιορίζει ήδη το πεδίο εφαρμογής και θα έχει συνέπειες στον καθορισμό των κριτηρίων.

71. [Παράδειγμα 3]

    Ένας μηχανισμός που ονομάζεται «HealthPrivacyMark» θα πρέπει να περιορίζει το πεδίο εφαρμογής του στον τομέα της υγείας. Το όνομα της σφραγίδας εγείρει την προσδοκία ότι έχουν εξεταστεί οι απαιτήσεις προστασίας δεδομένων αναφορικά με τα δεδομένα για την υγεία. Ως εκ τούτου, τα κριτήρια αυτού του μηχανισμού πρέπει να είναι κατάλληλα για την αξιολόγηση των απαιτήσεων προστασίας δεδομένων σε αυτό τον τομέα.

72. [Παράδειγμα 4]

    Ένας μηχανισμός που σχετίζεται με την πιστοποίηση πράξεων επεξεργασίας που περιλαμβάνουν συστήματα διακυβέρνησης στην επεξεργασία δεδομένων θα πρέπει να προσδιορίζει κριτήρια που δίνουν τη δυνατότητα να αναγνωριστούν και να αξιολογηθούν οι διαδικασίες διακυβέρνησης και τα τεχνικά και οργανωτικά μέτρα υποστήριξής της.

73. [Παράδειγμα 5]

    Τα κριτήρια για έναν μηχανισμό ο οποίος σχετίζεται με τη χρήση υπολογιστών σε cloud πρέπει να λαμβάνουν υπόψη τις ιδιαίτερες τεχνικές απαιτήσεις που είναι απαραίτητες για τη χρήση υπηρεσιών που βασίζονται στο cloud. Για παράδειγμα, αν οι διακομιστές χρησιμοποιούνται εκτός της ΕΕ, τα κριτήρια πρέπει να λαμβάνουν υπόψη τις προϋποθέσεις που θεσπίζονται στο κεφάλαιο V του ΓΚΠΔ αναφορικά με τις διαβιβάσεις δεδομένων προς τρίτες χώρες.

74. Τα κριτήρια που έχουν σχεδιαστεί για να αντιστοιχούν σε διαφορετικά αντικείμενα αξιολόγησης σε διάφορους τομείς και/ή κράτη μέλη θα πρέπει: να καθιστούν δυνατή την εφαρμογή σε διαφορετικά σενάρια· να καθιστούν δυνατό τον προσδιορισμό των κατάλληλων μέτρων που αντιστοιχούν σε μικρές, μεσαίες ή μεγάλες πράξεις επεξεργασίας και να αντανακλούν τους κινδύνους διαφορετικής πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων σύμφωνα με τον ΓΚΠΔ. Συνεπώς, οι διαδικασίες πιστοποίησης (π.χ. για τεκμηρίωση, εξέταση ή μέθοδο αξιολόγησης και βάθος) που ενσωματώνουν τα κριτήρια πρέπει να ανταποκρίνονται σε αυτές τις ανάγκες και, να καθιστούν δυνατό τον καθορισμό και την εφαρμογή κανόνων, για παράδειγμα για την εφαρμογή των σχετικών κριτηρίων σε μεμονωμένα έργα πιστοποίησης. Τα κριτήρια πρέπει να διευκολύνουν την αξιολόγηση ως προς το αν έχουν παρασχεθεί επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων.

6.3 Διάρκεια ζωής των κριτηρίων πιστοποίησης

75. Παρόλο που τα κριτήρια πιστοποίησης πρέπει να είναι αξιόπιστα μέσα στο χρόνο, δεν θα πρέπει να παραμένουν αναλλοίωτα. Αποτελούν αντικείμενο αναθεώρησης για παράδειγμα όταν:

    - τροποποιείται το νομικό πλαίσιο·

- οι όροι και οι διατάξεις ερμηνεύονται από αποφάσεις του Ευρωπαϊκού Δικαστηρίου· ή
- έχει εξελιχθεί η τεχνολογία.

