ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 27-04-2020

Αριθ. πρωτ.: Γ/ΕΞ/2883/27-04-2020

Α Π Ο Φ Α Σ Η 8 /2020

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε, μετά από πρόσκληση του Προέδρου της, σε τακτική συνεδρίαση μέσω τηλεδιάσκεψης την 07-04-2020 σε συνέχεια των από 25.02.2020, 03.03.2020 και 10.03.2020 συνεδριάσεων στην έδρα της, προκειμένου να εξετάσει το ζήτημα που αφορά τον ορισμό συμπληρωματικών απαιτήσεων για τη διαπίστευση των φορέων που χορηγούν πιστοποιήσεις σε υπευθύνους επεξεργασίας και εκτελούντες 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). Παρέστησαν ο Προέδρος, Κωνσταντίνος Μενουδάκος, και τα τακτικά μέλη Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, Χαράλαμπος Ανθόπουλος, ως εισηγητής και Ελένη Μαρτσούκου, επίσης ως εισηγήτρια. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, χωρίς δικαίωμα ψήφου, οι ειδικοί επιστήμονες Ευφροσύνη Σιουγλέ και Κωνσταντίνος Λιμνιώτης, πληροφορικοί, ως βοηθοί εισηγητές, οι οποίοι παρείχαν διευκρινίσεις και αποχώρησαν πριν από τη διάσκεψη και τη λήψη απόφασης, καθώς και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Το άρθρο 42 παράγραφος 1 του ΓΚΠΔ προβλέπει ότι τα κράτη μέλη, οι εποπτικές

αρχές, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) και η Επιτροπή ενθαρρύνουν τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων. Και τούτο διότι η θέσπιση των εθελοντικών αυτών εργαλείων λογοδοσίας 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 ΓΚΠΔ).

Ειδικότερα η τήρηση εγκεκριμένου μηχανισμού πιστοποίησης δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας (άρθρο 24 παρ. 3 ΓΚΠΔ) ή ως στοιχείο για να αποδειχθεί ότι ο εκτελών την επεξεργασία παρέχει επαρκείς διαβεβαιώσεις σύμφωνα με τις παρ. 1 και 4 του άρθρου 28 (άρθρο 28 παρ. 5 ΓΚΠΔ). Επίσης, λαμβάνεται υπόψη κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου καθώς και σχετικά με το ύψος του διοικητικού προστίμου (άρθρο 83 παράγραφος 2 στοιχείο ι) ΓΚΠΔ).

Η πιστοποίηση χορηγείται από διαπιστευμένο προς τούτο φορέα πιστοποίησης, βάσει του άρθρου 43 του ΓΚΠΔ, σε υπεύθυνο επεξεργασίας ή εκτελούντα 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 το μηχανισμό πιστοποίησης. Η διαπίστευση φορέα πιστοποίησης πραγματοποιείται από την αρμόδια εποπτική αρχή ή τον εθνικό οργανισμό διαπίστευσης ή από αμφότερους τους φορείς αυτούς (άρθρο 43 παρ. 1 ΓΚΠΔ) και χορηγείται για μέγιστη περίοδο πέντε ετών, μπορεί δε να αναθεωρηθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι ο φορέας πιστοποίησης πληροί τις απαιτήσεις του άρθρου 43 (άρθρο 43 παρ. 4 ΓΚΠΔ). Εάν η διαπίστευση διενεργείται από τον εθνικό οργανισμό διαπίστευσης σύμφωνα με το πρότυπο EN-ISO/IEC 17065/2012 (ISO 17065), πρέπει επίσης να εφαρμόζονται οι συμπληρωματικές απαιτήσεις που έχουν οριστεί από την αρμόδια εποπτική αρχή.

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

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

1. Στο άρθρο 43 παρ. 1 του ΓΚΠΔ προβλέπεται ότι «*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 (20), 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.»

