Αθήνα, 06-08-2020

Αριθ. πρωτ.: Γ/ΕΞ/5511/06-08-2020

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Α Π Ο Φ Α Σ Η 25/2020

Η Αρχή Προστασίας Δεδομένων Προσωπικού (Αρχή) συνήλθε, μετά από πρόσκληση του Προέδρου της, σε τακτική συνεδρίαση στην έδρα της την Τετάρτη 05.08.2020, σε συνέχεια της από 22.07.2020 συνεδρίασης, προκειμένου να εξετάσει το ζήτημα που αφορά τη διατήρηση ή τροποποίηση του σχεδίου των συμπληρωματικών απαιτήσεων για τη διαπίστευση των φορέων που χορηγούν πιστοποιήσεις σε υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία σύμφωνα με τα άρθρα 42 και 43 του Κανονισμού (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (Γενικός Κανονισμός Προστασίας Δεδομένων – ΓΚΠΔ) κατόπιν της με αριθμό 22/2020 σχετικής γνώμης που εξέδωσε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (Συμβούλιο). Παρέστησαν ο Πρόεδρος της Αρχής Κωνσταντίνος Μενουδάκος και τα τακτικά μέλη Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, ως εισηγητής και Χαράλαμπος Ανθόπουλος, επίσης ως εισηγητής. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, χωρίς δικαίωμα ψήφου, οι ειδικοί επιστήμονες Ευφροσύνη Σιουγλέ και Κωνσταντίνος Λιμνιώτης, πληροφορικοί ελεγκτές, ως βοηθοί εισηγητές καθώς και η Γεωργία Παλαιολόγου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Με την με αριθμό 8/2020 Απόφασή της, η Αρχή αποφάσισε την κατάρτιση σχεδίου στο οποίο ορίζονται οι συμπληρωματικές, σε σχέση με το πρότυπο EN-ISO/IEC 17065/2012, απαιτήσεις για τη διαπίστευση των φορέων πιστοποίησης κατά τα

προβλεπόμενα στα άρθρα 43 παρ. 1 στοιχείο β', 43 παρ. 3 και 57 παρ. 1 στοιχ. ιστ' του ΓΚΠΔ καθώς και στο άρθρο 37 παρ. 1 του ν.4624/2019. Η Αρχή, πριν την έγκριση του εν λόγω σχεδίου, εφάρμοσε το μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63 και ανακοίνωσε το σχέδιο αυτό στο Συμβούλιο, σύμφωνα με το άρθρο 64 παρ. 1 στοιχείο γ' του ΓΚΠΔ. Το Συμβούλιο, κατόπιν γραπτής διαδικασίας (written procedure), η οποία προβλέπεται στο άρθρο 24 παρ. 3 του εσωτερικού του Κανονισμού και η οποία ολοκληρώθηκε στις 23 Ιουλίου 2020, εξέδωσε τη γνώμη 22/2020 σχετικά με το εν λόγω σχέδιο της Αρχής βάσει του άρθρου 64 παρ. 3 του ΓΚΠΔ. Με τη γνώμη αυτή, η οποία εστάλη στην Αρχή με ηλεκτρονικό τρόπο στις 29 Ιουλίου 2020, το Συμβούλιο ζήτησε από την Αρχή την τροποποίηση του εν λόγω σχεδίου βάσει των περιλαμβανομένων σε αυτή συστάσεων προκειμένου για τη συνεκτική εφαρμογή της διαπίστευσης των φορέων πιστοποίησης.

Η Αρχή, αφού άκουσε τους εισηγητές και τους βοηθούς εισηγητές, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

1. Σύμφωνα με το άρθρο 9 του ν.4624/2019, ο οποίος έχει ως σκοπό – μεταξύ άλλων - τη λήψη μέτρων εφαρμογής του ΓΚΠΔ, η εποπτεία της εφαρμογής των διατάξεων του ΓΚΠΔ στην Ελληνική Επικράτεια ασκείται από την Αρχή.
2. Σύμφωνα με το άρθρο 15 παρ. 10 του ν.4624/2019 «*Οι κανονιστικές πράξεις της Αρχής, για τις οποίες δεν προβλέπεται δημοσίευσή τους στην Εφημερίδα της Κυβερνήσεως, δημοσιεύονται στην ιστοσελίδα της Αρχής*».
3. Σύμφωνα με το άρθρο 43 παρ. 6 του ΓΚΠΔ *«Οι απαιτήσεις της παραγράφου 3 του παρόντος άρθρου (...) δημοσιοποιούνται από την εποπτική αρχή σε ευχερώς προσβάσιμη μορφή. Οι εποπτικές αρχές διαβιβάζουν επίσης τις εν λόγω απαιτήσεις και τα κριτήρια στο Συμβούλιο Προστασίας Δεδομένων*».
4. Σύμφωνα με το άρθρο 57 παρ. 1 στοιχ. ιστ' του ΓΚΠΔ η Αρχή *«(...) σχεδιάζει και δημοσιεύει τις απαιτήσεις διαπίστευσης (...) φορέα πιστοποίησης σύμφωνα με το άρθρο 43 (...)»*
5. Σύμφωνα με το άρθρο 64 παρ. 1, 3, 6, 7 και 8 του ΓΚΠΔ:

«(παρ. 1) Το Συμβούλιο εκδίδει γνώμη όποτε μια αρμόδια εποπτική αρχή προτίθεται να θεσπίσει οποιοδήποτε από τα κατωτέρω μέτρα. Για τον σκοπό αυτό, η αρμόδια εποπτική αρχή ανακοινώνει το σχέδιο απόφασης στο Συμβούλιο, όταν: (...) γ) αποσκοπεί στην έγκριση των απαιτήσεων για τη διαπίστευση (...) φορέα πιστοποίησης σύμφωνα με το άρθρο 43 παράγραφος (...)».

«(παρ. 3) Στις περιπτώσεις που αναφέρονται στις παραγράφους 1 και 2, το Συμβούλιο Προστασίας Δεδομένων εκδίδει γνώμη σχετικά με το αντικείμενο που του υποβάλλεται, εφόσον δεν έχει ήδη εκδώσει γνώμη επί του ίδιου θέματος. Η γνώμη αυτή εκδίδεται εντός προθεσμίας οκτώ εβδομάδων με απλή πλειοψηφία των μελών του Συμβουλίου Προστασίας Δεδομένων. Η προθεσμία αυτή μπορεί να παραταθεί κατά έξι ακόμα εβδομάδες, λαμβάνοντας υπόψη την πολυπλοκότητα του θέματος (...)».

«(παρ. 6) Η αρμόδια εποπτική αρχή που αναφέρεται στην παράγραφο 1 δεν εγκρίνει το σχέδιο απόφασης που αναφέρεται στην παράγραφο 1 εντός της προθεσμίας που αναφέρεται στην παράγραφο 3».

«(παρ. 7) Η αρμόδια εποπτική αρχή που αναφέρεται στην παράγραφο 1 λαμβάνει ιδιαιτέρως υπόψη τη γνώμη του Συμβουλίου Προστασίας Δεδομένων και, εντός δύο εβδομάδων από την παραλαβή της γνώμης, ανακοινώνει στον Πρόεδρο του Συμβουλίου Προστασίας Δεδομένων με ηλεκτρονικά μέσα κατά πόσο θα διατηρήσει ή θα τροποποιήσει το σχέδιο απόφασης και, εφόσον συντρέχει περίπτωση, το τροποποιημένο σχέδιο απόφασης, χρησιμοποιώντας τυποποιημένο μορφότυπο».