Για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η Πρόεδρος

(Andrea Jelinek)

ΠΑΡΑΡΤΗΜΑ: ΚΑΘΗΚΟΝΤΑ ΚΑΙ ΕΞΟΥΣΙΕΣ ΤΩΝ ΕΠΟΠΤΙΚΩΝ ΑΡΧΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΙΣΤΟΠΟΙΗΣΗ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΓΚΠΔ

	Διατάξεις	Απαιτήσεις
Καθήκοντα	Άρθρο 43 παράγραφος 6	Απαιτεί από την εποπτική αρχή να δημοσιοποιεί τα κριτήρια που αναφέρονται στο άρθρο 42 παράγραφος 5 σε ευχερώς προσβάσιμη μορφή και να τα διαβιβάζει στο Συμβούλιο Προστασίας Δεδομένων.
	Άρθρο 57 παράγραφος 1 στοιχείο ιδ)	Απαιτεί από την εποπτική αρχή να εγκρίνει κριτήρια πιστοποίησης σύμφωνα με το άρθρο 42 παράγραφος 5.
	Άρθρο 57 παράγραφος 1 στοιχείο ιε)	Προβλέπει ότι κατά περίπτωση (δηλαδή όταν εκδίδει πιστοποίηση), η εποπτική αρχή διενεργεί περιοδική επανεξέταση των πιστοποιήσεων που εκδίδονται σύμφωνα με το άρθρο 42 παράγραφος 7.
	Άρθρο 64 παράγραφος 1 στοιχείο γ)	Απαιτεί από την εποπτική αρχή να ανακοινώνει το σχέδιο απόφασης στο Συμβούλιο Προστασίας Δεδομένων, όταν αποσκοπεί στην έγκριση των κριτηρίων πιστοποίησης που αναφέρονται στο άρθρο 42 παράγραφος 5.
Εξουσίες	Άρθρο 58 παράγραφος 1 στοιχείο γ)	Προβλέπει ότι η εποπτική αρχή διαθέτει την εξουσία να προβαίνει σε επανεξετάσεις της πιστοποίησης σύμφωνα με το άρθρο 42 παράγραφος 7.
	Άρθρο 58 παράγραφος 2 στοιχείο η)	Προβλέπει ότι η εποπτική αρχή διαθέτει την εξουσία να αποσύρει την πιστοποίηση ή να διατάξει τον φορέα πιστοποίησης να αποσύρει ένα πιστοποιητικό ή να διατάξει τον φορέα πιστοποίησης να μην εκδώσει πιστοποίηση.
	Άρθρο 58 παράγραφος 3 στοιχείο ε)	Προβλέπει ότι η εποπτική αρχή διαθέτει την εξουσία να παρέχει διαπίστευση σε φορείς πιστοποίησης.
	Άρθρο 58 παράγραφος 3 στοιχείο στ)	Προβλέπει ότι η εποπτική αρχή διαθέτει την εξουσία να εκδίδει πιστοποιητικά και να εγκρίνει κριτήρια πιστοποίησης.

