Κατευθυντήριες γραμμές 4/2018 σχετικά με τη διαπίστευση των φορέων πιστοποίησης βάσει του άρθρου 43 του Γενικού Κανονισμού για την Προστασία Δεδομένων (2016/679)

Έκδοση 3.0

4 Ιουνίου 2019

Ιστορικό εκδόσεων

Έκδοση 3.0	4 Ιουνίου 2019	Συμπερίληψη του παραρτήματος 1 (έκδοση 2.0 του παραρτήματος 1, που εγκρίθηκε στις 4 Ιουνίου 2019 μετά τη δημόσια διαβούλευση)
Έκδοση 2.0	4 Δεκεμβρίου 2018	Έγκριση των κατευθυντήριων γραμμών μετά τη δημόσια διαβούλευση — Την ίδια ημερομηνία εγκρίθηκε το παράρτημα 1 (έκδοση 1.0) για δημόσια διαβούλευση
Έκδοση 1.0	6 Φεβρουαρίου 2018	Έγκριση των κατευθυντήριων γραμμών από την ομάδα εργασίας του άρθρου 29 (έκδοση για δημόσια διαβούλευση). Η έκδοση αυτή εγκρίθηκε από το ΕΣΠΔ στις 25 Μαΐου 2018.

Πίνακας περιεχομένων

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,

Έχοντας υπόψη τα αποτελέσματα της δημόσιας διαβούλευσης σχετικά με τις κατευθυντήριες γραμμές, που πραγματοποιήθηκε τον Φεβρουάριο του 2018, και της διαβούλευσης σχετικά με το παράρτημα, που πραγματοποιήθηκε από τις 14 Δεκεμβρίου 2018 έως την 1η Φεβρουαρίου 2019, σύμφωνα με το άρθρο 70 παράγραφος 4 του ΓΚΠΔ

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ:

1 ΕΙΣΑΓΩΓΗ

1. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679) («ΓΚΠΔ»), ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2018, παρέχει ένα εκσυγχρονισμένο πλαίσιο συμμόρφωσης για την προστασία δεδομένων στην Ευρώπη, το οποίο βασίζεται στη λογοδοσία και στα θεμελιώδη δικαιώματα. Διάφορα μέτρα για τη διευκόλυνση της συμμόρφωσης με τις διατάξεις του ΓΚΠΔ έχουν βαρύνουσα σημασία στο νέο αυτό πλαίσιο. Στα μέτρα αυτά περιλαμβάνονται υποχρεωτικές απαιτήσεις σε ειδικές περιστάσεις (συμπεριλαμβανομένου του διορισμού υπευθύνων προστασίας δεδομένων και της διενέργειας εκτιμήσεων αντικτύπου σχετικά με την προστασία δεδομένων) και προαιρετικά μέτρα όπως κώδικες δεοντολογίας και μηχανισμοί πιστοποίησης.
2. Στο πλαίσιο της θέσπισης μηχανισμών πιστοποίησης και της έγκρισης σφραγίδων και σημάτων προστασίας δεδομένων, το άρθρο 43 παράγραφος 1 του ΓΚΠΔ υποχρεώνει τα κράτη μέλη να διασφαλίζουν ότι η διαπίστευση των φορέων πιστοποίησης που εκδίδουν πιστοποιήσεις βάσει του άρθρου 42 παράγραφος 1 πραγματοποιείται από την αρμόδια εποπτική αρχή ή τον εθνικό οργανισμό διαπίστευσης, ή από αμφότερους τους φορείς αυτούς. Εάν η διαπίστευση διενεργείται από τον εθνικό οργανισμό διαπίστευσης σύμφωνα με το πρότυπο ISO/IEC 17065/2012, πρέπει επίσης να εφαρμόζονται οι συμπληρωματικές απαιτήσεις που έχουν οριστεί από την αρμόδια εποπτική αρχή.
3. Η λειτουργία ουσιαστικών μηχανισμών πιστοποίησης μπορεί να ενισχύσει τη συμμόρφωση με τον ΓΚΠΔ και τη διαφάνεια για τα υποκείμενα των δεδομένων, καθώς και στις σχέσεις μεταξύ επιχειρήσεων (B2B), για παράδειγμα, μεταξύ υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία. Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την

επεξεργασία θα λαμβάνουν βεβαίωση ανεξάρτητου τρίτου μέρους για τον σκοπό της απόδειξης της συμμόρφωσης των πράξεων επεξεργασίας τους[1].

4. Στο πλαίσιο αυτό, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) αναγνωρίζει ότι είναι αναγκαία η παροχή κατευθυντήριων γραμμών σχετικά με τη διαπίστευση. Η ιδιαίτερη αξία και ο σκοπός της διαπίστευσης έγκεινται στο γεγονός ότι η διαπίστευση παρέχει επίσημη βεβαίωση της αρμοδιότητας των φορέων πιστοποίησης, η οποία καθιστά δυνατή την ανάπτυξη εμπιστοσύνης προς τον μηχανισμό πιστοποίησης.
5. Στόχος των κατευθυντήριων γραμμών είναι η παροχή καθοδήγησης σχετικά με τον τρόπο ερμηνείας και εφαρμογής των διατάξεων του άρθρου 43 του ΓΚΠΔ. Ειδικότερα, στόχος τους είναι να βοηθήσουν τα κράτη μέλη, τις εποπτικές αρχές και τους εθνικούς φορείς διαπίστευσης να καθιερώσουν μια συνεκτική, εναρμονισμένη βάση αναφοράς για τη διαπίστευση των φορέων πιστοποίησης που εκδίδουν πιστοποιήσεις σύμφωνα με τον ΓΚΠΔ.

2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΩΝ ΚΑΤΕΥΘΥΝΤΗΡΙΩΝ ΓΡΑΜΜΩΝ

6. Στις παρούσες κατευθυντήριες γραμμές:

- περιγράφεται ο σκοπός της διαπίστευσης στο πλαίσιο του ΓΚΠΔ·
- επεξηγούνται οι οδοί που είναι διαθέσιμες για τη διαπίστευση φορέων πιστοποίησης σύμφωνα με το άρθρο 43 παράγραφος 1 και προσδιορίζονται βασικά ζητήματα προς εξέταση·
- παρέχεται πλαίσιο για τον καθορισμό συμπληρωματικών απαιτήσεων διαπίστευσης όταν η διαπίστευση διεκπεραιώνεται από τον εθνικό οργανισμό διαπίστευσης· και
- παρέχεται πλαίσιο για τον καθορισμό απαιτήσεων διαπίστευσης όταν η διαπίστευση διεκπεραιώνεται από την εποπτική αρχή.

7. Οι κατευθυντήριες γραμμές δεν αποτελούν διαδικαστικό εγχειρίδιο για τη διαπίστευση των φορέων πιστοποίησης σύμφωνα με τον ΓΚΠΔ. Δεν αναπτύσσουν νέο τεχνικό πρότυπο για τη διαπίστευση των φορέων πιστοποίησης για τους σκοπούς του ΓΚΠΔ.
8. Οι κατευθυντήριες γραμμές απευθύνονται:
    - στα κράτη μέλη, τα οποία πρέπει να διασφαλίζουν ότι η διαπίστευση των φορέων πιστοποίησης πραγματοποιείται από την εποπτική αρχή και/ή τον εθνικό οργανισμό διαπίστευσης·
    - σε εθνικούς οργανισμούς διαπίστευσης που διενεργούν τη διαπίστευση φορέων πιστοποίησης βάσει του άρθρου 43 παράγραφος 1 στοιχείο β)·
    - στην αρμόδια εποπτική αρχή η οποία προσδιορίζει «συμπληρωματικές απαιτήσεις», επιπλέον εκείνων που ορίζονται στο πρότυπο ISO/IEC 17065/2012[2], όταν η διαπίστευση πραγματοποιείται από τον εθνικό οργανισμό διαπίστευσης βάσει του άρθρου 43 παράγραφος 1 στοιχείο β)·

[1] Στην αιτιολογική σκέψη 100 του ΓΚΠΔ αναφέρεται ότι η θέσπιση μηχανισμών πιστοποίησης μπορεί να βελτιώσει τη διαφάνεια και τη συμμόρφωση με τον κανονισμό και να επιτρέψει στα υποκείμενα των δεδομένων να αξιολογούν το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων και υπηρεσιών.

[2] Διεθνής Οργανισμός Τυποποίησης: Αξιολόγηση της συμμόρφωσης – Απαιτήσεις για φορείς πιστοποίησης προϊόντων, διεργασιών και υπηρεσιών.

- στο ΕΣΠΔ, κατά την έκδοση γνώμης και την έγκριση των απαιτήσεων διαπίστευσης της αρμόδιας εποπτικής αρχής δυνάμει του άρθρου 43 παράγραφος 3, του άρθρου 70 παράγραφος 1 στοιχείο ιστ) και του άρθρου 64 παράγραφος 1 στοιχείο γ)·
- στην αρμόδια εποπτική αρχή η οποία προσδιορίζει τις απαιτήσεις διαπίστευσης όταν η διαπίστευση πραγματοποιείται από την εποπτική αρχή βάσει του άρθρου 43 παράγραφος 1 στοιχείο α)·

- σε άλλους ενδιαφερομένους όπως μελλοντικοί φορείς πιστοποίησης ή κάτοχοι συστημάτων πιστοποίησης που παρέχουν κριτήρια και διαδικασίες πιστοποίησης[3].