«(παρ. 8) Όταν η αρμόδια εποπτική αρχή που αναφέρεται στην παράγραφο 1 ενημερώνει τον Πρόεδρο του Συμβουλίου Προστασίας Δεδομένων, εντός της προθεσμίας που αναφέρεται στην παράγραφο 7 του παρόντος άρθρου, ότι δεν προτίθεται να ακολουθήσει τη γνώμη του Συμβουλίου Προστασίας Δεδομένων, στο σύνολό της ή εν μέρει, παρέχοντας τη σχετική αιτιολογία, εφαρμόζεται το άρθρο 65 παράγραφος 1».

6. Ενόψει των ανωτέρω, η Αρχή, αφού έλαβε υπόψη και εξέτασε τις συστάσεις, περιλαμβανομένων των ενθαρρύνσεων, της γνώμης 22/2020 του Συμβουλίου, έκρινε ομόφωνα ότι όλες οι συστάσεις και οι ενθαρρύνσεις της εν λόγω γνώμης πρέπει να γίνουν δεκτές, να επέλθουν οι αναγκαίες μεταβολές στο σχέδιο των συμπληρωματικών απαιτήσεων διαπίστευσης, το οποίο είχε υποβάλει αρχικά στο Συμβούλιο και να ανακοινώσει το τροποποιημένο σχέδιο στο Συμβούλιο, εντός της προθεσμίας που αναφέρεται στο άρθρο 64 παρ. 7 του ΓΚΠΔ.

7. Για το σκοπό αυτό πραγματοποιήθηκαν επί του σχεδίου των συμπληρωματικών απαιτήσεων διαπίστευσης, το οποίο είχε καταρτιστεί με την υπ' αριθμ. 8/2020 Απόφαση της Αρχής, οι αναγκαίες μεταβολές προς εκπλήρωση του συνόλου των συστάσεων και ενθαρρύνσεων της γνώμης 22/2020 του Συμβουλίου.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή, αποφασίζει ομόφωνα, την τροποποίηση του σχεδίου των συμπληρωματικών απαιτήσεων για τη διαπίστευση των φορέων πιστοποίησης, βάσει των συστάσεων και των ενθαρρύνσεων της γνώμης 22/2020 του Συμβουλίου, και την ανακοίνωση του τροποποιημένου σχεδίου στο Συμβούλιο, σύμφωνα με το άρθρο 64 παρ. 7 του ΓΚΠΔ. Το τροποποιημένο σχέδιο θα δημοσιευτεί στο διαδικτυακό τόπο της Αρχής σύμφωνα με τα άρθρα 43 παρ. 6 και 57 παρ. 1 στοιχ. ιστ' του ΓΚΠΔ καθώς και το άρθρο 15 παρ. 10 του ν.4624/2019, μετά την ολοκλήρωση της εν λόγω διαδικασίας.
Κατόπιν τούτων, οι τροποποιημένες συμπληρωματικές απαιτήσεις διαπίστευσης παρατίθεται στο Παράρτημα της παρούσας απόφασης.

Ο Πρόεδρος **Η Γραμματέας**

Κωνσταντίνος Μενουδάκος **Γεωργία Παλαιολόγου**

Παράρτημα

Συμπληρωματικές απαιτήσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τη διαπίστευση των φορέων πιστοποίησης σύμφωνα με το άρθρο 43 παράγραφος 1 στοιχείο β) και το άρθρο 43 παράγραφος 3 του ΓΚΠΔ σε συνδυασμό με το πρότυπο EN-ISO/IEC 17065

Περιεχόμενα

Εισαγωγή..... 7

0. Πρόθεμα..... 7

1. Πεδίο εφαρμογής..... 8

2. Κανονιστικά έγγραφα αναφοράς..... 9

3. Όροι και ορισμοί..... 9

4. Γενικές απαιτήσεις για τη διαπίστευση..... 10

4.1 Νομικά και συμβατικά ζητήματα..... 10

4.1.1 Νομική ευθύνη..... 10

4.1.2 Συμφωνία πιστοποίησης..... 11

4.1.3 Χρήση σφραγίδων και σημάτων προστασίας δεδομένων..... 12

4.2 Διαχείριση της αμεροληψίας..... 12

4.3. Ευθύνη και χρηματοδότηση..... 13

4.6 Διαθέσιμες στο κοινό πληροφορίες..... 13

5. Διαρθρωτικές απαιτήσεις, άρθρο 43 παράγραφος 4 του ΓΚΠΔ [«ορθή» εκτίμηση].. 14

6. Απαιτούμενοι πόροι..... 14

6.1 Προσωπικό του φορέα πιστοποίησης..... 14

6.2 Πόροι για την αξιολόγηση..... 15

7. Διαδικαστικές απαιτήσεις, άρθρο 43 παράγραφος 2 στοιχεία γ), δ) του ΓΚΠΔ..... 15

7.1 Γενικά..... 15

7.2 Αίτηση..... 16

7.3 Εξέταση της αίτησης..... 17

7.4 Αξιολόγηση..... 17

7.5 Επανεξέταση..... 18

7.6 Απόφαση πιστοποίησης..... 18

7.7 Τεκμηρίωση πιστοποίησης..... 19

7.8 Ευρετήριο πιστοποιημένων προϊόντων..... 19

7.9 Εποπτεία 20
7.10 Αλλαγές που επηρεάζουν την πιστοποίηση 20
7.11 Καταγγελία, περιορισμός, αναστολή ή ανάκληση πιστοποίησης 20
7.12 Αρχεία 21
7.13 Καταγγελίες και προσφυγές, άρθρο 43 παράγραφος 2 στοιχείο δ) του ΓΚΠΔ 21
8. Απαιτήσεις για το σύστημα διαχείρισης 22
9. Περαιτέρω συμπληρωματικές απαιτήσεις 23
9.1 Επικαιροποίηση των μεθόδων αξιολόγησης 23
9.2 Διατήρηση της εμπειρογνωμοσύνης 23
9.3 Ευθύνες και αρμοδιότητες 23
9.3.1 Επικοινωνία μεταξύ του φορέα πιστοποίησης και των αιτούντων και πελατών του 23
9.3.3 Διαχείριση του χειρισμού καταγγελιών 23
9.3.4 Διαχείριση της ανάκλησης 24

Εισαγωγή

Η θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων προβλέπεται στο άρθρο 42 του ΓΚΠΔ. Η θέσπιση των μηχανισμών αυτών μπορεί να βελτιώσει τη διαφάνεια και τη συμμόρφωση με τον ΓΚΠΔ και να επιτρέπει στα υποκείμενα των δεδομένων να αξιολογούν το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων και υπηρεσιών (αιτιολογική σκέψη 100 του ΓΚΠΔ).

Η πιστοποίηση χορηγείται από διαπιστευμένο προς τούτο φορέα πιστοποίησης, βάσει του άρθρου 43 του ΓΚΠΔ, σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, ο οποίος έχει υποβάλει τη σχετική επεξεργασία του στο μηχανισμό πιστοποίησης. Η διαπίστευση των φορέων πιστοποίησης έχει ιδιαίτερη σημασία καθώς παρέχει επίσημη βεβαίωση της σχετικής αρμοδιότητας των φορέων αυτών καθιστώντας δυνατή την ανάπτυξη εμπιστοσύνης προς τον μηχανισμό πιστοποίησης.