ΠΑΡΑΡΤΗΜΑ 2

1 ΕΙΣΑΓΩΓΗ

Στο παράρτημα 2 παρέχεται καθοδήγηση για την επανεξέταση και την αξιολόγηση των κριτηρίων πιστοποίησης σύμφωνα με το άρθρο 42 παράγραφος 5. Προσδιορίζονται θέματα τα οποία η εποπτική αρχή προστασίας δεδομένων και το ΕΣΠΔ θα εξετάσουν και θα εφαρμόσουν για τον σκοπό της έγκρισης των κριτηρίων πιστοποίησης ενός μηχανισμού πιστοποίησης. Οι ερωτήσεις θα πρέπει να λαμβάνονται υπόψη από τους οργανισμούς πιστοποίησης και τους ιδιοκτήτες των συστημάτων που επιθυμούν να καταρτίσουν και να υποβάλουν κριτήρια προς έγκριση. Ο κατάλογος δεν είναι εξαντλητικός, αλλά παρουσιάζει τα βασικά θέματα που πρόκειται να εξεταστούν. Δεν είναι συναφείς όλες οι ερωτήσεις· ωστόσο, θα πρέπει να λαμβάνονται υπόψη κατά την κατάρτιση κριτηρίων, ενώ ενδέχεται να είναι αναγκαία η αιτιολόγηση για την εξήγηση των λόγων για τους οποίους τα κριτήρια δεν καλύπτουν συγκεκριμένες πτυχές. Ορισμένες ερωτήσεις επαναλαμβάνονται, καθώς υποβάλλονται από διαφορετικές οπτικές γωνίες. Η εν λόγω καθοδήγηση θα πρέπει να λαμβάνεται υπόψη σύμφωνα με τις νομικές απαιτήσεις που προβλέπονται από τον ΓΚΠΔ και, κατά περίπτωση, από την εθνική νομοθεσία.

2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΜΗΧΑΝΙΣΜΟΥ ΠΙΣΤΟΠΟΙΗΣΗΣ ΚΑΙ ΣΤΟΧΟΣ ΤΗΣ ΑΞΙΟΛΟΓΗΣΗΣ

α) Περιγράφεται με σαφήνεια το πεδίο εφαρμογής του μηχανισμού πιστοποίησης (για τον οποίο θα χρησιμοποιούνται τα κριτήρια προστασίας των δεδομένων);

β) Είναι το πεδίο εφαρμογής του μηχανισμού πιστοποίησης χρήσιμο, και όχι παραπλανητικό, για το κοινό στο οποίο απευθύνεται;

- *Παράδειγμα: Η «σφραγίδα εμπιστοσύνης» της εταιρείας («Trusted Company Seal») υποδηλώνει ότι οι δραστηριότητες επεξεργασίας μιας ολόκληρης εταιρείας έχουν ελεγχθεί, παρόλο που μόνο συγκεκριμένες εργασίες επεξεργασίας, π.χ. η διαδικασία ηλεκτρονικής πληρωμής, υπόκεινται πράγματι σε πιστοποίηση. Ως εκ τούτου, το πεδίο εφαρμογής είναι παραπλανητικό.*

γ) Αντικατοπτρίζονται στο πεδίο εφαρμογής του μηχανισμού πιστοποίησης όλες οι σχετικές πτυχές των πράξεων επεξεργασίας;

- *Παράδειγμα: Ένα «σήμα προστασίας των δεδομένων υγείας» πρέπει να περιλαμβάνει όλα τα δεδομένα αξιολόγησης που αφορούν την υγεία με σκοπό την κάλυψη των απαιτήσεων σύμφωνα με το άρθρο 9.*

δ) Επιτρέπει το πεδίο εφαρμογής του μηχανισμού πιστοποίησης την ουσιαστική πιστοποίηση της προστασίας των δεδομένων, λαμβανομένων υπόψη της φύσης, του περιεχομένου, του κινδύνου των σχετικών πράξεων επεξεργασίας;

- *Παράδειγμα: Αν το πεδίο εφαρμογής του μηχανισμού πιστοποίησης επικεντρώνεται μόνο σε συγκεκριμένες πτυχές των πράξεων επεξεργασίας, όπως η συλλογή δεδομένων, αλλά όχι στις πράξεις περαιτέρω επεξεργασίας, όπως η επεξεργασία με σκοπό τη δημιουργία διαφημιστικών προφίλ ή η διαχείριση των δικαιωμάτων του υποκειμένου των δεδομένων, τότε η προστασία των υποκειμένων των δεδομένων δεν θα είναι ουσιαστική.*

ε) Καλύπτει το πεδίο εφαρμογής του μηχανισμού πιστοποίησης την επεξεργασία δεδομένων προσωπικού χαρακτήρα στη σχετική χώρα εφαρμογής ή καλύπτει τη διασυνοριακή επεξεργασία και/ή διαβιβάσεις δεδομένων;