9. Ορισμοί
10. Σκοπός των ακόλουθων ορισμών είναι η προαγωγή της κοινής κατανόησης των βασικών στοιχείων της διαδικασίας διαπίστευσης. Οι ορισμοί θα πρέπει να εκληφθούν ως σημεία αναφοράς και δεν έχουν απαρέγκλιτο χαρακτήρα. Βασίζονται σε υφιστάμενα κανονιστικά πλαίσια και πρότυπα, ειδικότερα στις σχετικές διατάξεις του ΓΚΠΔ και του προτύπου ISO/IEC 17065/2012.
11. Για τους σκοπούς των παρουσών κατευθυντήριων γραμμών, ισχύουν οι ακόλουθοι ορισμοί:
12. «*διαπίστευση*» των φορέων πιστοποίησης: βλ. ενότητα 3 σχετικά με την ερμηνεία της διαπίστευσης για τους σκοπούς του άρθρου 43 του ΓΚΠΔ·
13. «*συμπληρωματικές απαιτήσεις*»: οι απαιτήσεις οι οποίες ορίζονται από την εποπτική αρχή που είναι αρμόδια και με βάση τις οποίες πραγματοποιείται η διαπίστευση[4]·
14. «*πιστοποίηση*»: η αξιολόγηση και η βεβαίωση από αμερόληπτο τρίτο[5] ότι έχει αποδειχθεί η εκπλήρωση των κριτηρίων πιστοποίησης·
15. «*φορέας πιστοποίησης*»: οργανισμός[6] αξιολόγησης της συμμόρφωσης τρίτων[7] ο οποίος διαχειρίζεται μηχανισμούς πιστοποίησης[8]·
16. «*σύστημα πιστοποίησης*»: σύστημα πιστοποίησης που συνδέεται με συγκεκριμένα προϊόντα, διεργασίες και υπηρεσίες στα οποία εφαρμόζονται οι ίδιες συγκεκριμένες απαιτήσεις και ειδικοί κανόνες και διαδικασίες[9]·

---

[3] Κάτοχος συστήματος είναι ένας αναγνωρίσιμος οργανισμός ο οποίος έχει καθορίσει κριτήρια πιστοποίησης και απαιτήσεις βάσει των οποίων πρέπει να αξιολογείται η συμμόρφωση. Η διαπίστευση αφορά τον οργανισμό που διενεργεί αξιολογήσεις (άρθρο 43 παράγραφος 4) με βάση τις απαιτήσεις του συστήματος πιστοποίησης και εκδίδει τα πιστοποιητικά (δηλ. ο φορέας πιστοποίησης, γνωστός και ως οργανισμός αξιολόγησης της συμμόρφωσης). Ο οργανισμός που διενεργεί τις αξιολογήσεις μπορεί να είναι ο οργανισμός που ανέπτυξε και κατέχει το σύστημα, αλλά θα μπορούσαν να υπάρχουν ρυθμίσεις στο πλαίσιο των οποίων το σύστημα ανήκει σε έναν οργανισμό και ένας άλλος (ή περισσότεροι άλλοι) οργανισμός διενεργεί τις αξιολογήσεις.

[4] Άρθρο 43 παράγραφοι 1, 3 και 6.

[5] Σημειώνεται ότι σύμφωνα με το πρότυπο ISO 17000, η βεβαίωση τρίτου (πιστοποίηση) «έχει εφαρμογή σε όλα τα αντικείμενα αξιολόγησης της συμμόρφωσης» (5.5) «με εξαίρεση τους ίδιους τους οργανισμούς αξιολόγησης της συμμόρφωσης, στους οποίους έχει εφαρμογή η διαπίστευση» (5.6).

[6] Βλ. ISO 17000, 2.5: «οργανισμός που παρέχει υπηρεσίες αξιολόγησης της συμμόρφωσης»· ISO 17011: «οργανισμός που παρέχει υπηρεσίες αξιολόγησης της συμμόρφωσης και μπορεί να αποτελεί το αντικείμενο διαπίστευσης»· ISO 17065, 3.12.

[7] Η δραστηριότητα αξιολόγησης της συμμόρφωσης τρίτων εκτελείται από οργανισμό ο οποίος είναι ανεξάρτητος από το πρόσωπο ή τον οργανισμό που παρέχει το αντικείμενο και από συμφέροντα χρήστη επί αυτού του αντικειμένου, πρβλ. ISO 17000, 2.4.

[8] Άρθρο 42 παράγραφος 1, άρθρο 42 παράγραφος 5 του ΓΚΠΔ.

[9] Βλ. σημείο 3.9 σε συνδυασμό με το παράρτημα Β του προτύπου ISO 17065.

17. «κριτήρια» ή κριτήρια πιστοποίησης: τα κριτήρια με βάση τα οποία διενεργείται η πιστοποίηση (αξιολόγηση της συμμόρφωσης)[10].
18. «εθνικός οργανισμός διαπίστευσης»: ο μόνος οργανισμός κράτους μέλος που ορίζεται σύμφωνα με τον Κανονισμό (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και εκτελεί τη διαπίστευση επί τη βάσει εξουσίας που του παρέχει το κράτος αυτό[11].

3 ΕΡΜΗΝΕΙΑ ΤΗΣ «ΔΙΑΠΙΣΤΕΥΣΗΣ» ΓΙΑ ΤΟΥΣ ΣΚΟΠΟΥΣ ΤΟΥ ΑΡΘΡΟΥ 43 ΤΟΥ ΓΚΠΔ

19. Στον ΓΚΠΔ δεν παρέχεται ορισμός του όρου «διαπίστευση». Στο άρθρο 2 σημείο 10 του Κανονισμού (ΕΚ) αριθ. 765/2008, ο οποίος καθορίζει γενικές απαιτήσεις για τη διαπίστευση, η διαπίστευση ορίζεται ως
20. «βεβαίωση από εθνικό οργανισμό διαπίστευσης ότι ένας οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις απαιτήσεις που έχουν τεθεί με εναρμονισμένα πρότυπα και, όπου είναι εφαρμοστέο, τις τυχόν πρόσθετες απαιτήσεις, συμπεριλαμβανομένων αυτών που καθορίζονται στα αντίστοιχα τομεακά συστήματα, για να εκτελεί μια συγκεκριμένη δραστηριότητα αξιολόγησης της συμμόρφωσης».
21. Δυνάμει του προτύπου ISO/IEC 17011,
22. «η διαπίστευση αναφέρεται σε βεβαίωση τρίτου μέρους, σχετική με οργανισμό αξιολόγησης της συμμόρφωσης, με την οποία παρέχεται επίσημη διαβεβαίωση της ικανότητας του οργανισμού να εκτελεί συγκεκριμένα καθήκοντα αξιολόγησης της συμμόρφωσης».
23. Το άρθρο 43 παράγραφος 1 ορίζει τα εξής:
24. «Με την επιφύλαξη των καθηκόντων και των αρμοδιοτήτων της αρμόδιας εποπτικής αρχής σύμφωνα με τα άρθρα 57 και 58, οι φορείς πιστοποίησης που διαθέτουν το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με την προστασία των δεδομένων, αφού ενημερώσουν την εποπτική αρχή προκειμένου να μπορέσει να ασκήσει τις αρμοδιότητές της δυνάμει του άρθρου 58 παράγραφος 2 στοιχείο η) όπου απαιτείται, χορηγούν και ανανεώνουν πιστοποιήσεις. Το κράτος μέλος διασφαλίζει ότι η διαπίστευση των εν λόγω φορέων πιστοποίησης πραγματοποιείται από ένα ή αμφότερα τα ακόλουθα:
    (α) την εποπτική αρχή που είναι αρμόδια δυνάμει των άρθρων 55 ή 56,
    (β) τον εθνικό οργανισμό διαπίστευσης που ορίζεται σύμφωνα με τον Κανονισμό (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σύμφωνα με το πρότυπο EN-ISO/IEC 17065/2012 και σύμφωνα με τις συμπληρωματικές απαιτήσεις που έχουν οριστεί από την εποπτική αρχή που είναι αρμόδια δυνάμει του άρθρου 55 ή 56.»
25. Όσον αφορά τον ΓΚΠΔ, οι απαιτήσεις διαπίστευσης καθοδηγούνται από:

- το πρότυπο ISO/IEC 17065/2012 και τις «συμπληρωματικές απαιτήσεις» οι οποίες έχουν οριστεί από την εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 43 παράγραφος 1 στοιχείο β), όταν η διαπίστευση διενεργείται από τον εθνικό οργανισμό διαπίστευσης, και από την εποπτική αρχή όταν διενεργεί η ίδια τη διαπίστευση.

[10] Βλέπε άρθρο 42 παράγραφος 5.
[11] Βλέπε άρθρο 2 σημείο 11 του Κανονισμού (ΕΚ) αριθ. 765/2008.

26. Και στις δύο περιπτώσεις, οι ενοποιημένες απαιτήσεις πρέπει να καλύπτουν τις απαιτήσεις που αναφέρονται στο άρθρο 43 παράγραφος 2.
27. Το ΕΣΠΔ αναγνωρίζει ότι σκοπός της διαπίστευσης είναι να παράσχει επίσημη βεβαίωση της αρμοδιότητας ενός οργανισμού να διενεργεί πιστοποιήσεις (δραστηριότητες αξιολόγησης της συμμόρφωσης)[12]. Η διαπίστευση βάσει του ΓΚΠΔ νοείται ως εξής:
28. βεβαίωση[13] από εθνικό οργανισμό διαπίστευσης και/ή εποπτική αρχή ότι ένας φορέας πιστοποίησης[14] διαθέτει τα απαιτούμενα προσόντα για τη διενέργεια πιστοποιήσεων δυνάμει των άρθρων 42 και 43 του ΓΚΠΔ, λαμβανομένων υπόψη του προτύπου ISO/IEC 17065/2012 και των συμπληρωματικών απαιτήσεων που έχουν οριστεί από την εποπτική αρχή και/ή το Συμβούλιο Προστασίας Δεδομένων.

4 ΔΙΑΠΙΣΤΕΥΣΗ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΑΡΘΡΟ 43 ΠΑΡΑΓΡΑΦΟΣ 1 ΤΟΥ ΓΚΠΔ

29. Το άρθρο 43 παράγραφος 1 αναγνωρίζει ότι υπάρχουν διάφορες επιλογές για τη διαπίστευση των φορέων πιστοποίησης. Ο ΓΚΠΔ απαιτεί από τις εποπτικές αρχές και τα κράτη μέλη να ορίσουν τη διαδικασία διαπίστευσης των φορέων πιστοποίησης. Στην παρούσα ενότητα παρατίθενται οι οδοί διαπίστευσης που προβλέπονται στο άρθρο 43.

4.1 Ρόλος των κρατών μελών

30. Το άρθρο 43 παράγραφος 1 απαιτεί από τα κράτη μέλη *να διασφαλίζουν* ότι οι φορείς πιστοποίησης είναι διαπιστευμένοι, αλλά παρέχει σε κάθε κράτος μέλος τη δυνατότητα να αποφασίζει ποιος θα είναι υπεύθυνος για τη διενέργεια της αξιολόγησης που οδηγεί στη διαπίστευση. Βάσει του άρθρου 43 παράγραφος 1, διατίθενται τρεις επιλογές· η διαπίστευση πραγματοποιείται:

(1) αποκλειστικά από την εποπτική αρχή, με βάση τις δικές της απαιτήσεις·
(2) αποκλειστικά από τον εθνικό οργανισμό διαπίστευσης που ορίζεται σύμφωνα με τον Κανονισμό (ΕΚ) αριθ. 765/2008, βάσει του προτύπου ISO/IEC 17065/2012 και σύμφωνα με τις συμπληρωματικές απαιτήσεις που ορίζονται από την αρμόδια εποπτική αρχή· ή
(3) από αμφότερους τους φορείς –εποπτική αρχή και εθνικός οργανισμός διαπίστευσης (και σύμφωνα με όλες τις απαιτήσεις που παρατίθενται στο σημείο 2 ανωτέρω).