Σύμφωνα με το άρθρο 37 παράγραφος 1 του ν.4624/2019, η διαπίστευση των φορέων που χορηγούν πιστοποιήσεις, σύμφωνα με το άρθρο 42 του ΓΚΠΔ, πραγματοποιείται από το Εθνικό Σύστημα Διαπίστευσης (εφεξής Ε.ΣΥ.Δ.) (www.esyd.gr), με βάση το πρότυπο EN-ISO/IEC 17065/2012 (εφεξής ISO 17065) και σύμφωνα με τις συμπληρωματικές απαιτήσεις διαπίστευσης που ορίζονται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής ΑΠΔΠΧ). Το Ε.ΣΥ.Δ. εφαρμόζει τις παρούσες συμπληρωματικές απαιτήσεις κατά τη διαδικασία διαπίστευσης σε συνδυασμό με το πρότυπο ISO 17065.

Το παρόν έγγραφο περιλαμβάνει τις συμπληρωματικές απαιτήσεις διαπίστευσης που θέτει η ΑΠΔΠΧ σε σχέση με το πρότυπο ISO 17065 και σύμφωνα με τα άρθρα 43 παράγραφος 1 στοιχείο β) και 43 παράγραφος 3 του ΓΚΠΔ.

Οι εν λόγω απαιτήσεις βασίζονται στις προτεινόμενες απαιτήσεις των κατευθυντήριων γραμμών 4/2018[1] του ΕΣΠΔ και πρέπει να εφαρμόζονται σε συνδυασμό με το πρότυπο ISO 17065. Η αρίθμηση των ενοτήτων που χρησιμοποιείται εδώ αντιστοιχεί στην αρίθμηση που χρησιμοποιείται στο ISO 17065 και στις κατευθυντήριες γραμμές του ΕΣΠΔ. Ωστόσο, κάποιες από τις ενότητες του ISO 17065 δεν περιλαμβάνονται στο παρόν έγγραφο. Αυτό σημαίνει ότι για τις συγκεκριμένες ενότητες δεν τίθενται συμπληρωματικές απαιτήσεις διαπίστευσης αλλά εφαρμόζονται οι απαιτήσεις της αντίστοιχης κάθε φορά ενότητας του ISO 17065.

0. Πρόθεμα

Στο σημείο αυτό παρατίθενται όροι συνεργασίας μεταξύ της ΑΠΔΠΧ και του Ε.ΣΥ.Δ. στο πλαίσιο της διαπίστευσης των φορέων πιστοποίησης. Αναλυτικότεροι όροι συνεργασίας, ρόλοι, αρμοδιότητες και διαδικασίες σε σχέση με τη διαπίστευση θα συμφωνηθούν μεταξύ της ΑΠΔΠΧ και του Ε.ΣΥ.Δ.

Το Ε.ΣΥ.Δ. πρέπει να ενημερώνει γραπτώς την ΑΠΔΠΧ:

1) Σχετικά με όλα τα αιτήματα διαπίστευσης που υποβάλλονται από τους φορείς πιστοποίησης. Ειδικότερα, το Ε.ΣΥ.Δ. παρέχει στην ΑΠΔΠΧ συνοπτική περιγραφή του αιτήματος, την επωνυμία και τα στοιχεία επικοινωνίας του φορέα πιστοποίησης, το σχήμα πιστοποίησης για το οποίο ζητείται η διαπίστευση καθώς

[1] *'Κατευθυντήριες γραμμές 4/2018 σχετικά με τη διαπίστευση των φορέων πιστοποίησης βάσει του άρθρου 43 του Γενικού Κανονισμού για την Προστασία Δεδομένων (2016/679)'*
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_4_2018_accreditation_en.pdf

και αν είναι εγκεκριμένα τα κριτήρια πιστοποίησης από την αρμόδια εποπτική αρχή ή το ΕΣΠΔ. Σε περίπτωση που το αίτημα διαπίστευσης υποβληθεί στο Ε.ΣΥ.Δ. πριν από την οριστική έγκριση των κριτηρίων πιστοποίησης, το Ε.ΣΥ.Δ δεν χορηγεί τη διαπίστευση έως ότου τα κριτήρια πιστοποίησης λάβουν οριστική έγκριση.

2) Σχετικά με τους λόγους χορήγησης ή ανάκλησης της διαπίστευσης, πριν από κάθε χορήγηση ή ανάκληση διαπίστευσης. Η ενημέρωση προς την ΑΠΔΠΧ περιλαμβάνει κατ' ελάχιστον πληροφορίες σχετικά με την επωνυμία και τα στοιχεία του φορέα πιστοποίησης, το χρονικό διάστημα χορήγησης της διαπίστευσης, την ημερομηνία της αρχικής διαπίστευσης, τις ημερομηνίες έναρξης και λήξης της τρέχουσας διαπίστευσης καθώς και το σχήμα πιστοποίησης που αφορά η διαπίστευση.

3) Για τις ενέργειες στις οποίες προέβη σχετικά με την ανάκληση της διαπίστευσης στην περίπτωση που το Ε.ΣΥ.Δ. ενημερωθεί από την ΑΠΔΠΧ ότι δεν πληρούνται πλέον οι απαιτήσεις διαπίστευσης ή ο φορέας πιστοποίησης παραβαίνει τον ΓΚΠΔ και τις διατάξεις του ν. 4624/2019 (άρθρο 37 παρ. 2 του ν.4624/2019).

Η ΑΠΔΠΧ, εφόσον κρίνει, ενημερώνει σε εύλογο χρονικό διάστημα το Ε.ΣΥ.Δ. για τυχόν σημαντικούς λόγους μη συμμόρφωσης του φορέα πιστοποίησης με τον ΓΚΠΔ. Στην περίπτωση αυτή, το Ε.ΣΥ.Δ. δύναται να συνεχίσει τη διαδικασία διαπίστευσης, αλλά δεν την ολοκληρώνει πριν από την οριστική σχετική κρίση της ΑΠΔΠΧ. Το Ε.ΣΥ.Δ. είναι ελεύθερο να αποφασίζει σχετικά με τη χορήγηση της διαπίστευσης. Θα πρέπει, ωστόσο, να λαμβάνει υπόψη την οριστική απόφαση της ΑΠΔΠΧ χωρίς να θίγεται η εξουσία της ΑΠΔΠΧ να ανακαλέσει εκ των υστέρων την διαπίστευση, εφόσον το κρίνει σκόπιμο.

Οι πληροφορίες που παρέχονται από την ΑΠΔΠΧ στο Ε.ΣΥ.Δ. στο πλαίσιο της διαδικασίας διαπίστευσης πρέπει να τηρούνται με εμπιστευτικότητα.

Το Ε.ΣΥ.Δ. πρέπει να διασφαλίζει πλήρη διαφάνεια προς την ΑΠΔΠΧ όσον αφορά τη διαδικασία διαπίστευσης σύμφωνα με τα άρθρα 43 παρ. 4 και 7, 58 παρ. 1 στοιχείο β) του ΓΚΠΔ και το άρθρο 37 παρ. 2 του ν. 4624/2019.

Το προσωπικό του Ε.ΣΥ.Δ. που είναι αρμόδιο για τις αξιολογήσεις και εμπλέκεται στη διαδικασία διαπίστευσης των φορέων πιστοποίησης, πρέπει να διαθέτει αποδεδειγμένη γνώση του ΓΚΠΔ και της προστασίας προσωπικών δεδομένων.

1. Πεδίο εφαρμογής

Το παρόν έγγραφο περιέχει τις συμπληρωματικές προς το πρότυπο ISO 17065 απαιτήσεις διαπίστευσης της ΑΠΔΠΧ σύμφωνα με τα άρθρα 43 παράγραφος 1 στοιχείο β) και 43 παράγραφος 3 του ΓΚΠΔ, λαμβάνοντας υπόψη τις κατευθυντήριες γραμμές 4/2018 του ΕΣΠΔ.