στ) Περιγράφεται επαρκώς στα κριτήρια πιστοποίησης ο τρόπος με τον οποίο θα πρέπει να καθορίζεται ο στόχος της αξιολόγησης;

- *Παράδειγμα: Μια «σφραγίδα ιδιωτικότητας» που παρέχει μόνο γενικό πεδίο εφαρμογής και απαιτεί μόνο «προδιαγραφές της επεξεργασίας που υπόκειται σε πιστοποίηση» δεν θα παρέχει επαρκώς σαφή καθοδήγηση σχετικά με τον τρόπο καθορισμού και περιγραφής ενός στόχου της αξιολόγησης.*
- *Παράδειγμα: Ένα (ειδικό) πεδίο εφαρμογής, «η σφραγίδα ψηφιακού θησαυροφυλακίου ιδιωτικότητας», που έχει σκοπό την ασφαλή αποθήκευση, θα πρέπει να περιγράφει λεπτομερώς τις απαιτήσεις για την κάλυψη αυτού του πεδίου εφαρμογής στα κριτήριά του, π.χ. τον ορισμό του ψηφιακού θησαυροφυλακίου, τις απαιτήσεις του συστήματος, τα υποχρεωτικά τεχνικά και οργανωτικά μέτρα (ΤΟΜ). Στην περίπτωση αυτή, το πεδίο εφαρμογής μπορεί να ορίζει σαφώς τον στόχο της αξιολόγησης.*

    1) Απαιτούν τα κριτήρια να περιλαμβάνονται στον στόχο της αξιολόγησης ταυτοποίηση όλων των σχετικών πράξεων επεξεργασίας, απεικόνιση των ροών δεδομένων και προσδιορισμός του τομέα εφαρμογής του στόχου της αξιολόγησης;

        - *Παράδειγμα: Ένας μηχανισμός πιστοποίησης παρέχει πιστοποίηση των πράξεων επεξεργασίας των υπευθύνων επεξεργασίας στο πλαίσιο του ΓΚΠΔ χωρίς να προσδιορίζει περαιτέρω τον τομέα εφαρμογής (γενικό πεδίο εφαρμογής). Τα κριτήρια που χρησιμοποιούνται από τον μηχανισμό απαιτούν από τον αιτούντα υπεύθυνο επεξεργασίας να προσδιορίσει τη στοχευόμενη πράξη επεξεργασίας (στόχος της αξιολόγησης) από την άποψη των ειδών δεδομένων, των συστημάτων και των εφαρμοζόμενων διαδικασιών.*

    2) Απαιτούν τα κριτήρια από τον αιτούντα να καθιστά σαφές πού αρχίζει και πού τελειώνει η επεξεργασία που υπόκειται σε αξιολόγηση; Απαιτούν τα κριτήρια να περιλαμβάνονται στον στόχο της αξιολόγησης διεπαφές όπου οι αλληλεξαρτώμενες πράξεις επεξεργασίας δεν περιλαμβάνονται ως μέρος του στόχου της αξιολόγησης; Αιτιολογείται η απαίτηση αυτή ικανοποιητικά;

        - *Παράδειγμα: Ένας στόχος της αξιολόγησης που περιγράφει με επαρκείς λεπτομέρειες την πράξη επεξεργασίας μιας υπηρεσίας που βασίζεται στο διαδίκτυο, αναφέροντας ότι περιλαμβάνεται η καταχώριση των χρηστών, η παροχή υπηρεσιών, η τιμολόγηση, η καταγραφή διευθύνσεων IP, οι διεπαφές με χρήστες και τρίτους, και ότι δεν περιλαμβάνεται ο διακομιστής φιλοξενίας (αλλά περιλαμβάνονται οι συμφωνίες επεξεργασίας και ΤΟΜ).*

ζ) Εγγυώνται τα κριτήρια ότι οι (επιμέρους) στόχοι της αξιολόγησης είναι κατανοητοί στο κοινό στο οποίο απευθύνονται, συμπεριλαμβανομένων των υποκειμένων των δεδομένων, κατά περίπτωση;