31. Εναπόκειται στο εκάστοτε κράτος μέλος να αποφασίσει αν οι εν λόγω δραστηριότητες διαπίστευσης θα εκτελούνται από τον εθνικό οργανισμό διαπίστευσης ή την εποπτική αρχή ή και από τους δύο μαζί, αλλά σε κάθε περίπτωση το κράτος μέλος θα πρέπει να διασφαλίζει την παροχή επαρκών πόρων[15].

4.2 Αλληλεπίδραση με τον Κανονισμό (ΕΚ) αριθ. 765/2008

[12] Βλέπε αιτιολογική σκέψη 15 του Κανονισμού (ΕΚ) αριθ. 765/2008.
[13] Βλέπε άρθρο 2 σημείο 10 του Κανονισμού (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για τον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας της αγοράς όσον αφορά την εμπορία των προϊόντων.
[14] Πρβλ. με τον ορισμό του όρου «διαπίστευση» δυνάμει του προτύπου ISO 17011.
[15] Βλέπε άρθρο 4 παράγραφος 9 του Κανονισμού (ΕΚ) αριθ. 765/2008.

32. Το ΕΣΠΔ επισημαίνει ότι στο άρθρο 2 σημείο 11 του Κανονισμού (ΕΚ) αριθ. 765/2008 ο εθνικός οργανισμός διαπίστευσης ορίζεται ως «ο *μόνος* οργανισμός κράτους μέλους που εκτελεί τη διαπίστευση επί τη βάσει εξουσίας που του παρέχει το κράτος αυτό».
33. Θα μπορούσε να θεωρηθεί ότι το άρθρο 2 σημείο 11 δεν συνάδει με το άρθρο 43 παράγραφος 1 του ΓΚΠΔ, το οποίο επιτρέπει τη διενέργεια διαπίστευσης από φορέα διαφορετικό από τον εθνικό οργανισμό διαπίστευσης του κράτους μέλους. Το ΕΣΠΔ θεωρεί ότι πρόθεση της νομοθεσίας της ΕΕ ήταν να υπάρξει παρέκκλιση από τη γενική αρχή βάσει της οποίας η διαπίστευση πρέπει να πραγματοποιείται αποκλειστικά από τον εθνικό οργανισμό διαπίστευσης, μέσω της χορήγησης στις εποπτικές αρχές της ίδιας εξουσίας όσον αφορά τη διαπίστευση των φορέων πιστοποίησης. Συνεπώς, το άρθρο 43 παράγραφος 1 αποτελεί lex specialis έναντι του άρθρου 2 σημείο 11 του Κανονισμού (ΕΚ) αριθ. 765/2008.

4.3 Ο ρόλος του εθνικού οργανισμού διαπίστευσης

34. Το άρθρο 43 παράγραφος 1 στοιχείο β) προβλέπει ότι ο εθνικός οργανισμός διαπίστευσης διαπιστεύει φορείς πιστοποίησης σύμφωνα με το πρότυπο ISO/IEC 17065/2012 και τις συμπληρωματικές απαιτήσεις που έχουν οριστεί από την αρμόδια εποπτική αρχή.
35. Για λόγους σαφήνειας, το ΕΣΠΔ επισημαίνει ότι η ειδική αναφορά «του στοιχείου β) της παραγράφου 1» που γίνεται στο άρθρο 43 παράγραφος 3 συνεπάγεται ότι η φράση «οι εν λόγω απαιτήσεις» παραπέμπει στις «συμπληρωματικές απαιτήσεις» που ορίζονται από την αρμόδια εποπτική αρχή βάσει του άρθρου 43 παράγραφος 1 στοιχείο β) και στις απαιτήσεις που ορίζονται στο άρθρο 43 παράγραφος 2.
36. Κατά τη διαδικασία διαπίστευσης, οι εθνικοί οργανισμοί διαπίστευσης εφαρμόζουν τις συμπληρωματικές απαιτήσεις που καθορίζονται από τις εποπτικές αρχές.
37. Φορέας πιστοποίησης που διαθέτει ήδη διαπίστευση βάσει του προτύπου ISO/IEC 17065/2012 για συστήματα πιστοποίησης που δεν αφορούν τον ΓΚΠΔ και ο οποίος επιθυμεί να επεκτείνει το πεδίο εφαρμογής της διαπίστευσής του ώστε να καλύπτει πιστοποιήσεις που εκδίδονται σύμφωνα με τον ΓΚΠΔ θα πρέπει να πληροί τις συμπληρωματικές απαιτήσεις που ορίζονται από την εποπτική αρχή εάν η διαπίστευση διεκπεραιώνεται από τον εθνικό οργανισμό διαπίστευσης. Εάν η διαπίστευση για πιστοποιήσεις βάσει του ΓΚΠΔ παρέχεται μόνο από την αρμόδια εποπτική αρχή, ο φορέας πιστοποίησης που υποβάλλει αίτηση διαπίστευσης θα πρέπει να πληροί τις απαιτήσεις που ορίζονται από την αντίστοιχη εποπτική αρχή.

4.4 Ο ρόλος της εποπτικής αρχής

38. Το ΕΣΠΔ επισημαίνει ότι το άρθρο 57 παράγραφος 1 στοιχείο ιζ) προβλέπει ότι η εποπτική αρχή *διενεργεί* τη διαπίστευση φορέα πιστοποίησης σύμφωνα με το άρθρο 43 ως «καθήκον της εποπτικής αρχής» δυνάμει του άρθρου 57 και το άρθρο 58 παράγραφος 3 στοιχείο ε) προβλέπει ότι η εποπτική αρχή διαθέτει την αδειοδοτική και συμβουλευτική εξουσία να παρέχει διαπίστευση σε φορείς πιστοποίησης σύμφωνα με το άρθρο 43. Η διατύπωση του άρθρου 43 παράγραφος 1 παρέχει έναν βαθμό ευελιξίας και η λειτουργία διαπίστευσης της εποπτικής αρχής θα πρέπει να θεωρείται καθήκον μόνο κατά περίπτωση. Για τη διευκρίνιση του σημείου αυτού μπορεί να χρησιμοποιηθεί νομοθεσία σε επίπεδο κρατών μελών. Ωστόσο, κατά τη διαδικασία διαπίστευσης από εθνικό οργανισμό διαπίστευσης, ο φορέας πιστοποίησης υποχρεούται βάσει του άρθρου 43 παράγραφος 2 στοιχείο α) να αποδεικνύει

την ανεξαρτησία και την εμπειρογνωμοσύνη του σε σχέση με το αντικείμενο του μηχανισμού πιστοποίησης τον οποίο παρέχει, κατά την κρίση της αρμόδιας εποπτικής αρχής[16].

39. Εάν ένα κράτος μέλος προβλέπει ότι οι φορείς πιστοποίησης πρέπει να διαπιστεύονται από την εποπτική αρχή, η εποπτική αρχή θα πρέπει να ορίσει απαιτήσεις διαπίστευσης στις οποίες περιλαμβάνονται, μεταξύ άλλων, οι απαιτήσεις που παρατίθενται αναλυτικά στο άρθρο 43 παράγραφος 2. Σε σύγκριση με τις υποχρεώσεις που αφορούν τη διαπίστευση των φορέων πιστοποίησης από εθνικούς οργανισμούς διαπίστευσης, το άρθρο 43 παρέχει λιγότερες οδηγίες σχετικά με τις απαιτήσεις διαπίστευσης όταν η εποπτική αρχή διενεργεί η ίδια τη διαπίστευση. Με σκοπό τη συμβολή σε μια εναρμονισμένη προσέγγιση της διαπίστευσης, τα κριτήρια διαπίστευσης που χρησιμοποιούνται από την εποπτική αρχή θα πρέπει να καθοδηγούνται από το πρότυπο ISO/IEC 17065 και θα πρέπει να συμπληρώνονται από τις συμπληρωματικές απαιτήσεις τις οποίες ορίζει η εποπτική αρχή δυνάμει του άρθρου 43 παράγραφος 1 στοιχείο β). Το ΕΣΠΔ επισημαίνει ότι το άρθρο 43 παράγραφος 2 στοιχεία α) έως ε) αντικατοπτρίζει και προσδιορίζει τις απαιτήσεις του προτύπου ISO 17065 που θα συμβάλουν στη επίτευξη συνεκτικότητας.
40. Εάν ένα κράτος μέλος προβλέπει ότι οι φορείς πιστοποίησης πρέπει να διαπιστεύονται από τους εθνικούς οργανισμούς διαπίστευσης, η εποπτική αρχή θα πρέπει να ορίσει συμπληρωματικές απαιτήσεις οι οποίες θα συμπληρώνουν τις υφιστάμενες συμβάσεις διαπίστευσης που προβλέπονται στον Κανονισμό (ΕΚ) αριθ. 765/2008 (του οποίου τα άρθρα 3 έως 14 αφορούν την οργάνωση και τη λειτουργία της διαπίστευσης των οργανισμών αξιολόγησης της συμμόρφωσης) και τους τεχνικούς κανόνες που περιγράφουν τις μεθόδους και τις διαδικασίες των φορέων πιστοποίησης. Εν προκειμένω, ο Κανονισμός (ΕΚ) αριθ. 765/2008 παρέχει περαιτέρω καθοδήγηση: Το άρθρο 2 σημείο 10 ορίζει τη διαπίστευση και αναφέρεται σε «εναρμονισμένα πρότυπα» και «τυχόν πρόσθετες απαιτήσεις, συμπεριλαμβανομένων αυτών που καθορίζονται στα αντίστοιχα τομεακά συστήματα». Από τα ανωτέρω συνάγεται ότι οι συμπληρωματικές απαιτήσεις που ορίζονται από την εποπτική αρχή θα πρέπει να περιλαμβάνουν ειδικές απαιτήσεις και να εστιάζουν στη διευκόλυνση της αξιολόγησης, μεταξύ άλλων, της ανεξαρτησίας και του επιπέδου εμπειρογνωμοσύνης των φορέων πιστοποίησης στον τομέα της προστασίας δεδομένων, για παράδειγμα, της ικανότητάς τους να αξιολογούν και να πιστοποιούν πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα από υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία δυνάμει του άρθρου 42 παράγραφος 1. Στο πλαίσιο αυτό περιλαμβάνεται η ικανότητα που απαιτείται από τα τομεακά συστήματα και όσον αφορά την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ειδικότερα του δικαιώματός τους στην προστασία των δεδομένων προσωπικού χαρακτήρα[17]. Το παράρτημα των παρουσών κατευθυντήριων γραμμών μπορεί να αποτελέσει βοήθημα για τις αρμόδιες εποπτικές αρχές κατά τον καθορισμό των «συμπληρωματικών απαιτήσεων» σύμφωνα με το άρθρο 43 παράγραφος 1 στοιχείο β) και το άρθρο 43 παράγραφος 3.
41. Το άρθρο 43 παράγραφος 6 προβλέπει ότι «[ο]ι απαιτήσεις της παραγράφου 3 του παρόντος άρθρου και τα κριτήρια που αναφέρονται στο άρθρο 42 παράγραφος 5 δημοσιοποιούνται

[16] Στις συμπληρωματικές απαιτήσεις που ορίζονται από την εποπτική αρχή δυνάμει του άρθρου 43 παράγραφος 1 στοιχείο β) θα πρέπει να προσδιορίζονται οι απαιτήσεις όσον αφορά την ανεξαρτησία και την εμπειρογνωμοσύνη. Βλ. επίσης παράρτημα 1 των κατευθυντήριων γραμμών.
[17] Άρθρο 1 παράγραφος 2 του ΓΚΠΔ.