Το πεδίο εφαρμογής του προτύπου ISO 17065 πρέπει να εφαρμόζεται σύμφωνα με τον ΓΚΠΔ. Οι κατευθυντήριες γραμμές 4/2018 του ΕΣΔΠ σχετικά με τη διαπίστευση και οι κατευθυντήριες γραμμές 1/2018 σχετικά με την πιστοποίηση παρέχουν περαιτέρω πληροφορίες. Το ευρύτερο πεδίο εφαρμογής του προτύπου ISO 17065 που καλύπτει προϊόντα, διαδικασίες και υπηρεσίες δεν 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.

Το πεδίο εφαρμογής ενός μηχανισμού πιστοποίησης (για παράδειγμα, πιστοποίηση πράξεων επεξεργασίας υπηρεσιών υπολογιστικού νέφους), πρέπει να λαμβάνεται υπόψη στην αξιολόγηση από το Ε.ΣΥ.Δ. κατά τη διάρκεια της διαδικασίας διαπίστευσης, ιδίως όσον αφορά τα κριτήρια, την εμπειρογνωμοσύνη και τη μεθοδολογία αξιολόγησης.

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

2. Κανονιστικά έγγραφα αναφοράς

Ο ΓΚΠΔ υπερισχύει του προτύπου ISO 17065. 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. Όροι και ορισμοί

Ισχύουν οι όροι και οι ορισμοί των κατευθυντήριων γραμμών για τη διαπίστευση (ΕΣΠΔ 4/2018) και την πιστοποίηση (ΕΣΠΔ 1/2018), οι οποίοι υπερισχύουν των ορισμών των προτύπων ISO.

Προς διευκόλυνση παρατίθενται οι παρακάτω βασικοί ορισμοί:

- *«ΓΚΠΔ»*: Κανονισμός 2016/679/ΕΚ - Γενικός Κανονισμός Προστασίας Δεδομένων.

- «*ISO 17065*»: EN-ISO/IEC 17065/2012.

- *«Πιστοποίηση»*: η αξιολόγηση και η βεβαίωση από αμερόληπτο τρίτο ότι έχει αποδειχθεί η εκπλήρωση των κριτηρίων πιστοποίησης στο πλαίσιο της πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 του ΓΚΠΔ για πράξεις επεξεργασίας υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία.

- *«Διαπίστευση»*: η βεβαίωση τρίτου σχετικά με τις δραστηριότητες φορέα αξιολόγησης της συμμόρφωσης, με την οποία παρέχεται επίσημη διαβεβαίωση της ικανότητας του φορέα να διενεργεί πιστοποιήσεις δυνάμει των άρθρων 42 και 43 του ΓΚΠΔ. Αυτό είναι το αποτέλεσμα της διαδικασίας αξιολόγησης ενός φορέα πιστοποίησης ο οποίος πιστοποιείται επιτυχώς (στο πλαίσιο της διαδικασίας διαπίστευσης).

- «*Φορέας πιστοποίησης»*: οργανισμός αξιολόγησης της συμμόρφωσης τρίτων ο οποίος διαχειρίζεται σχήματα πιστοποίησης.

- «*Κριτήρια πιστοποίησης*»: τα κριτήρια με βάση τα οποία διενεργείται η πιστοποίηση για συγκεκριμένο σχήμα πιστοποίησης.

- *«Σχήμα πιστοποίησης»:* σύστημα πιστοποίησης που αφορά συγκεκριμένα προϊόντα, διαδικασίες και υπηρεσίες, για τα οποία ισχύουν οι ίδιες απαιτήσεις,

κανόνες και διαδικασίες. Περιλαμβάνει κυρίως τα κριτήρια πιστοποίησης και τη μεθοδολογία αξιολόγησης.

- *«Μηχανισμός πιστοποίησης»:* το σύστημα με βάση το οποίο πιστοποιείται ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία. Πρόκειται για εγκεκριμένο σχήμα πιστοποίησης το οποίο είναι διαθέσιμο στον αιτούντα μαζί με ένα σύνολο υφιστάμενων διαδικασιών. Αποτελεί υπηρεσία η οποία παρέχεται από διαπιστευμένο φορέα πιστοποίησης με βάση εγκεκριμένα κριτήρια και μεθοδολογία αξιολόγησης.

- *«Αντικείμενο αξιολόγησης»:* το αντικείμενο της πιστοποίησης. Στην περίπτωση της πιστοποίησης ΓΚΠΔ πρόκειται για τις σχετικές πράξεις επεξεργασίας για την αξιολόγηση και πιστοποίηση των οποίων ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία υποβάλλει αίτηση.

- *«Αιτών»:* ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, ο οποίος υποβάλλει αίτηση για πιστοποίηση των πράξεων επεξεργασίας του.

- *«Πελάτης»:* ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, ο οποίος έχει πιστοποιηθεί.

4. Γενικές απαιτήσεις για τη διαπίστευση

4.1 Νομικά και συμβατικά ζητήματα

4.1.1 Νομική ευθύνη

Ο φορέας πιστοποίησης πρέπει να είναι σε θέση να αποδεικνύει (ανά πάσα στιγμή) στο Ε.ΣΥ.Δ. 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 ΓΚΠΔ.

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 ΓΚΠΔ και τον ν. 4624/2019 και ότι εφαρμόζει μέτρα που αποσκοπούν ειδικά στον έλεγχο και τη διαχείριση των δεδομένων προσωπικού χαρακτήρα του οργανισμού-πελάτη στο πλαίσιο της διαδικασίας πιστοποίησης.

Ο φορέας πιστοποίησης πρέπει:

- να είναι σε θέση να παρέχει τα στοιχεία που αποδεικνύουν συμμόρφωση με τον ΓΚΠΔ ανά πάσα στιγμή κατά τη διαδικασία της διαπίστευσης·

- να ενημερώνει το Ε.ΣΥ.Δ. σχετικά με παραβιάσεις του ΓΚΠΔ ή του ν. 4624/2019 που διαπιστώνονται από την ΑΠΔΠΧ ή/και τις δικαστικές αρχές οι οποίες ενδέχεται να επηρεάσουν τη διαπίστευση·

- να διασφαλίζει πλήρη διαφάνεια προς την ΑΠΔΠΧ όσον αφορά τις διαδικασίες διαπίστευσης και πιστοποίησης σύμφωνα με τα άρθρα 42 παρ. 7, 43 παρ. 4 του ΓΚΠΔ, 58 παρ. 1 στοιχείο β) και γ) του ΓΚΠΔ και το άρθρο 37 παρ. 2 του ν. 4624/2019.