3 ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

α) Προσδιορίζονται, επεξηγούνται και περιγράφονται όλοι οι σχετικοί όροι που χρησιμοποιούνται στον κατάλογο κριτηρίων (δηλαδή το σύνολο των κριτηρίων πιστοποίησης);

β) Προσδιορίζονται όλες οι κανονιστικές παραπομπές;

γ) Περιλαμβάνουν τα κριτήρια τον ορισμό των αρμοδιοτήτων, των διαδικασιών και της επεξεργασίας για την προστασία των δεδομένων που καλύπτονται από το πεδίο εφαρμογής του μηχανισμού πιστοποίησης;

4 ΠΡΑΞΗ ΕΠΕΞΕΡΓΑΣΙΑΣ, ΑΡΘΡΟ 42 ΠΑΡΑΓΡΑΦΟΣ 1

Όσον αφορά το πεδίο εφαρμογής του μηχανισμού πιστοποίησης (γενικό ή ειδικό), καλύπτουν τα κριτήρια όλα τα σχετικά στοιχεία των πράξεων επεξεργασίας (δεδομένα, συστήματα και διαδικασίες);

α) Απαιτούν τα κριτήρια προσδιορισμό των έγκυρων νομικών βάσεων της επεξεργασίας σε σχέση με τον στόχο της αξιολόγησης;

β) Όσον αφορά τον στόχο της αξιολόγησης, αναγνωρίζουν τα κριτήρια τα σχετικά στάδια της επεξεργασίας και τον πλήρη κύκλο ζωής των δεδομένων, συμπεριλαμβανομένης της διαγραφής ή/και της ανωνυμοποίησης;

γ) Όσον αφορά τον στόχο της αξιολόγησης, απαιτούν τα κριτήρια τη φορητότητα των δεδομένων;

δ) Όσον αφορά τον στόχο της αξιολόγησης, επιτρέπουν τα κριτήρια τον εντοπισμό και την αποτύπωση ειδικών τύπων πράξεων επεξεργασίας, π.χ. της αυτοματοποιημένης λήψης αποφάσεων ή της κατάρτισης προφίλ;

ε) Όσον αφορά τον στόχο της αξιολόγησης, επιτρέπουν τα κριτήρια τον προσδιορισμό ειδικών κατηγοριών δεδομένων;

στ) Επιτρέπουν, και απαιτούν, τα κριτήρια αξιολόγηση του κινδύνου των επιμέρους πράξεων επεξεργασίας και των αναγκών προστασίας των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων;

ζ) Επιτρέπουν, και απαιτούν, τα κριτήρια να λαμβάνονται επαρκώς υπόψη οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων;

...

5 ΝΟΜΙΜΟΤΗΤΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

α) Απαιτούν τα κριτήρια έλεγχο της νομιμότητας της επεξεργασίας για επιμέρους πράξεις επεξεργασίας όσον αφορά τον σκοπό και την αναγκαιότητα της επεξεργασίας;

β) Απαιτούν τα κριτήρια τον έλεγχο όλων των απαιτήσεων μιας νομικής βάσης για επιμέρους πράξεις επεξεργασίας;

6 ΑΡΧΕΣ, ΑΡΘΡΟ 5

α) Καλύπτουν τα κριτήρια επαρκώς όλες τις αρχές προστασίας των δεδομένων σύμφωνα με το άρθρο 5;

β) Απαιτούν τα κριτήρια να αποδεικνύεται η ελαχιστοποίηση των δεδομένων για τον επιμέρους στόχο της αξιολόγησης;

...