από την εποπτική αρχή σε ευχερώς προσβάσιμη μορφή». Συνεπώς, για τη διασφάλιση της διαφάνειας, όλα τα κριτήρια και οι απαιτήσεις που εγκρίνονται από εποπτική αρχή δημοσιεύονται. Όσον αφορά την ποιότητα και την εμπιστοσύνη στους φορείς πιστοποίησης, θα ήταν επιθυμητό να καθίστανται ευχερώς διαθέσιμες στο κοινό όλες οι απαιτήσεις διαπίστευσης.

4.5 Λειτουργία της εποπτικής αρχής ως φορέα πιστοποίησης

42. Το άρθρο 42 παράγραφος 5 προβλέπει ότι η εποπτική αρχή μπορεί να εκδίδει πιστοποιήσεις, αλλά ο ΓΚΠΔ δεν απαιτεί να είναι διαπιστευμένη προκειμένου να πληροί τις απαιτήσεις του Κανονισμού (ΕΚ) αριθ. 765/2008. Το ΕΣΠΔ επισημαίνει ότι το άρθρο 43 παράγραφος 1 στοιχείο α) και ειδικότερα το άρθρο 58 παράγραφος 2 στοιχείο η) και παράγραφος 3 στοιχεία α και ε) έως στ) εξουσιοδοτούν τις εποπτικές αρχές να διενεργούν τόσο διαπίστευση όσο και πιστοποίηση, και παράλληλα να παρέχουν συμβουλές και, κατά περίπτωση, να αποσύρουν πιστοποιήσεις ή να διατάσσουν φορείς πιστοποίησης να μην εκδίδουν πιστοποιήσεις.
43. Ενδέχεται να υπάρχουν περιπτώσεις στις οποίες ο διαχωρισμός των ρόλων και των καθηκόντων διαπίστευσης και πιστοποίησης κρίνεται σκόπιμος ή αναγκαίος, για παράδειγμα, εάν η εποπτική αρχή και άλλοι φορείς πιστοποίησης συνυπάρχουν σε ένα κράτος μέλος και εκδίδουν το ίδιο φάσμα πιστοποιήσεων. Ως εκ τούτου, οι εποπτικές αρχές θα πρέπει να λαμβάνουν επαρκή οργανωτικά μέτρα για τον διαχωρισμό των καθηκόντων βάσει του ΓΚΠΔ με σκοπό την εδραίωση και τη διευκόλυνση των μηχανισμών πιστοποίησης, λαμβάνοντας παράλληλα προφυλάξεις για την αποφυγή συγκρούσεων συμφερόντων που ενδέχεται να προκύπτουν από τα καθήκοντα αυτά. Επιπλέον, τα κράτη μέλη και οι εποπτικές αρχές θα πρέπει να λαμβάνουν υπόψη το εναρμονισμένο ευρωπαϊκό επίπεδο κατά τη διαμόρφωση εθνικής νομοθεσίας και εθνικών διαδικασιών που αφορούν τη διαπίστευση και την πιστοποίηση σύμφωνα με τον ΓΚΠΔ.

4.6 Απαιτήσεις διαπίστευσης

44. Στο παράρτημα των παρουσών κατευθυντήριων γραμμών παρέχεται καθοδήγηση σχετικά με τρόπους προσδιορισμού συμπληρωματικών απαιτήσεων διαπίστευσης. Προσδιορίζονται οι σχετικές διατάξεις του ΓΚΠΔ και προτείνονται απαιτήσεις τις οποίες οι εποπτικές αρχές και οι εθνικοί οργανισμοί διαπίστευσης θα πρέπει να εξετάζουν για τη διασφάλιση της συμμόρφωσης με τον ΓΚΠΔ.
45. Όπως διαπιστώθηκε ανωτέρω, όταν οι φορείς πιστοποίησης έχουν διαπιστευτεί από τον εθνικό οργανισμό διαπίστευσης δυνάμει του Κανονισμού (ΕΚ) αριθ. 765/2008, το πρότυπο ISO/IEC 17065/2012 αποτελεί το σχετικό πρότυπο διαπίστευσης το οποίο συμπληρώνεται με τις συμπληρωματικές απαιτήσεις που ορίζονται από την εποπτική αρχή. Το άρθρο 43 παράγραφος 2 αντικατοπτρίζει γενικές διατάξεις του προτύπου ISO/IEC 17065/2012 λαμβανομένης υπόψη της προστασίας των θεμελιωδών δικαιωμάτων βάσει του ΓΚΠΔ. Το πλαίσιο του παραρτήματος χρησιμοποιεί το άρθρο 43 παράγραφος 2 και το πρότυπο ISO/IEC 17065/2012 ως βάση για τον προσδιορισμό των απαιτήσεων σε συνδυασμό με περαιτέρω κριτήρια που αφορούν την αξιολόγηση της εμπειρογνωμοσύνης των φορέων πιστοποίησης στον τομέα της προστασίας δεδομένων και της ικανότητάς τους να σέβονται τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα όπως κατοχυρώνονται στον ΓΚΠΔ. Το ΕΣΠΔ σημειώνει ότι δίνει ιδιαίτερη έμφαση

στο να διασφαλιστεί ότι οι φορείς πιστοποίησης διαθέτουν κατάλληλο επίπεδο εμπειρογνωμοσύνης στον τομέα της προστασίας δεδομένων σύμφωνα με το άρθρο 43 παράγραφος 1.

46. Οι συμπληρωματικές απαιτήσεις διαπίστευσης που ορίζονται από την εποπτική αρχή θα εφαρμόζονται σε όλους τους φορείς πιστοποίησης που ζητούν διαπίστευση. Ο οργανισμός διαπίστευσης θα αξιολογεί αν ο φορέας πιστοποίησης διαθέτει την ικανότητα να εκτελέσει τη δραστηριότητα πιστοποίησης σύμφωνα με τις συμπληρωματικές απαιτήσεις και το αντικείμενο της πιστοποίησης. Θα γ ίνεται αναφορά σε συγκεκριμένους τομείς ή πεδία πιστοποίησης για τα οποία διαπιστεύεται ο φορέας πιστοποίησης.
47. Το ΕΣΠΔ επισημαίνει επίσης ότι, πέραν των απαιτήσεων του προτύπου ISO/IEC 17065/2012, απαιτείται επίσης ειδική εμπειρογνωμοσύνη στον τομέα της προστασίας δεδομένων εάν άλλοι, εξωτερικοί φορείς, όπως εργαστήρια ή ελεγκτές, εκτελούν μέρη ή συνιστώσες των δραστηριοτήτων πιστοποίησης για λογαριασμό διαπιστευμένου φορέα πιστοποίησης. Στις περιπτώσεις αυτές, η διαπίστευση αυτών των εξωτερικών φορέων βάσει του ΓΚΠΔ δεν είναι δυνατή. Ωστόσο, προκειμένου να διασφαλιστεί η καταλληλότητα αυτών των φορέων για τη δραστηριότητα που εκτελούν για λογαριασμό των διαπιστευμένων φορέων πιστοποίησης, ο διαπιστευμένος φορέας πιστοποίησης πρέπει να διασφαλίζει ότι η εμπειρογνωμοσύνη στον τομέα της προστασίας δεδομένων που απαιτείται για τον διαπιστευμένο φορέα πρέπει επίσης να υφίσταται και να αποδεικνύεται από τον εξωτερικό φορέα σε σχέση με τη σχετική εκτελούμενη δραστηριότητα.
48. Το πλαίσιο για τον προσδιορισμό των συμπληρωματικών απαιτήσεων διαπίστευσης όπως παρουσιάζεται στο παράρτημα των παρουσών κατευθυντήριων γραμμών δεν αποτελεί διαδικαστικό εγχειρίδιο για τη διαδικασία διαπίστευσης που διεξάγεται από τον εθνικό οργανισμό διαπίστευσης ή την εποπτική αρχή. Παρέχει καθοδήγηση σχετικά με τη δομή και τη μεθοδολογία και αποτελεί, συνεπώς, δέσμη εργαλείων για τις εποπτικές αρχές προκειμένου να προσδιορίζουν τις συμπληρωματικές απαιτήσεις διαπίστευσης.

ΠΑΡΑΡΤΗΜΑ 1

Το παράρτημα 1 παρέχει καθοδήγηση για τον προσδιορισμό των «συμπληρωματικών» απαιτήσεων διαπίστευσης σε σχέση με το ISO/IEC 17065/2012 και σύμφωνα με το άρθρο 43 παράγραφος 1 στοιχείο β) και παράγραφος 3 του ΓΚΠΔ.

Το παρόν παράρτημα ορίζει προτεινόμενες απαιτήσεις τις οποίες εκπονεί η εποπτική αρχή προστασίας δεδομένων και οι οποίες εφαρμόζονται κατά τη διαπίστευση φορέα πιστοποίησης από τον εθνικό οργανισμό διαπίστευσης ή την αρμόδια εποπτική αρχή[18]. Οι συμπληρωματικές απαιτήσεις αυτές πρέπει να κοινοποιούνται στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων πριν από την έγκρισή τους σύμφωνα με το άρθρο 64 παράγραφος 1 στοιχείο γ).

Το παρόν παράρτημα θα πρέπει να διαβάζεται σε συνδυασμό με το πρότυπο ISO/IEC 17065/2012. Η αρίθμηση των ενοτήτων που χρησιμοποιείται εδώ αντιστοιχεί στην αρίθμηση που χρησιμοποιείται στο πρότυπο ISO/IEC 17065/2012. Όταν οι εποπτικές αρχές πραγματοποιούν διαπίστευση βάσει του άρθρου 43 παράγραφος 1 στοιχείο α), η ορθή πρακτική θα ήταν να ακολουθείται αυτή η προσέγγιση, όπου είναι εφικτό. Με αυτό τον τρόπο ευνοείται η εναρμονισμένη διαπίστευση της ΕΕ.