4.1.2 Συμφωνία πιστοποίησης

Επιπλέον της παραγράφου 4.1.2.1 του προτύπου ISO 17065, η νομικώς εκτελεστή συμφωνία πρέπει να καταρτίζεται γραπτώς. Ο φορέας πιστοποίησης αποδεικνύει ότι, επιπλέον των σχετικών απαιτήσεων του προτύπου ISO 17065, 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 17065 και με τα κριτήρια πιστοποίησης που έχουν εγκριθεί από την ΑΠΔΠΧ ή το ΕΣΠΔ σύμφωνα με τα άρθρα 43 παράγραφος 2 στοιχείο β) και 42 παράγραφος 5 του ΓΚΠΔ·

2. απαιτούν από τον αιτούντα να διασφαλίζει πλήρη διαφάνεια για την ΑΠΔΠΧ όσον αφορά τη διαδικασία πιστοποίησης, συμπεριλαμβανομένων εμπιστευτικών θεμάτων της σύμβασης που σχετίζονται με τη συμμόρφωση με την προστασία των δεδομένων, σύμφωνα με τα άρθρα 42 παράγραφος 7 και 58 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ·

3. δεν μειώνουν την ευθύνη του αιτούντα ως προς τη συμμόρφωση με τον ΓΚΠΔ και δεν θίγουν τα καθήκοντα και τις εξουσίες της ΑΠΔΠΧ σύμφωνα με το άρθρο 42 παράγραφος 5 του ΓΚΠΔ·

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 του ΓΚΠΔ·

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 17065, ορίζουν τους κανόνες ισχύος, ανανέωσης και ανάκλησης σύμφωνα με τα άρθρα 42 παράγραφος 7 και 43 παράγραφος 4 του ΓΚΠΔ, συμπεριλαμβανομένων κανόνων που ορίζουν κατάλληλα χρονικά διαστήματα για επαναξιολόγηση ή επανεξέταση (περιοδικότητα) σύμφωνα με το άρθρο 42 παράγραφος 7 του ΓΚΠΔ και την ενότητα 7.9 των εν λόγω απαιτήσεων·

7. επιτρέπουν στον φορέα πιστοποίησης να αποκαλύπτει στην ΑΠΔΠΧ όλες τις πληροφορίες που είναι αναγκαίες για τη χορήγηση ή ανάκληση της

πιστοποίησης και τους λόγους της σχετικής απόφασης, σύμφωνα με τα άρθρα 42 παράγραφος 8 και 43 παράγραφος 5 του ΓΚΠΔ·

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) του ISO 17065, με διαφανή και εύκολα προσβάσιμο τρόπο, ενώ περιλαμβάνουν επίσης ρητές δηλώσεις σχετικά με τις δομές και τις διαδικασίες για τη διαχείριση καταγγελιών σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο δ) του ΓΚΠΔ·

9. επιπλέον των ελάχιστων απαιτήσεων που αναφέρονται στην παράγραφο 4.1.2.2 του προτύπου ISO 17065, η συμφωνία πιστοποίησης πρέπει να περιλαμβάνει εξήγηση των συνεπειών της ανάκλησης ή της αναστολής της διαπίστευσης για τον φορέα πιστοποίησης καθώς και τον αντίκτυπο που έχουν στον πελάτη. Σε αυτήν την περίπτωση, οι συνέπειες για τον πελάτη πρέπει να αντιμετωπίζονται και με την ενσωμάτωση κατάλληλων διαδικασιών στο σύστημα διαχείρισης του φορέα πιστοποίησης·

10. απαιτούν από τον αιτούντα να ενημερώνει τον φορέα πιστοποίησης σε περίπτωση σημαντικών αλλαγών στην πραγματική ή νομική του κατάσταση και στα προϊόντα, τις διαδικασίες και τις υπηρεσίες του, τα οποία αφορά η πιστοποίηση·

11. απαιτούν από τον αιτούντα να ενημερώνει τον φορέα πιστοποίησης σχετικά με τυχόν παραβιάσεις του ΓΚΠΔ, οι οποίες διαπιστώνονται από την ΑΠΔΠΧ ή/και τις δικαστικές αρχές και ενδέχεται να επηρεάσουν την πιστοποίηση·

12. ορίζουν τους όρους και τις προϋποθέσεις που καθορίζουν τη διάρκεια της διαδικασίας πιστοποίησης καθώς και τις δεσμευτικές μεθόδους αξιολόγησης όσον αφορά το αντικείμενο αξιολόγησης.

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 του ΓΚΠΔ και τις κατευθυντήριες γραμμές για τη διαπίστευση και την πιστοποίηση.

4.2 Διαχείριση της αμεροληψίας

Το Ε.ΣΥ.Δ. εξασφαλίζει ότι, επιπλέον των απαιτήσεων της παραγράφου 4.2 του προτύπου ISO 17065:

1. ο φορέας πιστοποίησης συμμορφώνεται με τις συμπληρωματικές απαιτήσεις της ΑΠΔΠΧ [σύμφωνα με το άρθρο 43 παράγραφος 1 στοιχείο β) του ΓΚΠΔ]

   α. σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο α) του ΓΚΠΔ, 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. ο φορέας πιστοποίησης πρέπει να παρέχει χωριστά στοιχεία που να αποδεικνύουν ότι τα καθήκοντα και οι υποχρεώσεις του δεν οδηγούν σε σύγκρουση συμφερόντων σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο ε) του ΓΚΠΔ·

2. ο φορέας πιστοποίησης δεν έχει συναφώς καμία σχέση ούτε συνδέεται με τον πελάτη που αξιολογεί. Ο φορέας πιστοποίησης δεν θα πρέπει να ανήκει στον ίδιο όμιλο εταιρειών ούτε να ελέγχεται με οποιονδήποτε τρόπο από τον πελάτη που αξιολογεί.

Ο φορέας πιστοποίησης πρέπει να διασφαλίζει ότι δεν υφίστανται συγκρούσεις συμφερόντων και ότι είναι σε θέση να αποδεικνύει σε τακτική βάση ότι διενεργεί τις δραστηριότητες αξιολόγησης της συμμόρφωσης με αμεροληψία, δεν επιτρέπει την άσκηση εμπορικών, οικονομικών και άλλων πιέσεων που θέτουν σε κίνδυνο την αμεροληψία, καθώς και ότι διαχειρίζεται τυχόν συγκρούσεις συμφερόντων που ενδέχεται να διαπιστωθούν.

4.3. Ευθύνη και χρηματοδότηση

Το Ε.ΣΥ.Δ., εκτός από τις απαιτήσεις της παραγράφου 4.3.1 του προτύπου ISO 17065, εξασφαλίζει σε τακτική βάση ότι ο φορέας πιστοποίησης:

1. έχει αξιολογήσει τους κινδύνους που σχετίζονται με τις δραστηριότητες πιστοποίησης που διενεργεί και διαθέτει κατάλληλα μέτρα (π.χ. ασφάλιση ή αποθεματικά) για την κάλυψη των υποχρεώσεών του που απορρέουν από τις λειτουργίες του και τους τομείς δραστηριοτήτων του στις γεωγραφικές περιοχές στις οποίες δραστηριοποιείται, και

2. μπορεί να αποδεικνύει επαρκώς ότι διαθέτει οικονομική σταθερότητα και τους απαιτούμενους πόρους για τις λειτουργίες του.

4.6 Διαθέσιμες στο κοινό πληροφορίες

Το Ε.ΣΥ.Δ., εκτός από την απαίτηση της παραγράφου 4.6 του προτύπου ISO 17065, απαιτεί από τον φορέα πιστοποίησης τουλάχιστον

1. όλες οι εκδόσεις (τρέχουσες και προηγούμενες) των εγκεκριμένων κριτηρίων που χρησιμοποιούνται κατά την έννοια του άρθρου 42 παράγραφος 5 του ΓΚΠΔ, 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) του ΓΚΠΔ.

5. Διαρθρωτικές απαιτήσεις, άρθρο 43 παράγραφος 4 του ΓΚΠΔ [«ορθή» εκτίμηση]

5.1 Οργανωτική δομή και ανώτατα διοικητικά στελέχη

Το Ε.ΣΥ.Δ., εκτός από τις απαιτήσεις της παραγράφου 5.1.3 του προτύπου ISO 17065, πρέπει να απαιτεί από τον φορέα πιστοποίησης να ορίζει πρόσωπο με τον γενικό έλεγχο και την ευθύνη να επιβλέπει την προστασία δεδομένων σχετικά με την αξιολόγηση, τις αποφάσεις και την εποπτεία της πιστοποίησης.