7 ΓΕΝΙΚΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΥΠΕΥΘΥΝΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΤΩΝ ΕΚΤΕΛΟΥΝΤΩΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

α) Απαιτούν τα κριτήρια αποδεικτικά στοιχεία για τις συμβατικές συμφωνίες μεταξύ των εκτελούντων την επεξεργασία και των υπευθύνων επεξεργασίας;

β) Υπόκεινται σε αξιολόγηση οι συμφωνίες μεταξύ υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία;

γ) Αντικατοπτρίζουν τα κριτήρια τις υποχρεώσεις του υπευθύνου επεξεργασίας σύμφωνα με το κεφάλαιο IV;

δ) Απαιτούν τα κριτήρια αποδεικτικά στοιχεία για την επανεξέταση και την επικαιροποίηση των τεχνικών και οργανωτικών μέτρων που εφαρμόζει ο υπεύθυνος επεξεργασίας σύμφωνα με το άρθρο 24 παράγραφος 1;

ε) Επαληθεύουν τα κριτήρια ότι ο οργανισμός έχει εκτιμήσει κατά πόσον θα πρέπει να διοριστεί υπεύθυνος προστασίας δεδομένων (ΥΠΔ), όπως απαιτείται από το άρθρο 37; Αν υπάρχει ΥΠΔ, πληρούνται οι απαιτήσεις των άρθρων 37 έως 39;

στ) Επαληθεύουν τα κριτήρια ότι απαιτούνται αρχεία των δραστηριοτήτων επεξεργασίας σύμφωνα με το άρθρο 30 παράγραφος 5 και ότι πληρούνται δεόντως οι απαιτήσεις του άρθρου 30;

8 ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

α) Εξετάζουν τα κριτήρια επαρκώς το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων και απαιτούν την εφαρμογή αντίστοιχων μέτρων;

β) Απαιτούν τα κριτήρια να διαθέτουν τα υποκείμενα των δεδομένων επαρκή ή ακόμη και μεγαλύτερη πρόσβαση και έλεγχο των δεδομένων τους, συμπεριλαμβανομένης της φορητότητας των δεδομένων;

γ) Απαιτούν τα κριτήρια τη λήψη μέτρων που να προβλέπουν τη δυνατότητα παρέμβασης στη διαδικασία επεξεργασίας προκειμένου να διασφαλίζονται τα δικαιώματα των υποκειμένων των δεδομένων και να επιτρέπονται διορθώσεις, διαγραφή ή περιορισμοί;

...

9 ΚΙΝΔΥΝΟΙ ΓΙΑ ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ ΤΙΣ ΕΛΕΥΘΕΡΙΕΣ ΤΩΝ ΦΥΣΙΚΩΝ ΠΡΟΣΩΠΩΝ

α) Επιτρέπουν, και απαιτούν, τα κριτήρια αξιολόγηση του κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων;

β) Προβλέπουν, ή απαιτούν, τα κριτήρια αναγνωρισμένη μεθοδολογία αξιολόγησης κινδύνων; Αν ναι, είναι η μεθοδολογία αυτή κατάλληλη;

γ) Επιτρέπουν, και απαιτούν, τα κριτήρια αξιολόγηση του αντικτύπου των προβλεπόμενων πράξεων επεξεργασίας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων;

δ) Απαιτούν τα κριτήρια εκ των προτέρων διαβούλευση σχετικά με τους εναπομείναντες κινδύνους που δεν μπορούσαν να μετριαστούν, με βάση τα αποτελέσματα της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ);

10 ΤΕΧΝΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΠΟΥ ΕΓΓΥΩΝΤΑΙ ΤΗΝ ΠΡΟΣΤΑΣΙΑ

α) Απαιτούν τα κριτήρια την εφαρμογή τεχνικών και οργανωτικών μέτρων για την εμπιστευτικότητα των πράξεων επεξεργασίας;

β) Απαιτούν τα κριτήρια την εφαρμογή τεχνικών και οργανωτικών μέτρων για την ακεραιότητα των πράξεων επεξεργασίας;

γ) Απαιτούν τα κριτήρια την εφαρμογή τεχνικών και οργανωτικών μέτρων για τη διαθεσιμότητα των πράξεων επεξεργασίας;

δ) Απαιτούν τα κριτήρια την εφαρμογή μέτρων για τη διαφάνεια των πράξεων επεξεργασίας όσον αφορά

ε) τη λογοδοσία;

στ) τα δικαιώματα των υποκειμένων των δεδομένων;