Με την επιφύλαξη των ακόλουθων κατευθυντήριων γραμμών ή σε περίπτωση απουσίας κατευθυντήριων γραμμών για οποιοδήποτε στοιχείο του προτύπου ISO/IEC 17065/2012, η αρμόδια εποπτική αρχή μπορεί να διατυπώσει περαιτέρω συμπληρωματικές απαιτήσεις σχετικά με τα εν λόγω στοιχεία, αν είναι σύμφωνες με το εθνικό δίκαιο.

0 ΠΡΟΘΕΜΑ

[Η παρούσα ενότητα αφορά τυχόν συμφωνηθέντες όρους συνεργασίας, κατά περίπτωση, μεταξύ του εθνικού οργανισμού διαπίστευσης και της εποπτικής αρχής προστασίας δεδομένων, π.χ. σχετικά με το ποιος θα πρέπει να είναι υπεύθυνος για την παραλαβή αιτήσεων ή για τον τρόπο οργάνωσης της αναγνώρισης των εγκεκριμένων κριτηρίων στο πλαίσιο της διαδικασίας διαπίστευσης.]

1 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ[19]

Το πεδίο εφαρμογής του προτύπου ISO/IEC 17065/2012 εφαρμόζεται σύμφωνα με τον ΓΚΠΔ. Οι κατευθυντήριες γραμμές για τη διαπίστευση και την πιστοποίηση παρέχουν περαιτέρω πληροφορίες. Το πεδίο εφαρμογής ενός μηχανισμού πιστοποίησης (για παράδειγμα, πιστοποίηση πράξεων επεξεργασίας υπηρεσιών του υπολογιστικού νέφους) θα πρέπει να λαμβάνεται υπόψη κατά την αξιολόγηση από τον εθνικό οργανισμό διαπίστευσης και την αρμόδια εποπτική αρχή κατά τη διάρκεια της διαδικασίας διαπίστευσης, ιδίως όσον αφορά τα κριτήρια, την εμπειρογνωμοσύνη και τη μεθοδολογία αξιολόγησης. Το ευρύτερο πεδίο εφαρμογής του προτύπου ISO/IEC 17065/2012 που καλύπτει προϊόντα, διαδικασίες και υπηρεσίες δεν θα πρέπει να μετριάζει ούτε να υπερβαίνει τις απαιτήσεις του ΓΚΠΔ, π.χ. ένας μηχανισμός διακυβέρνησης δεν μπορεί να αποτελεί το μοναδικό στοιχείο ενός μηχανισμού πιστοποίησης, δεδομένου ότι η πιστοποίηση πρέπει να περιλαμβάνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα, δηλαδή τις πράξεις επεξεργασίας. Σύμφωνα με το

[18] Για πληροφορίες σχετικά με τη διαδικασία έγκρισης των κριτηρίων πιστοποίησης, ανατρέξτε στην ενότητα 4 των κατευθυντήριων γραμμών για την πιστοποίηση.

[19] Η αρίθμηση αναφέρεται στο πρότυπο ISO/IEC 17065/2012.

άρθρο 42 παράγραφος 1, η πιστοποίηση ΓΚΠΔ εφαρμόζεται μόνο στις πράξεις επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία.

2 ΚΑΝΟΝΙΣΤΙΚΑ ΕΓΓΡΑΦΑ ΑΝΑΦΟΡΑΣ

Ο ΓΚΠΔ υπερισχύει του προτύπου ISO/IEC 17065/2012. Αν στις συμπληρωματικές απαιτήσεις ή μέσω του μηχανισμού πιστοποίησης γίνεται αναφορά σε άλλα πρότυπα ISO, αυτά ερμηνεύονται σύμφωνα με τις απαιτήσεις που ορίζονται στον ΓΚΠΔ.

3 ΟΡΟΙ ΚΑΙ ΟΡΙΣΜΟΙ

Στο πλαίσιο του παρόντος παραρτήματος, ισχύουν οι όροι και οι ορισμοί των κατευθυντήριων γραμμών για τη διαπίστευση (WP 261) και την πιστοποίηση (ΕΣΠΔ 1/2018), οι οποίοι υπερισχύουν των ορισμών των προτύπων ISO.

4 ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΗ ΔΙΑΠΙΣΤΕΥΣΗ

4.1 Νομικά και συμβατικά ζητήματα

4.1.1 Νομική ευθύνη

Ένας φορέας πιστοποίησης θα πρέπει να είναι σε θέση να αποδεικνύει (ανά πάσα στιγμή) στον εθνικό οργανισμό διαπίστευσης ή στην αρμόδια εποπτική αρχή ότι διαθέτει επικαιροποιημένες διαδικασίες που αποδεικνύουν τη συμμόρφωση με τις ευθύνες που απορρέουν από τον νόμο και οι οποίες ορίζονται στους όρους διαπίστευσης, συμπεριλαμβανομένων των συμπληρωματικών απαιτήσεων σε σχέση με την εφαρμογή του Κανονισμού 2016/679/ΕΚ. Επισημαίνεται ότι, επειδή ο φορέας πιστοποίησης είναι ο ίδιος υπεύθυνος επεξεργασίας/εκτελών την επεξεργασία δεδομένων, πρέπει να είναι σε θέση να παρουσιάζει στοιχεία που να αποδεικνύουν ότι οι διαδικασίες του συμμορφώνονται με τον Κανονισμό 2016/679/ΕΚ και ότι εφαρμόζει μέτρα που αποσκοπούν ειδικά στον έλεγχο και τη διαχείριση των δεδομένων προσωπικού χαρακτήρα του οργανισμού-πελάτη στο πλαίσιο της διαδικασίας πιστοποίησης.

Η αρμόδια εποπτική αρχή μπορεί να αποφασίσει να προσθέσει περαιτέρω απαιτήσεις και διαδικασίες για τον έλεγχο της συμμόρφωσης των φορέων πιστοποίησης με τον ΓΚΠΔ πριν από τη διαπίστευση.

4.1.2 Συμφωνία πιστοποίησης

Οι ελάχιστες απαιτήσεις για τη συμφωνία πιστοποίησης συμπληρώνονται από τα ακόλουθα σημεία:

Ο φορέας πιστοποίησης αποδεικνύει ότι, επιπλέον των απαιτήσεων του προτύπου ISO/IEC 17065/2012, οι συμφωνίες πιστοποίησης που συνάπτει:

1. απαιτούν από τον αιτούντα να συμμορφώνεται πάντα με τις γενικές απαιτήσεις πιστοποίησης κατά την έννοια της παραγράφου 4.1.2.2 στοιχείο α) του προτύπου ISO/IEC 17065/2012 και με τα κριτήρια που έχουν εγκριθεί από την αρμόδια εποπτική αρχή ή το ΕΣΠΔ σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο β) και το άρθρο 42 παράγραφος 5·
2. απαιτούν από τον αιτούντα να διασφαλίζει πλήρη διαφάνεια για την αρμόδια εποπτική αρχή όσον αφορά τη διαδικασία πιστοποίησης, συμπεριλαμβανομένων εμπιστευτικών θεμάτων της σύμβασης που σχετίζονται με τη συμμόρφωση με την προστασία των

δεδομένων, σύμφωνα με το άρθρο 42 παράγραφος 7 και το άρθρο 58 παράγραφος 1 στοιχείο γ)·

3. δεν μειώνουν την ευθύνη του αιτούντα ως προς τη συμμόρφωση με τον Κανονισμό 2016/679/ΕΚ και δεν θίγουν τα καθήκοντα και τις εξουσίες των εποπτικών αρχών που είναι αρμόδιες σύμφωνα με το άρθρο 42 παράγραφος 5·
4. απαιτούν από τον αιτούντα να παρέχει στον φορέα πιστοποίησης κάθε πληροφορία και πρόσβαση στις δραστηριότητες επεξεργασίας που απαιτείται για τη διεξαγωγή της διαδικασίας πιστοποίησης σύμφωνα με το άρθρο 42 παράγραφος 6·
5. απαιτούν από τον αιτούντα να τηρεί τις ισχύουσες προθεσμίες και διαδικασίες. Η συμφωνία πιστοποίησης πρέπει να ορίζει ότι οι προθεσμίες και οι διαδικασίες που προκύπτουν, για παράδειγμα, από το πρόγραμμα πιστοποίησης ή από άλλες κανονιστικές ρυθμίσεις πρέπει να τηρούνται και να εφαρμόζονται·
6. όσον αφορά την παράγραφο 4.1.2.2 στοιχείο γ) αριθ. 1 του προτύπου ISO/IEC 17065/2012, ορίζουν τους κανόνες ισχύος, ανανέωσης και ανάκλησης σύμφωνα με το άρθρο 42 παράγραφος 7 και το άρθρο 43 παράγραφος 4, συμπεριλαμβανομένων κανόνων που ορίζουν κατάλληλα χρονικά διαστήματα για επαναξιολόγηση ή επανεξέταση (κανονικότητα) σύμφωνα με το άρθρο 42 παράγραφος 7·
7. επιτρέπουν στον φορέα πιστοποίησης να αποκαλύπτει όλες τις πληροφορίες που είναι αναγκαίες για τη χορήγηση της πιστοποίησης σύμφωνα με το άρθρο 42 παράγραφος 8 και το άρθρο 43 παράγραφος 5·
8. περιλαμβάνουν κανόνες σχετικά με τις αναγκαίες προφυλάξεις, που πρέπει να εφαρμόζονται για τη διερεύνηση των καταγγελιών κατά την έννοια της παραγράφου 4.1.2.2 στοιχείο γ) αριθ. 2, και στοιχείο ι)· περιλαμβάνουν επίσης ρητές δηλώσεις σχετικά με τις δομές και τις διαδικασίες για τη διαχείριση καταγγελιών σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο δ)·
9. επιπλέον των ελάχιστων απαιτήσεων που αναφέρονται στην παράγραφο 4.1.2.2 του προτύπου ISO/IEC 17065/2012, αν οι συνέπειες της ανάκλησης ή αναστολής της διαπίστευσης για τον φορέα πιστοποίησης έχουν αντίκτυπο στον πελάτη, τότε οι συνέπειες για τον πελάτη θα πρέπει επίσης να αντιμετωπιστούν·
10. απαιτούν από τον αιτούντα να ενημερώνει τον φορέα πιστοποίησης σε περίπτωση σημαντικών αλλαγών στην πραγματική ή νομική του κατάσταση και στα προϊόντα, στις διαδικασίες και στις υπηρεσίες του, τα οποία αφορά η πιστοποίηση.