6. Απαιτούμενοι πόροι

6.1 Προσωπικό του φορέα πιστοποίησης

Το Ε.ΣΥ.Δ., εκτός από την απαίτηση της παραγράφου 6 του προτύπου ISO 17065, 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 του ΓΚΠΔ·

2. διαθέτει ανεξαρτησία και διαρκή εμπειρογνωμοσύνη σε σχέση με το αντικείμενο αξιολόγησης σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο α) του ΓΚΠΔ και δεν συντρέχει σύγκρουση συμφερόντων σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο ε) του ΓΚΠΔ·

3. έχει δεσμευτεί να σέβεται τα κριτήρια που αναφέρονται στο άρθρο 42 παράγραφος 5 του ΓΚΠΔ, σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο β) του ΓΚΠΔ·

4. διαθέτει σχετικές και κατάλληλες γνώσεις και πείρα όσον αφορά την εφαρμογή της νομοθεσίας για την προστασία των διδομένων ·

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 εν λόγω συμπληρωματικές απαιτήσεις:

Για προσωπικό με *τεχνική εμπειρογνωμοσύνη:*

- Πρέπει να έχει αποκτήσει πτυχίο στους τομείς της πληροφορικής, της επιστήμης των υπολογιστών ή των μαθηματικών τουλάχιστον επιπέδου ΕΠΠ 6 από ελληνικό ή αλλοδαπό πανεπιστήμιο, ή ισότιμη επαγγελματική εκπαίδευση με αναγνωρισμένο τίτλο ο οποίος είναι κατοχυρωμένος από το κράτος μέλος έκδοσής του. Το πτυχίο του αλλοδαπού πανεπιστημίου πρέπει να είναι αναγνωρισμένο από το κράτος. Επιπροσθέτως, πρέπει να έχει αποκτήσει ακαδημαϊκό τίτλο σπουδών Master ή ισοδύναμο τίτλο, και να διαθέτει συναφή επαγγελματική εμπειρία.
- *Το προσωπικό που είναι αρμόδιο για τις αποφάσεις πιστοποίησης* πρέπει να αποδεικνύει ότι διαθέτει τουλάχιστον διετή επαγγελματική και ολοκληρωμένη

εμπειρία και εμπειρογνωμοσύνη στον προσδιορισμό και την εφαρμογή μέτρων προστασίας δεδομένων.

- *Το προσωπικό που είναι αρμόδιο για τις αξιολογήσεις* πρέπει να αποδεικνύει ότι διαθέτει τουλάχιστον διετή επαγγελματική εμπειρία στις τεχνικές προστασίας δεδομένων, καθώς και γνώσεις, εξειδικευμένη εμπειρογνωμοσύνη και επαγγελματική εμπειρία σε τεχνικές διαδικασίες (π.χ. έλεγχοι και πιστοποιήσεις).

Για προσωπικό με *νομική εμπειρογνωμοσύνη*:

- Πρέπει να έχει αποκτήσει πτυχίο νομικής από ελληνικό ή αλλοδαπό πανεπιστήμιο. Το πτυχίο νομικής του αλλοδαπού πανεπιστημίου πρέπει να είναι αναγνωρισμένο από το κράτος. Επιπροσθέτως, πρέπει να έχει αποκτήσει ακαδημαϊκό τίτλο σπουδών Master (LL.M.) ή ισοδύναμο τίτλο, και να διαθέτει συναφή επαγγελματική εμπειρία.
- *Το προσωπικό που είναι αρμόδιο για τις αποφάσεις πιστοποίησης* πρέπει να αποδεικνύει ότι διαθέτει τουλάχιστον διετή επαγγελματική και ολοκληρωμένη εμπειρία και εμπειρογνωμοσύνη στον τομέα των μέτρων πιστοποίησης σχετικά με το δίκαιο περί προστασίας δεδομένων.
- *Το προσωπικό που είναι αρμόδιο για τις αξιολογήσεις* πρέπει να αποδεικνύει τουλάχιστον διετή επαγγελματική εμπειρία στον τομέα του δικαίου περί προστασίας δεδομένων καθώς και γνώσεις, εξειδικευμένη εμπειρογνωμοσύνη και επαγγελματική εμπειρία σε τεχνικές διαδικασίες (π.χ. έλεγχοι και πιστοποιήσεις).

Το προσωπικό με τεχνική και νομική εμπειρογνωμοσύνη 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

Ο φορέας πιστοποίησης, εκτός από τις απαιτήσεις της ενότητας 6.2 του προτύπου ISO 17065, πρέπει να αποδεικνύει ότι οι προϋποθέσεις της παραγράφου 6.1 των εν λόγω απαιτήσεων συντρέχουν για το προσωπικό των φορέων στους οποίους ο φορέας πιστοποίησης έχει αναθέσει δραστηριότητες αξιολόγησης.

7. Διαδικαστικές απαιτήσεις, άρθρο 43 παράγραφος 2 στοιχεία γ), δ) του ΓΚΠΔ

7.1 Γενικά

Το Ε.ΣΥ.Δ., εκτός από τις απαιτήσεις της ενότητας 7.1 του προτύπου ISO 17065, διασφαλίζει ότι:

1. οι φορείς πιστοποίησης συμμορφώνονται με τις συμπληρωματικές απαιτήσεις της ΑΠΔΠΧ (σύμφωνα με το άρθρο 43 παράγραφος 1 στοιχείο β) του ΓΚΠΔ), ώστε τα καθήκοντα και οι υποχρεώσεις να μην οδηγούν σε σύγκρουση συμφερόντων σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο β) του ΓΚΠΔ·

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·

3. οι φορείς πιστοποίησης έχουν θεσπίσει διαδικασίες για να αξιολογούν ότι οι διαδικασίες και οι μηχανισμοί του αιτούντος για την επεξεργασία και διαχείριση των προσωπικών δεδομένων που σχετίζονται με το πεδίο εφαρμογής της πιστοποίησης και το αντικείμενο αξιολόγησης συμμορφώνονται με τον ΓΚΠΔ·

4. οι φορείς πιστοποίησης έχουν θεσπίσει διαδικασίες/μηχανισμούς προκειμένου η ΑΠΔΠΧ να ενημερώνεται γραπτώς πριν από τη χορήγηση, παράταση, ανανέωση ή ανάκληση/αναστολή της αιτηθείσας πιστοποίησης. Ο φορέας πιστοποίησης πρέπει να εκθέτει στην ΑΠΔΠΧ τους λόγους της σχετικής απόφασης και να προσκομίζει αντίγραφο της περίληψης της έκθεσης αξιολόγησης που αναφέρεται στην ενότητα 7.8 (συμπεριλαμβανομένων των εξής στοιχείων: της επωνυμίας του πελάτη, της περιγραφής του αντικειμένου αξιολόγησης της πιστοποίησης και σύντομης αξιολόγησης προσβάσιμης από το κοινό)·

5. οι φορείς πιστοποίησης έχουν θεσπίσει διαδικασίες για να διερευνούν και ανταποκρίνονται αμελλητί γραπτώς σε τυχόν αιτήματα της ΑΠΔΠΧ σχετικά με την παροχή συγκεντρωτικών στοιχείων για τις πιστοποιήσεις μεταξύ άλλων και για υποβαλλόμενα παράπονα αλλά και για παροχή λεπτομερών στοιχείων που αφορούν συγκεκριμένη περίπτωση.