ζ) την αξιολόγηση επιμέρους πράξεων επεξεργασίας, π.χ. για αλγοριθμική διαφάνεια;

η) Απαιτούν τα κριτήρια την εφαρμογή τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν τα δικαιώματα των υποκειμένων των δεδομένων, π.χ. την ικανότητα παροχής πληροφοριών ή τη φορητότητα των δεδομένων;

θ) Απαιτούν τα κριτήρια την εφαρμογή τεχνικών και οργανωτικών μέτρων που να προβλέπουν την ικανότητα παρέμβασης στην πράξη επεξεργασίας προκειμένου να διασφαλίζονται τα δικαιώματα των υποκειμένων των δεδομένων και να επιτρέπονται διορθώσεις, διαγραφή ή περιορισμοί;

ι) Απαιτούν τα κριτήρια την εφαρμογή μέτρων που προβλέπουν την ικανότητα παρέμβασης στην πράξη επεξεργασίας για την κάλυψη κενών ή τον έλεγχο του συστήματος ή της διαδικασίας;

ια) Απαιτούν τα κριτήρια την εφαρμογή τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ελαχιστοποίησης των δεδομένων, όπως, για παράδειγμα, η αποσύνδεση ή ο διαχωρισμός των δεδομένων από το υποκείμενο των δεδομένων, η ανωνυμοποίηση ή ψευδωνυμοποίηση ή απομόνωση των συστημάτων δεδομένων;

ιβ) Απαιτούν τα κριτήρια τεχνικά μέτρα για την εφαρμογή της προστασίας των δεδομένων εξ ορισμού;

ιγ) Απαιτούν τα κριτήρια τεχνικά και οργανωτικά μέτρα για την εφαρμογή της προστασίας των δεδομένων ήδη από τον σχεδιασμό, π.χ. ένα σύστημα διαχείρισης της προστασίας των δεδομένων

για την απόδειξη, την ενημέρωση, τον έλεγχο και την επιβολή των απαιτήσεων για την προστασία των δεδομένων;

ιδ) Απαιτούν τα κριτήρια τεχνικά και οργανωτικά μέτρα για την εφαρμογή κατάλληλης περιοδικής κατάρτισης και εκπαίδευσης για το προσωπικό που έχει μόνιμη ή τακτική πρόσβαση σε δεδομένα προσωπικού χαρακτήρα;

ιε) Απαιτούν τα κριτήρια επανεξέταση των μέτρων;

ιστ) Απαιτούν τα κριτήρια αυτοαξιολόγηση/εσωτερικό έλεγχο;

ιζ) Απαιτούν τα κριτήρια τη λήψη μέτρων που να διασφαλίζουν ότι τα καθήκοντα κοινοποίησης της παραβίασης δεδομένων προσωπικού χαρακτήρα εκτελούνται σε εύθετο χρόνο και με την ενδεδειγμένη εμβέλεια;

ιη) Απαιτούν τα κριτήρια να εφαρμόζονται και να επαληθεύονται διαδικασίες διαχείρισης συμβάντων;

ιθ) Απαιτούν τα κριτήρια την παρακολούθηση των υπό εξέλιξη ζητημάτων ιδιωτικότητας και τεχνολογίας και την επικαιροποίηση του συστήματος όπως απαιτείται;

...

11 ΆΛΛΕΣ ΕΙΔΙΚΕΣ ΠΤΥΧΕΣ ΠΟΥ ΕΥΝΟΟΥΝ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

α) Απαιτούν τα κριτήρια την εφαρμογή τεχνικών βελτίωσης της προστασίας των δεδομένων; Εδώ θα μπορούσαν να περιλαμβάνονται τα κριτήρια που απαιτούν ενισχυμένη προστασία των δεδομένων με την εξάλειψη ή τον περιορισμό των δεδομένων προσωπικού χαρακτήρα και/ή του κινδύνου προστασίας των δεδομένων.