4.1.3 Χρήση σφραγίδων και σημάτων προστασίας δεδομένων

Τα πιστοποιητικά, οι σφραγίδες και τα σήματα χρησιμοποιούνται μόνο σύμφωνα με τα άρθρα 42 και 43 και τις κατευθυντήριες γραμμές για τη διαπίστευση και την πιστοποίηση.

4.2 Διαχείριση της αμεροληψίας

Ο οργανισμός διαπίστευσης εξασφαλίζει ότι, επιπλέον της απαίτησης της παραγράφου 4.2. του προτύπου ISO/IEC 17065/2012,

1. ο φορέας πιστοποίησης συμμορφώνεται με τις συμπληρωματικές απαιτήσεις της αρμόδιας εποπτικής αρχής [σύμφωνα με το άρθρο 43 παράγραφος 1 στοιχείο β)]

    α) σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο α), παρέχει χωριστά αποδεικτικά στοιχεία για την ανεξαρτησία του. Αυτό ισχύει ιδίως για τα αποδεικτικά στοιχεία σχετικά με τη χρηματοδότηση του φορέα πιστοποίησης, στον βαθμό που αφορούν τη διασφάλιση της αμεροληψίας·

β) τα καθήκοντα και οι υποχρεώσεις του δεν οδηγούν σε σύγκρουση συμφερόντων σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο ε)·

2. ο φορέας πιστοποίησης δεν έχει συναφώς καμία σχέση με τον πελάτη που αξιολογεί.

4.3 Ευθύνη και χρηματοδότηση

Ο οργανισμός διαπίστευσης, εκτός από την απαίτηση της παραγράφου 4.3.1 του προτύπου ISO/IEC 17065/2012, εξασφαλίζει σε τακτική βάση ότι ο φορέας πιστοποίησης διαθέτει κατάλληλα μέτρα (π.χ. ασφάλιση ή αποθεματικά) για την κάλυψη των υποχρεώσεών του στις γεωγραφικές περιοχές στις οποίες δραστηριοποιείται.

4.4 Όροι που δεν εισάγουν διακρίσεις

Συμπληρωματικές απαιτήσεις μπορούν να διατυπώνονται από την εποπτική αρχή αν είναι σύμφωνες με το εθνικό δίκαιο.

4.5 Εμπιστευτικότητα

Συμπληρωματικές απαιτήσεις μπορούν να διατυπώνονται από την εποπτική αρχή αν είναι σύμφωνες με το εθνικό δίκαιο.

4.6 Διαθέσιμες στο κοινό πληροφορίες

Ο οργανισμός διαπίστευσης, εκτός από την απαίτηση της παραγράφου 4.6 του προτύπου ISO/IEC 17065/2012, απαιτεί από τον φορέα πιστοποίησης τουλάχιστον τα εξής:

1. όλες οι εκδόσεις (τρέχουσες και προηγούμενες) των εγκεκριμένων κριτηρίων που χρησιμοποιούνται κατά την έννοια του άρθρου 42 παράγραφος 5, καθώς και όλες οι διαδικασίες πιστοποίησης, να δημοσιεύονται και να είναι εύκολα προσβάσιμες από το κοινό, με γενική αναφορά της αντίστοιχης περιόδου ισχύος·
2. οι πληροφορίες σχετικά με διαδικασίες διαχείρισης των καταγγελιών και προσφυγές να δημοσιοποιούνται σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο δ).

5 ΔΙΑΡΘΡΩΤΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ, ΑΡΘΡΟ 43 ΠΑΡΑΓΡΑΦΟΣ 4 [«ΟΡΘΗ» ΕΚΤΙΜΗΣΗ]

5.1 Οργανωτική δομή και ανώτατα διοικητικά στελέχη

Η εποπτική αρχή μπορεί να διατυπώνει συμπληρωματικές απαιτήσεις.

5.2 Μηχανισμοί διασφάλισης της αμεροληψίας

Η εποπτική αρχή μπορεί να διατυπώνει συμπληρωματικές απαιτήσεις.

6 ΑΠΑΙΤΟΥΜΕΝΟΙ ΠΟΡΟΙ

6.1 Προσωπικό του φορέα πιστοποίησης

Ο οργανισμός διαπίστευσης, εκτός από την απαίτηση της παραγράφου 6 του προτύπου ISO/IEC 17065/2012, διασφαλίζει ότι το προσωπικό κάθε φορέα πιστοποίησης:

1. έχει αποδείξει ότι διαθέτει κατάλληλη και διαρκή εμπειρογνωμοσύνη (γνώση και πείρα) όσον αφορά την προστασία των δεδομένων σύμφωνα με το άρθρο 43 παράγραφος 1·

2. διαθέτει ανεξαρτησία και διαρκή εμπειρογνωμοσύνη σε σχέση με το αντικείμενο της πιστοποίησης σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο α) και δεν συντρέχει σύγκρουση συμφερόντων σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο ε)·
3. έχει δεσμευτεί να σέβεται τα κριτήρια που αναφέρονται στο άρθρο 42 παράγραφος 5, σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο β)·
4. διαθέτει σχετικές και κατάλληλες γνώσεις και πείρα όσον αφορά την εφαρμογή της νομοθεσίας για την προστασία των δεδομένων·
5. διαθέτει σχετικές και κατάλληλες γνώσεις και πείρα όσον αφορά τα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων, κατά περίπτωση·
6. είναι σε θέση να αποδείξει εμπειρία στους τομείς που αναφέρονται συγκεκριμένα στις συμπληρωματικές απαιτήσεις 6.1.1, 6.1.4 και 6.1.5·

Για προσωπικό με τεχνική εμπειρογνωμοσύνη:

- έχει αποκτήσει τίτλο σπουδών σε συναφή τομέα τεχνικής εμπειρογνωμοσύνης τουλάχιστον στο επίπεδο 6 του ΕΠΕΠ[20] ή αναγνωρισμένο προστατευόμενο τίτλο (π.χ. Dipl. Ing.) για το σχετικό νομοθετικά κατοχυρωμένο επάγγελμα ή διαθέτει σημαντική επαγγελματική πείρα.
- *Το προσωπικό που είναι αρμόδιο για τις αποφάσεις πιστοποίησης* πρέπει να διαθέτει σημαντική επαγγελματική πείρα στον προσδιορισμό και την εφαρμογή μέτρων προστασίας δεδομένων.
- *Το προσωπικό που είναι αρμόδιο για τις αξιολογήσεις* πρέπει να διαθέτει επαγγελματική πείρα στην προστασία τεχνικών δεδομένων, καθώς και γνώσεις και πείρα σε παρεμφερή διαδικασία (π.χ. πιστοποιήσεις/έλεγχοι), και να είναι εγγεγραμμένο σε μητρώο, κατά περίπτωση.

Το προσωπικό αποδεικνύει ότι διατηρεί ειδικές τομεακές γνώσεις όσον αφορά τις τεχνικές και τις ελεγκτικές του ικανότητες μέσω συνεχούς επαγγελματικής εξέλιξης.

Για προσωπικό με νομική εμπειρογνωμοσύνη:

- νομικές σπουδές σε ευρωπαϊκό ή αναγνωρισμένο από το κράτος πανεπιστήμιο για οκτώ τουλάχιστον εξάμηνα, συμπεριλαμβανομένου του ακαδημαϊκού τίτλου σπουδών Master (LL.M.) ή ισοδύναμου τίτλου, ή σημαντική επαγγελματική πείρα.
- *Το προσωπικό που είναι αρμόδιο για τις αποφάσεις πιστοποίησης* πρέπει να αποδεικνύει ότι διαθέτει σημαντική επαγγελματική πείρα στον τομέα του δικαίου περί προστασίας δεδομένων και να είναι εγγεγραμμένο σε μητρώο όπως απαιτείται από το κράτος μέλος.
- *Το προσωπικό που είναι αρμόδιο για τις αξιολογήσεις* πρέπει να αποδεικνύει τουλάχιστον διετή επαγγελματική πείρα στον τομέα του δικαίου περί προστασίας δεδομένων, καθώς και γνώσεις και πείρα σε συγκρίσιμες διαδικασίες (π.χ. πιστοποιήσεις/έλεγχοι), και εφόσον το απαιτεί το κράτος μέλος, να είναι εγγεγραμένο σε μητρώο.
    - Το προσωπικό πρέπει να αποδεικνύει ότι διατηρεί ειδικές τομεακές γνώσεις όσον αφορά τις τεχνικές και τις ελεγκτικές του ικανότητες μέσω συνεχούς επαγγελματικής εξέλιξης.

6.2 Πόροι για την αξιολόγηση

[20] Βλέπε το εργαλείο σύγκρισης του πλαισίου επαγγελματικών προσόντων στη διεύθυνση https://ec.europa.eu/ploteus/en/compare?

Συμπληρωματικές απαιτήσεις μπορούν να διατυπώνονται από την εποπτική αρχή αν είναι σύμφωνες με το εθνικό δίκαιο.

7 ΔΙΑΔΙΚΑΣΤΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ, ΑΡΘΡΟ 43 ΠΑΡΑΓΡΑΦΟΣ 2 ΣΤΟΙΧΕΙΑ Γ), Δ)

7.1 Γενικά

Ο οργανισμός διαπίστευσης, εκτός από την απαίτηση της ενότητας 7.1 του προτύπου ISO/IEC 17065/2012, οφείλει να διασφαλίζει ότι:

1. οι φορείς πιστοποίησης συμμορφώνονται με τις συμπληρωματικές απαιτήσεις της αρμόδιας εποπτικής αρχής [σύμφωνα με το άρθρο 43 παράγραφος 1 στοιχείο β)] κατά την υποβολή της αίτησης, ώστε τα καθήκοντα και οι υποχρεώσεις να μην οδηγούν σε σύγκρουση συμφερόντων σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο β)·
2. οι αρμόδιες εποπτικές αρχές έχουν ενημερωθεί προτού ένας φορέας πιστοποίησης αρχίσει να χρησιμοποιεί μια εγκεκριμένη ευρωπαϊκή σφραγίδα προστασίας δεδομένων σε νέο κράτος μέλος μέσω τοπικού γραφείου του.

7.2 Αίτηση

Επιπλέον της παραγράφου 7.2 του προτύπου ISO/IEC 17065/2012, θα πρέπει να απαιτούνται τα εξής:

1. το αντικείμενο της πιστοποίησης (αντικείμενο αξιολόγησης) πρέπει να περιγράφεται λεπτομερώς στην αίτηση. Περιλαμβάνονται επίσης διεπαφές και διαβιβάσεις σε άλλα συστήματα και οργανισμούς, πρωτόκολλα και άλλες διασφαλίσεις·
2. στην αίτηση πρέπει να διευκρινίζεται αν χρησιμοποιούνται εκτελούντες την επεξεργασία και, όταν η αίτηση υποβάλλεται από εκτελούντες την επεξεργασία, πρέπει να περιγράφονται οι αρμοδιότητες και τα καθήκοντά τους και η αίτηση να περιλαμβάνει τη σχετική σύμβαση/συμβάσεις του οικείου υπεύθυνου επεξεργασίας/εκτελούντος την επεξεργασία.