7.2 Αίτηση

Εκτός από την απαίτηση της ενότητας 7.2 του προτύπου ISO 17065, πρέπει να απαιτούνται τα εξής:

1. το 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·

3. στην αίτηση πρέπει να διευκρινίζεται αν στην επεξεργασία συμμετέχουν από κοινού υπεύθυνοι επεξεργασίας, και όταν η αίτηση υποβάλλεται από τους από κοινού υπεύθυνους επεξεργασίας, πρέπει να περιγράφονται οι αρμοδιότητες και τα καθήκοντά τους, και η αίτηση να περιλαμβάνει τις συμφωνηθείσες ρυθμίσεις.

Κατά το στάδιο της αίτησης, ο φορέας πιστοποίησης πρέπει να παρέχει στην ΑΠΔΠΧ σύντομη περιγραφή για κάθε μια εκ των αιτήσεων.

7.3 Εξέταση της αίτησης

Επιπλέον της παραγράφου 7.3 του προτύπου ISO 17065, πρέπει να απαιτούνται τα εξής:

1. οι δεσμευτικές μέθοδοι αξιολόγησης όσον αφορά το αντικείμενο αξιολόγησης πρέπει να καθορίζονται στη συμφωνία πιστοποίησης·

2. η αξιολόγηση των παραγράφων 7.3.1 στοιχείο ε) και 7.3.3 του ISO 17065 πρέπει να λαμβάνει υπόψη τόσο την τεχνική όσο και τη νομική εμπειρογνωμοσύνη στον τομέα της προστασίας των δεδομένων, στον βαθμό που απαιτείται·

3. η εξέταση της αίτησης πρέπει να λαμβάνει υπόψη όλες τις πληροφορίες που αναφέρονται στην παράγραφο 7.2 των εν λόγω απαιτήσεων.

7.4 Αξιολόγηση

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

1. μεθόδου για την εκτίμηση 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 αξιολόγησης, και

3. μεθόδου για την εκτίμηση 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 αξιολόγησης, και για να αποδεικνύεται ότι πληρούνται οι νομικές απαιτήσεις που ορίζονται στα κριτήρια που έχουν υιοθετηθεί και

4. τεκμηρίωσης των μεθόδων και των πορισμάτων.

Ο φορέας πιστοποίησης 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 17065, πρέπει να επιτρέπεται η διενέργεια της αξιολόγησης από εξωτερικούς εμπειρογνώμονες που έχουν αναγνωριστεί από τον φορέα πιστοποίησης. Οι ίδιες απαιτήσεις που περιγράφονται στην ενότητα 6 των εν λόγω απαιτήσεων αναφορικά με το προσωπικό ισχύουν και για τους εν λόγω εξωτερικούς εμπειρογνώμονες.

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

Επιπλέον της παραγράφου 7.4.6 του προτύπου ISO 17065, πρέπει να απαιτείται από τον φορέα πιστοποίησης να καθορίζει λεπτομερώς στο σχήμα πιστοποίησής του τον τρόπο με τον οποίο οι πληροφορίες που απαιτούνται από την παράγραφο 7.4.6 χρησιμεύουν για ενημέρωση του αιτούντα σχετικά με τις παρατυπίες του σχήματος. Στο πλαίσιο αυτό, πρέπει να καθορίζονται τουλάχιστον η φύση και το χρονοδιάγραμμα των εν λόγω πληροφοριών.

Επιπλέον της παραγράφου 7.4.9 του προτύπου ISO 17065, πρέπει να απαιτείται να παρέχεται πλήρης πρόσβαση στα έγγραφα αυτά από την ΑΠΔΠΧ κατόπιν σχετικού αιτήματος.

7.5 Επανεξέταση

Επιπλέον της παραγράφου 7.5 του προτύπου ISO 17065, απαιτούνται διαδικασίες για τη χορήγηση, την τακτική επανεξέταση και την ανάκληση των αντίστοιχων πιστοποιήσεων σύμφωνα με τα άρθρα 43 παράγραφος 2 και 43 παράγραφος 3 του ΓΚΠΔ.

Επιπλέον της παραγράφου 7.5.1 του προτύπου ISO 17065, ο φορέας πιστοποίησης πρέπει να αποδεικνύει τον τρόπο με το οποίο το/τα πρόσωπο/πρόσωπα στο/στα οποίο/οποία ανατίθεται η επανεξέταση δεν συμμετέχει/συμμετέχουν άμεσα ή έμμεσα στη διαδικασία αξιολόγησης.

7.6 Απόφαση πιστοποίησης

Επιπλέον της παραγράφου 7.6.1 του προτύπου ISO 17065, ο φορέας πιστοποίησης 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.

Ο φορέας πιστοποίησης πρέπει να ενημερώνει γραπτώς την ΑΠΔΠΧ πριν από την έκδοση της απόφασης πιστοποίησης και να εκθέτει τους λόγους της σχετικής απόφασης.

Επιπλέον της παραγράφου 7.6.6 του προτύπου ISO 17065, ο φορέας πιστοποίησης πρέπει να αναφέρει τον τόπο, τον τρόπο και την προθεσμία για να ασκήσει ο αιτών προσφυγή κατά της απόφασης του φορέα πιστοποίησης περί μη χορήγησης πιστοποίησης ή να ζητήσει επανεξέτασή της.

7.7 Τεκμηρίωση πιστοποίησης

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

Επιπλέον της παραγράφου 7.7.1.ε του προτύπου ISO 17065, πρέπει να απαιτείται τεκμηρίωση και της περιόδου της προβλεπόμενης παρακολούθησης κατά την έννοια της ενότητας 7.9 των εν λόγω απαιτήσεων.

Επιπλέον της παραγράφου 7.7.1.στ του προτύπου ISO 17065, ο φορέας πιστοποίησης πρέπει να υποχρεούται να αναφέρει το αντικείμενο αξιολόγησης 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 17065, ο φορέας πιστοποίησης 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 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. Περιλαμβάνει τα εξής:

α) την επωνυμία και τα στοιχεία επικοινωνίας του πελάτη,

β) το πεδίο εφαρμογής της πιστοποίησης και ουσιαστική περιγραφή του αντικειμένου αξιολόγησης,

γ) τα αντίστοιχα κριτήρια πιστοποίησης (συμπεριλαμβανομένης της έκδοσης ή της λειτουργικής κατάστασης),

δ) τις μεθόδους αξιολόγησης και τις δοκιμές που έχουν διεξαχθεί,

ε) το αποτέλεσμα/τα αποτελέσματα,

στ) την ημερομηνία χορήγησης και την ημερομηνία λήξης της ισχύουσας πιστοποίησης και

ζ) τις ημερομηνίες αρχικής πιστοποίησης και επαναπιστοποίησης.

Επιπλέον της παραγράφου 7.8 του προτύπου ISO 17065 και σύμφωνα με το άρθρο 43 παράγραφος 5 του ΓΚΠΔ, ο φορέας πιστοποίησης ενημερώνει την ΑΠΔΠΧ 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 17065, και σύμφωνα με το άρθρο 43 παράγραφος 2 στοιχείο γ) του ΓΚΠΔ, απαιτείται η θέσπιση μέτρων τακτικής παρακολούθησης για τη διατήρηση της πιστοποίησης κατά τη διάρκεια της περιόδου παρακολούθησης. Τα μέτρα αυτά θα πρέπει να λαμβάνονται βάσει κινδύνου και να είναι αναλογικά, ενώ οι δραστηριότητες εποπτείας θα πρέπει να διενεργούνται τουλάχιστον δύο φορές κατά τη διάρκεια της περιόδου πιστοποίησης.

Ο τύπος και η περιοδικότητα των δραστηριοτήτων εποπτείας πρέπει να καθορίζονται στο σχήμα πιστοποίησης.