- *Παράδειγμα: Κριτήρια που απαιτούν ενισχυμένη μη συνδεσιμότητα μέσω της χρήσης διαχείρισης ταυτότητας με επίκεντρο τον χρήστη, όπως τα διαπιστευτήρια με βάση τα χαρακτηριστικά (attribute-based credentials – ABC), αντί διαχείρισης ταυτότητας με επίκεντρο τον οργανισμό, θα αντανακλούν μια τεχνική ενισχυμένης προστασίας των δεδομένων.*

β) Απαιτούν τα κριτήρια την εφαρμογή ενισχυμένων ελέγχων των υποκειμένων των δεδομένων ώστε να διευκολύνεται ο αυτοπροσδιορισμός και η επιλογή;

...

12 ΚΡΙΤΗΡΙΑ ΜΕ ΣΚΟΠΟ ΤΗΝ ΑΠΟΔΕΙΞΗ ΤΗΣ ΥΠΑΡΞΗΣ ΚΑΤΑΛΛΗΛΩΝ ΕΓΓΥΗΣΕΩΝ ΓΙΑ ΤΗ ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Τα κριτήρια θα εξεταστούν στις προσεχείς κατευθυντήριες γραμμές για το άρθρο 42 παράγραφος 2.

13 ΠΡΟΣΘΕΤΑ ΚΡΙΤΗΡΙΑ ΓΙΑ ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΣΦΡΑΓΙΔΑ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

α) Προβλέπουν τα κριτήρια την κάλυψη όλων των κρατών μελών;

β) Μπορούν τα κριτήρια να λαμβάνουν υπόψη τη νομοθεσία ή τα σενάρια των κρατών μελών περί προστασίας των δεδομένων;

γ) Απαιτούν τα κριτήρια αξιολόγηση των επιμέρους στόχων της αξιολόγησης σε σχέση με την ειδική τομεακή νομοθεσία των κρατών μελών περί προστασίας των δεδομένων;

δ) Απαιτούν τα κριτήρια από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία να παρέχουν πληροφορίες στα υποκείμενα των δεδομένων και στα ενδιαφερόμενα μέρη στις γλώσσες των κρατών μελών

ε) για την επεξεργασία/τους στόχους της αξιολόγησης;

στ) για την τεκμηρίωση της επεξεργασίας/των στόχων της αξιολόγησης;

ζ) για τα αποτελέσματα της αξιολόγησης:

...

14 ΣΥΝΟΛΙΚΗ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΚΡΙΤΗΡΙΩΝ

α) Καλύπτουν τα κριτήρια ολόκληρο το πεδίο εφαρμογής του μηχανισμού πιστοποίησης (δηλ. ολοκληρωμένα κριτήρια) προκειμένου να παρέχονται επαρκείς εγγυήσεις, ώστε να είναι η πιστοποίηση αξιόπιστη;

- *Παράδειγμα: Αν το πεδίο εφαρμογής του μηχανισμού πιστοποίησης εστιάζεται στις δραστηριότητες επεξεργασίας δεδομένων για την υγεία, θα πρέπει να διασφαλίζεται υψηλό επίπεδο προστασίας των δεδομένων μέσω του καθορισμού κριτηρίων που εξασφαλίζουν, για παράδειγμα, την ενδελεχή αξιολόγηση και την εφαρμογή αρχών προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού.*

β) Είναι τα κριτήρια κατάλληλα για το μέγεθος της πράξης επεξεργασίας που αντιμετωπίζεται από το πεδίο εφαρμογής του μηχανισμού πιστοποίησης, για την ευαισθησία των πληροφοριών και για τον κίνδυνο της επεξεργασίας;

γ) Είναι πιθανόν τα κριτήρια να βελτιώσουν τη συμμόρφωση των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία όσον αφορά την προστασία των δεδομένων;

δ) Θα επωφεληθούν τα υποκείμενα των δεδομένων όσον αφορά τα δικαιώματά τους για ενημέρωση, συμπεριλαμβανομένης της εξήγησης των επιθυμητών αποτελεσμάτων στα υποκείμενα των δεδομένων;