7.3 Εξέταση της αίτησης

Επιπλέον της παραγράφου 7.3 του προτύπου ISO/IEC 17065/2012, θα πρέπει να απαιτούνται τα εξής:

1. οι δεσμευτικές μέθοδοι αξιολόγησης όσον αφορά το αντικείμενο της αξιολόγησης πρέπει να καθορίζονται στη συμφωνία πιστοποίησης·
2. η αξιολόγηση της παραγράφου 7.3 στοιχείο ε) του κατά πόσον υπάρχει επαρκής εμπειρογνωμοσύνη πρέπει να λαμβάνει υπόψη τόσο την τεχνική όσο και τη νομική εμπειρογνωμοσύνη στον τομέα της προστασίας των δεδομένων, στον βαθμό που απαιτείται.

7.4 Αξιολόγηση

Επιπλέον της παραγράφου 7.4 του προτύπου ISO/IEC 17065/2012, οι μηχανισμοί πιστοποίησης πρέπει να περιγράφουν επαρκείς μεθόδους αξιολόγησης για την αξιολόγηση της συμμόρφωσης της πράξης/των πράξεων επεξεργασίας με τα κριτήρια πιστοποίησης, συμπεριλαμβανομένων, για παράδειγμα, κατά περίπτωση:

1. μεθόδου για την αξιολόγηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τον σκοπό τους και τα σχετικά υποκείμενα των δεδομένων·
2. μεθόδου για την αξιολόγηση της κάλυψης, της σύνθεσης και της εκτίμησης όλων των κινδύνων που έχουν εξεταστεί από τον υπεύθυνο επεξεργασίας και τον εκτελούντα την

επεξεργασία όσον αφορά τις νομικές συνέπειες σύμφωνα με τα άρθρα 30, 32, 35 και 36 του ΓΚΠΔ, καθώς και όσον αφορά τον καθορισμό τεχνικών και οργανωτικών μέτρων σύμφωνα με τα άρθρα 24, 25 και 32 του ΓΚΠΔ, στον βαθμό που τα προαναφερθέντα άρθρα εφαρμόζονται για το αντικείμενο της πιστοποίησης, και

3. μεθόδου για την αξιολόγηση των διορθωτικών μέτρων, συμπεριλαμβανομένων των εγγυήσεων, των διασφαλίσεων και των διαδικασιών για να εξασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της επεξεργασίας, που πρέπει να χορηγούνται στο αντικείμενο της πιστοποίησης, και για να αποδειχθεί ότι πληρούνται οι νομικές απαιτήσεις που ορίζονται στα κριτήρια· και
4. τεκμηρίωσης των μεθόδων και των πορισμάτων.

Ο φορέας πιστοποίησης θα πρέπει να υποχρεούται να διασφαλίζει ότι οι εν λόγω μέθοδοι αξιολόγησης είναι τυποποιημένες και εφαρμόζονται εν γένει. Αυτό σημαίνει ότι χρησιμοποιούνται συγκρίσιμες μέθοδοι αξιολόγησης για συγκρίσιμα αντικείμενα αξιολόγησης. Κάθε απόκλιση από τη διαδικασία αυτή πρέπει να αιτιολογείται από τον φορέα πιστοποίησης.

Επιπλέον της παραγράφου 7.4.2 του προτύπου ISO/IEC 17065/2012, θα πρέπει να επιτρέπεται η διενέργεια της αξιολόγησης από εξωτερικούς εμπειρογνώμονες που έχουν αναγνωριστεί από τον φορέα πιστοποίησης.

Επιπλέον της παραγράφου 7.4.5 του προτύπου ISO/IEC 17065/2012, θα πρέπει να απαιτείται να υπάρχει δυνατότητα συμπερίληψης σε ισχύουσα πιστοποίηση της πιστοποίησης προστασίας των δεδομένων σύμφωνα με τα άρθρα 42 και 43 του ΓΚΠΔ, η οποία καλύπτει ήδη μέρος του αντικειμένου της πιστοποίησης. Ωστόσο, δεν θα αρκεί να αντικατασταθούν πλήρως οι (μερικές) αξιολογήσεις. Ο φορέας πιστοποίησης θα υποχρεούται να ελέγχει τη συμμόρφωση με τα κριτήρια. Για την αναγνώριση θα απαιτείται, σε κάθε περίπτωση, η διαθεσιμότητα πλήρους έκθεσης αξιολόγησης ή πληροφοριών που να επιτρέπουν την αξιολόγηση της προηγούμενης δραστηριότητας πιστοποίησης και των αποτελεσμάτων της. Μια δήλωση πιστοποίησης ή παρόμοιες βεβαιώσεις πιστοποίησης δεν θα πρέπει να θεωρούνται επαρκείς για την αντικατάσταση έκθεσης.

Επιπλέον της παραγράφου 7.4.6 του προτύπου ISO/IEC 17065/2012, θα πρέπει να απαιτείται από τον φορέα πιστοποίησης να καθορίζει λεπτομερώς στον μηχανισμό πιστοποίησής του τον τρόπο με τον οποίο οι πληροφορίες που απαιτούνται από την παράγραφο 7.4.6 χρησιμεύουν για ενημέρωση του πελάτη (αιτούντα πιστοποίηση) σχετικά με τις παρατυπίες ενός μηχανισμού πιστοποίησης. Στο πλαίσιο αυτό, θα πρέπει να καθορίζονται τουλάχιστον η φύση και το χρονοδιάγραμμα των εν λόγω πληροφοριών.

Επιπλέον της παραγράφου 7.4.9 του προτύπου ISO/IEC 17065/2012, θα πρέπει να απαιτείται να παρέχεται πλήρης πρόσβαση στα έγγραφα αυτά από την εποπτική αρχή προστασίας δεδομένων κατόπιν σχετικού αιτήματος.

7.5 Επανεξέταση

Επιπλέον της παραγράφου 7.5 του προτύπου ISO/IEC 17065/2012, απαιτούνται διαδικασίες για τη χορήγηση, την τακτική επανεξέταση και την ανάκληση των αντίστοιχων πιστοποιήσεων σύμφωνα με το άρθρο 43 παράγραφος 2 και το άρθρο 43 παράγραφος 3.

7.6 Απόφαση πιστοποίησης

Επιπλέον της παραγράφου 7.6.1 του προτύπου ISO/IEC 17065/2012, ο φορέας πιστοποίησης θα πρέπει να υποχρεούται να καθορίζει λεπτομερώς στις διαδικασίες του τον τρόπο με τον οποίο εξασφαλίζονται η ανεξαρτησία και η ευθύνη του όσον αφορά τις μεμονωμένες αποφάσεις πιστοποίησης.

7.7 Τεκμηρίωση πιστοποίησης

Επιπλέον της παραγράφου 7.7.1.ε του προτύπου ISO/IEC 17065/2012 και σύμφωνα με το άρθρο 42 παράγραφος 7 του ΓΚΠΔ, θα πρέπει να απαιτείται να μην υπερβαίνει η διάρκεια ισχύος των πιστοποιήσεων τα τρία έτη.

Επιπλέον της παραγράφου 7.7.1.ε του προτύπου ISO/IEC 17065/2012, θα πρέπει να απαιτείται τεκμηρίωση και της περιόδου της προβλεπόμενης παρακολούθησης κατά την έννοια της ενότητας 7.9.

Επιπλέον της παραγράφου 7.7.1.στ του προτύπου ISO/IEC 17065/2012, ο φορέας πιστοποίησης θα πρέπει να υποχρεούται να αναφέρει το αντικείμενο της πιστοποίησης στην τεκμηρίωση πιστοποίησης (δηλώνοντας την κατάσταση έκδοσης ή παρόμοια χαρακτηριστικά, κατά περίπτωση).

7.8 Ευρετήριο πιστοποιημένων προϊόντων

Επιπλέον της παραγράφου 7.8 του προτύπου ISO/IEC 17065/2012, ο φορέας πιστοποίησης θα πρέπει να υποχρεούται να διατηρεί τις πληροφορίες σχετικά με πιστοποιημένα προϊόντα, διαδικασίες και υπηρεσίες προσβάσιμες σε εσωτερικό επίπεδο και από το κοινό. Ο φορέας πιστοποίησης θα παρέχει στο κοινό περίληψη της έκθεσης αξιολόγησης. Στόχος της εν λόγω περίληψης είναι να συμβάλει στη διαφάνεια γύρω από το τι έχει πιστοποιηθεί και τον τρόπο με τον οποίο αξιολογήθηκε. Θα περιλαμβάνει τα εξής:

- το πεδίο εφαρμογής της πιστοποίησης και ουσιαστική περιγραφή του αντικειμένου της πιστοποίησης (αντικείμενο αξιολόγησης),
- τα αντίστοιχα κριτήρια πιστοποίησης (συμπεριλαμβανομένης της έκδοσης ή της λειτουργικής κατάστασης),
- τις μεθόδους αξιολόγησης και τις δοκιμές που έχουν διεξαχθεί και
- το αποτέλεσμα/τα αποτελέσματα.

Επιπλέον της παραγράφου 7.8 του προτύπου ISO/IEC 17065/2012 και σύμφωνα με το άρθρο 43 παράγραφος 5 του ΓΚΠΔ, ο φορέας πιστοποίησης ενημερώνει τις αρμόδιες εποπτικές αρχές για τους λόγους χορήγησης ή ανάκλησης της αιτούμενης πιστοποίησης.

7.9 Εποπτεία

Επιπλέον των παραγράφων 7.9.1, 7.9.2 και 7.9.3 του προτύπου ISO/IEC 17065/2012 και σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο γ) του ΓΚΠΔ, θα πρέπει να απαιτείται η θέσπιση μέτρων τακτικής παρακολούθησης ως προϋπόθεση για τη διατήρηση της πιστοποίησης κατά τη διάρκεια της περιόδου παρακολούθησης.