7.10 Αλλαγές που επηρεάζουν την πιστοποίηση

Επιπλέον των παραγράφων 7.10.1 και 7.10.2 του προτύπου ISO 17065, 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 το άρθρο 43 παράγραφοι 8 και 9 του ΓΚΠΔ,
- αποφάσεις και έγγραφα που εκδίδονται από το ΕΣΠΔ και
- δικαστικές αποφάσεις σχετικά με την προστασία δεδομένων.

Στις παραπάνω αλλαγές περιλαμβάνεται και η περίπτωση κατά την οποία οι τελευταίες εξελίξεις της τεχνολογίας, οι οποίες ίσχυαν κατά τη στιγμή της πιστοποίησης και οι οποίες ελήφθησαν υπόψη για τη χορήγησή της, έχουν καταστεί πλέον παρωχημένες λόγω των πρόσφατων εξελίξεων της τεχνολογίας.

Οι διαδικασίες τροποποίησης που θα διενεργηθούν από τον φορέα πιστοποίησης πρέπει να περιλαμβάνουν τα εξής: μεταβατικές περιόδους, διαδικασία έγκρισης από την ΑΠΔΠΧ, 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 της παραγράφου 7.11.1 του προτύπου ISO 17065, ο φορέας πιστοποίησης πρέπει να υποχρεούται να ενημερώνει αμέσως και γραπτώς την ΑΠΔΠΧ και το Ε.ΣΥ.Δ. σχετικά με τα μέτρα που λαμβάνονται και σχετικά με τη συνέχιση, τους περιορισμούς, την αναστολή και την ανάκληση της πιστοποίησης.

Επιπρόσθετα, σε περιπτώσεις στις οποίες ο φορέας πιστοποίησης διαπιστώνει μη συμμόρφωση, οφείλει να καθορίζει στις απαιτήσεις του ποια μέτρα πρέπει να ληφθούν.

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

περιπτώσεις, ο φορέας πιστοποίησης πρέπει να παρέχει στην ΑΠΔΠΧ σαφή και τεκμηριωμένα στοιχεία που να αποδεικνύουν ότι έχουν ληφθεί τα κατάλληλα μέτρα.

Σοβαρά περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα που σχετίζονται με το πεδίο εφαρμογής της πιστοποίησης και το αντικείμενο αξιολόγησης πρέπει να θεωρούνται ως μη συμμόρφωση με την πιστοποίηση και κατάλληλες ενέργειες πρέπει να λαμβάνονται από το φορέα πιστοποίησης. Για τις ενέργειες αυτές ο φορέας πιστοποίησης πρέπει να ενημερώνει αμελλητί την ΑΠΔΠΧ γραπτώς. Η απαίτηση αυτή δεν επηρεάζει την υποχρέωση του πελάτη να ενημερώνει την ΑΠΔΠΧ σχετικά με περιστατικά παραβίασης δεδομένων σύμφωνα με τις διατάξεις του ΓΚΠΔ.

7.12 Αρχεία

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

Επιπλέον των παραγράφων 7.10 και 7.12 του ISO 17065, ο φορέας πιστοποίησης πρέπει να τηρεί αρχείο με όλες τις αλλαγές που επηρεάζουν την πιστοποίηση, τα μέτρα που λαμβάνονται για την πραγματοποίηση των αλλαγών και την κατάσταση της πιστοποίησης.

Τα στοιχεία των προσώπων του φορέα πιστοποίησης που είναι αρμόδια για την αξιολόγηση και την απόφαση της πιστοποίησης πρέπει να τηρούνται σε αρχείο ξεχωριστά για κάθε περίπτωση πιστοποίησης και να είναι στη διάθεση της ΑΠΔΠΧ εφόσον ζητηθεί. Σκοπός της εν λόγω απαίτησης είναι η ΑΠΔΠΧ να έχει τη δυνατότητα, όταν κρίνεται σκόπιμο, να εξακριβώνει ότι το προσωπικό που είναι αρμόδιο για τις αξιολογήσεις είναι διαφορετικό από το προσωπικό που είναι αρμόδιο για τις αποφάσεις πιστοποίησης για κάθε περίπτωση πιστοποίησης (ήτοι, διαχωρισμός καθηκόντων).

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

Επιπλέον της παραγράφου 7.13.1 του προτύπου ISO 17065, 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 17065, 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 των παραγράφων 7.13.7 και 7.13.8 του προτύπου ISO 17065, ο φορέας πιστοποίησης πρέπει να υποχρεούται να καθορίζει εύλογα χρονικά όρια για την ορθή ενημέρωση των ενδιαφερομένων που έχουν υποβάλει καταγγελίες σχετικά με την πρόοδο, την έκβαση και την περάτωση της διαδικασίας καταγγελιών.

Επιπλέον της παραγράφου 7.13.1 του προτύπου ISO 17065, 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.

Οι φορείς πιστοποίησης πρέπει να δημοσιεύουν τη διαδικασία χειρισμού των καταγγελιών και να την καθιστούν εύκολα προσβάσιμη στο κοινό.

8. Απαιτήσεις για το σύστημα διαχείρισης

Μια γενική απαίτηση για το σύστημα διαχείρισης σύμφωνα με το κεφάλαιο 8 του προτύπου ISO 17065 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 διαπιστευμένο 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 του ΓΚΠΔ και στη συνέχεια κατόπιν αιτήματος της ΑΠΔΠΧ 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) του ΓΚΠΔ ή επανεξέτασης των πιστοποιήσεων που εκδίδονται σύμφωνα με το άρθρο 42 παράγραφος 7 του ΓΚΠΔ, κατ' άρθρο 58 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ.

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 του ΓΚΠΔ).

9. Περαιτέρω συμπληρωματικές απαιτήσεις

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 των εν λόγω απαιτήσεων. 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 των εν λόγω απαιτήσεων.

9.3 Ευθύνες και αρμοδιότητες

9.3.1 Επικοινωνία μεταξύ του φορέα πιστοποίησης και των αιτούντων και πελατών του

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

1. 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.

2. Διατήρηση διαδικασίας υποβολής αίτησης με σκοπό:

    α) την ενημέρωση σχετικά με την πορεία της αίτησης·

    β) αξιολογήσεις της ΑΠΔΠΧ σε σχέση με

        i. σχόλια·

        ii. αποφάσεις της ΑΠΔΠΧ.

9.3.3 Διαχείριση του χειρισμού καταγγελιών

Η διαδικασία χειρισμού 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 17065.

Οι σχετικές καταγγελίες και ενστάσεις πρέπει να ανακοινώνονται στην ΑΠΔΠΧ.

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.

Τίτλος: Συμπληρωματικές απαιτήσεις της Αρχής για τη διαπίστευση των φορέων πιστοποίησης με ενσωματωμένες τις συστάσεις της σχετικής γνώμης 22/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Περίληψη: Η Αρχή, με την με αριθμό 25/2020 Απόφασή της, αποφάσισε ομόφωνα, την τροποποίηση του σχεδίου των συμπληρωματικών απαιτήσεων για τη διαπίστευση των φορέων πιστοποίησης, βάσει των συστάσεων και των ενθαρρύνσεων της σχετικής γνώμης 22/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων και την ανακοίνωση του τροποποιημένου σχεδίου στο Συμβούλιο. Το αρχικό σχέδιο, όπως είχε διαμορφωθεί με την υπ' αριθμ. 8/2020 Απόφαση της Αρχής, είχε υποβληθεί στο Συμβούλιο στο πλαίσιο του μηχανισμού συνεκτικότητας του ΓΚΠΔ. Οι τροποποιημένες συμπληρωματικές απαιτήσεις θα δημοσιευθούν από την Αρχή στο διαδικτυακό της τόπο μετά την ολοκλήρωση της εν λόγω διαδικασίας.