7.10 Αλλαγές που επηρεάζουν την πιστοποίηση

Επιπλέον των παραγράφων 7.10.1 και 7.10.2 του προτύπου EN ISO/IEC 17065/2012, στις αλλαγές που επηρεάζουν την πιστοποίηση οι οποίες λαμβάνονται υπόψη από τον φορέα πιστοποίησης περιλαμβάνονται: τροποποιήσεις της νομοθεσίας για την προστασία των δεδομένων, έκδοση κατ' εξουσιοδότηση πράξεων της Ευρωπαϊκής Επιτροπής σύμφωνα με τα άρθρα 43 παράγραφοι 8 και 9, αποφάσεις του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων και δικαστικές αποφάσεις σχετικά με την προστασία δεδομένων. Οι διαδικασίες τροποποίησης που θα συμφωνηθούν σύμφωνα με τα ανωτέρω θα μπορούσαν να περιλαμβάνουν τα εξής: μεταβατικές περιόδους, διαδικασία έγκρισης από την αρμόδια εποπτική αρχή, επαναξιολόγηση του σχετικού αντικειμένου της πιστοποίησης και κατάλληλα μέτρα για την ανάκληση της πιστοποίησης, αν η πιστοποιημένη πράξη επεξεργασίας δεν πληροί πλέον τα επικαιροποιημένα κριτήρια.

7.11 Καταγγελία, περιορισμός, αναστολή ή ανάκληση πιστοποίησης

Επιπλέον του κεφαλαίου 7.11.1 του προτύπου ISO/IEC 17065/2012, ο φορέας πιστοποίησης θα πρέπει να υποχρεούται να ενημερώνει αμέσως και γραπτώς την αρμόδια εποπτική αρχή και τον ΕΟΔ, κατά περίπτωση, σχετικά με τα μέτρα που λαμβάνονται και σχετικά με τη συνέχιση, τους περιορισμούς, την αναστολή και την ανάκληση της πιστοποίησης.

Σύμφωνα με το άρθρο 58 παράγραφος 2 στοιχείο η), ο φορέας πιστοποίησης οφείλει να αποδέχεται τις αποφάσεις και εντολές της αρμόδιας εποπτικής αρχής για ανάκληση ή μη χορήγηση πιστοποίησης σε πελάτη (αιτούντα), αν οι απαιτήσεις πιστοποίησης δεν ικανοποιούνται ή έχουν παύσει να ικανοποιούνται.

7.12 Αρχεία

Ο φορέας πιστοποίησης θα πρέπει να υποχρεούται να διατηρεί όλα τα έγγραφα πλήρη, κατανοητά, ενημερωμένα και κατάλληλα για έλεγχο.

7.13 Καταγγελίες και προσφυγές, άρθρο 43 παράγραφος 2 στοιχείο δ)

Επιπλέον της παραγράφου 7.13.1 του προτύπου ISO/IEC 17065/2012, θα πρέπει να απαιτείται από τον φορέα πιστοποίησης να καθορίζει:

α) ποιος μπορεί να υποβάλει καταγγελίες ή ενστάσεις,

β) ποιος τις επεξεργάζεται από την πλευρά του φορέα πιστοποίησης,

γ) ποιες επαληθεύσεις πραγματοποιούνται στο πλαίσιο αυτό, και

δ) τις δυνατότητες διαβούλευσης με τα ενδιαφερόμενα μέρη.

Επιπλέον της παραγράφου 7.13.2 του προτύπου ISO/IEC 17065/2012, θα πρέπει να απαιτείται από τον φορέα πιστοποίησης να καθορίζει:

α) με ποιον τρόπο και σε ποιον πρέπει να δοθεί αυτή η επιβεβαίωση,

β) ποιες είναι οι σχετικές προθεσμίες, και

γ) ποιες διεργασίες ξεκινούν στη συνέχεια.

Επιπλέον της παραγράφου 7.13.1 του προτύπου ISO/IEC 17065/2012, ο φορέας πιστοποίησης πρέπει να καθορίζει τον τρόπο με τον οποίο εξασφαλίζεται ο διαχωρισμός μεταξύ των δραστηριοτήτων πιστοποίησης και του χειρισμού των προσφυγών και των καταγγελιών.

8 ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΟ ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ

Μια γενική απαίτηση για το σύστημα διαχείρισης σύμφωνα με το κεφάλαιο 8 του προτύπου ISO/IEC 17065/2012 είναι ότι η εφαρμογή όλων των απαιτήσεων από τα προηγούμενα κεφάλαια στο πεδίο εφαρμογής του μηχανισμού πιστοποίησης από τον διαπιστευμένο φορέα πιστοποίησης πρέπει να τεκμηριώνεται, να αξιολογείται, να ελέγχεται και να παρακολουθείται ανεξάρτητα.

Η βασική αρχή της διαχείρισης είναι ο καθορισμός ενός συστήματος σύμφωνα με το οποίο οι στόχοι του καθορίζονται αποτελεσματικά και αποδοτικά, και συγκεκριμένα: η υλοποίηση των υπηρεσιών πιστοποίησης μέσω κατάλληλων προδιαγραφών. Αυτό απαιτεί διαφάνεια και επαληθευσιμότητα της εφαρμογής των απαιτήσεων διαπίστευσης από τον φορέα πιστοποίησης και διαρκή συμμόρφωσή του.

Για τον σκοπό αυτό, το σύστημα διαχείρισης πρέπει να καθορίζει μια μεθοδολογία για την ικανοποίηση και τον έλεγχο των απαιτήσεων αυτών σύμφωνα με τις κανονιστικές ρυθμίσεις για την

προστασία των δεδομένων και για τη διαρκή επαλήθευσή τους από τον ίδιο τον πιστοποιημένο φορέα.

Οι εν λόγω αρχές διαχείρισης και η τεκμηριωμένη εφαρμογή τους πρέπει να είναι διαφανείς και να γνωστοποιούνται από τον διαπιστευμένο φορέα πιστοποίησης βάσει της διαδικασίας διαπίστευσης και σύμφωνα με το άρθρο 58 και στη συνέχεια κατόπιν αιτήματος της εποπτικής αρχής προστασίας δεδομένων ανά πάσα στιγμή κατά τη διάρκεια έρευνας με τη μορφή ελέγχων για την προστασία των δεδομένων σύμφωνα με το άρθρο 58 παράγραφος 1 στοιχείο β) ή επανεξέτασης των πιστοποιήσεων που εκδίδονται σύμφωνα με το άρθρο 42 παράγραφος 7, κατ' άρθρο 58 παράγραφος 1 στοιχείο γ).

Ειδικότερα, ο διαπιστευμένος φορέας πιστοποίησης πρέπει να δημοσιοποιεί μονίμως και συνεχώς τις πιστοποιήσεις που χορήγησε και τη βάση (ή τους μηχανισμούς ή τα συστήματα πιστοποίησης) που χρησιμοποιήθηκε για τη χορήγησή τους, το χρονικό διάστημα ισχύος των πιστοποιήσεων, το πλαίσιο και τις προϋποθέσεις υπό τα οποία ισχύουν (αιτιολογική σκέψη 100).

8.1 Γενικές απαιτήσεις του συστήματος διαχείρισης

Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.

8.2 Τεκμηρίωση του συστήματος διαχείρισης

Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.

8.3 Έλεγχος εγγράφων

Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.

8.4 Έλεγχος αρχείων

Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.

8.5 Επανεξέταση από τη διοίκηση

Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.

8.6 Εσωτερικοί έλεγχοι

Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.

8.7 Διορθωτικά μέτρα

Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.

8.8 Προληπτικά μέτρα

Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.

9 ΠΕΡΑΙΤΕΡΩ ΣΥΜΠΛΗΡΩΜΑΤΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ[21]

9.1 Επικαιροποίηση των μεθόδων αξιολόγησης

Ο φορέας πιστοποίησης πρέπει να καθορίζει διαδικασίες για την καθοδήγηση της επικαιροποίησης των μεθόδων αξιολόγησης που εφαρμόζονται στο πλαίσιο της αξιολόγησης της παραγράφου 7.4. Η επικαιροποίηση πρέπει να πραγματοποιείται στο πλαίσιο αλλαγών του νομικού πλαισίου, του/των σχετικού/-ών κινδύνου/-ων, καθώς και της εξέλιξης της τεχνολογίας και του κόστους εφαρμογής των τεχνικών και οργανωτικών μέτρων.

9.2 Διατήρηση της εμπειρογνωμοσύνης

Οι φορείς πιστοποίησης πρέπει να θεσπίζουν διαδικασίες για τη διασφάλιση της κατάρτισης των υπαλλήλων τους με σκοπό την επικαιροποίηση των δεξιοτήτων τους, λαμβάνοντας υπόψη τις εξελίξεις που αναφέρονται στην παράγραφο 9.1.

9.3 Ευθύνες και αρμοδιότητες

9.3.1 Επικοινωνία μεταξύ του φορέα πιστοποίησης και των πελατών του

Πρέπει να υπάρχουν διαδικασίες για την εφαρμογή κατάλληλων διαδικασιών και δομών επικοινωνίας μεταξύ του φορέα πιστοποίησης και του πελάτη του. Σε αυτές περιλαμβάνονται οι ακόλουθες:

5. Διατήρηση των εγγράφων τεκμηρίωσης για τα καθήκοντα και τις αρμοδιότητες από τον διαπιστευμένο φορέα πιστοποίησης, με σκοπό:
    α) αιτήματα παροχής πληροφοριών, ή
    β) τη δυνατότητα επαφής σε περίπτωση καταγγελίας σχετικά με την πιστοποίηση.
6. Διατήρηση διαδικασίας υποβολής αίτησης με σκοπό
    α) την ενημέρωση σχετικά με την πορεία της αίτησης·
    β) αξιολογήσεις της αρμόδιας εποπτικής αρχής σε σχέση με
        i. σχόλια·
        ii. αποφάσεις της αρμόδιας εποπτικής αρχής.

9.3.2 Τεκμηρίωση των δραστηριοτήτων αξιολόγησης

Η εποπτική αρχή μπορεί να διατυπώνει συμπληρωματικές απαιτήσεις.

9.3.3 Διαχείριση του χειρισμού καταγγελιών

Ο χειρισμός των καταγγελιών πρέπει να αποτελεί αναπόσπαστο μέρος του συστήματος διαχείρισης, το οποίο εφαρμόζει ιδίως τις απαιτήσεις της παραγράφου 4.1.2.2 στοιχεία γ) και ι), της παραγράφου 4.6 στοιχείο δ) και της παραγράφου 7.13 του προτύπου ISO/IEC 17065/2012.

Οι σχετικές καταγγελίες και ενστάσεις θα πρέπει να κοινοποιούνται στην αρμόδια εποπτική αρχή.

9.3.4 Διαχείριση της ανάκλησης

Οι διαδικασίες σε περίπτωση αναστολής ή ανάκλησης της διαπίστευσης πρέπει να ενσωματώνονται στο σύστημα διαχείρισης του φορέα πιστοποίησης, συμπεριλαμβανομένων των κοινοποιήσεων στους πελάτες.

---

[21] Η αρμόδια εποπτική αρχή μπορεί να καθορίζει και να προσθέτει συμπληρωματικές απαιτήσεις, αν είναι σύμφωνες με το εθνικό δίκαιο.