2. Στο άρθρο 43 παρ. 3 του ΓΚΠΔ προβλέπεται ότι «*Η διαπίστευση των φορέων πιστοποίησης όπως αναφέρεται στις παραγράφους 1 και 2 του παρόντος άρθρου πραγματοποιείται βάσει των απαιτήσεων που έχουν εγκριθεί από την εποπτική αρχή που είναι αρμόδια δυνάμει του άρθρου 55 ή 56, ή από το Συμβούλιο Προστασίας Δεδομένων δυνάμει του άρθρου 63. Σε περίπτωση διαπίστευσης δυνάμει του στοιχείου β) της παραγράφου 1 του παρόντος άρθρου, οι εν λόγω απαιτήσεις συμπληρώνουν τις απαιτήσεις που προβλέπονται στον κανονισμό (ΕΚ) αριθ. 765/2008 και τους τεχνικούς κανόνες που περιγράφουν τις μεθόδους και τις διαδικασίες των φορέων πιστοποίησης».*

3. Στο άρθρο 37 παρ. 1 του ν. 4624/2019 προβλέπεται ότι «*Η διαπίστευση των φορέων που χορηγούν πιστοποιήσεις σύμφωνα με το άρθρο 42 του ΓΚΠΔ πραγματοποιείται από το Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.) με βάση το πρότυπο EN-ISO/IEC17065:2012 και σύμφωνα με συμπληρωματικές απαιτήσεις που έχουν οριστεί από την Αρχή.».*

4. Στο άρθρο 43 παρ. 6 του ΓΚΠΔ προβλέπεται ότι «*Οι απαιτήσεις της παραγράφου 3 του παρόντος άρθρου και τα κριτήρια που αναφέρονται στο άρθρο 42 παράγραφος 5 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».

5. Στο άρθρο 64 παρ. 1 του ΓΚΠΔ προβλέπεται ότι «*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 σύμφωνα με το άρθρο 41 παράγραφος 3, φορέα πιστοποίησης σύμφωνα με το άρθρο 43 παράγραφος 3 ή των κριτηρίων πιστοποίησης του άρθρου 42 παράγραφος 5 (…)».

6. Το ΕΣΠΔ εξέδωσε τις κατευθυντήριες γραμμές 4/2018 με τίτλο «*Κατευθυντήριες γραμμές 4/2018 σχετικά με τη διαπίστευση των φορέων πιστοποίησης βάσει του άρθρου 43 του Γενικού Κανονισμού για την Προστασία Δεδομένων (2016/679)*»[1]. Στόχος τους είναι η παροχή καθοδήγησης σχετικά με τον τρόπο ερμηνείας και εφαρμογής των διατάξεων του άρθρου 43 του ΓΚΠΔ ώστε να καθιερωθεί μια συνεκτική και εναρμονισμένη βάση αναφοράς για τη διαπίστευση των φορέων πιστοποίησης που εκδίδουν πιστοποιήσεις σύμφωνα με τον ΓΚΠΔ. Ειδικότερα, στο παράρτημα των κατευθυντήριων αυτών γραμμών παρέχεται καθοδήγηση σχετικά με τρόπους προσδιορισμού συμπληρωματικών απαιτήσεων διαπίστευσης και προτείνονται απαιτήσεις τις οποίες οι εποπτικές αρχές και οι εθνικοί οργανισμοί διαπίστευσης πρέπει να εξετάζουν για τη διασφάλιση της συμμόρφωσης με τον ΓΚΠΔ.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή, αποφασίζει τον ορισμό συμπληρωματικών, σε σχέση με το πρότυπο ISO 17065, απαιτήσεων για τη διαπίστευση των φορέων πιστοποίησης προς εκπλήρωση της υποχρέωσής της όπως απορρέει από το άρθρο 43 παρ. 1 στοιχείο β) και παρ. 3 του ΓΚΠΔ καθώς και το άρθρο 37 παρ. 1 του ν.4624/2019. Οι εν λόγω συμπληρωματικές απαιτήσεις διαπίστευσης βασίζονται στις κατευθυντήριες γραμμές 4/2018 του ΕΣΠΔ

[1] Διαθέσιμες στο σύνδεσμο https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_el

και εφαρμόζονται από το Ε.ΣΥ.Δ. κατά τη διαδικασία διαπίστευσης των φορέων πιστοποίησης σε συνδυασμό με το ως άνω πρότυπο.

Οι παρούσες συμπληρωματικές απαιτήσεις διαπίστευσης υποβάλλονται στο ΕΣΠΔ σύμφωνα με τον προβλεπόμενο στο άρθρο 63 του ΓΚΠΔ μηχανισμό συνεκτικότητας και δεν δημοσιοποιούνται από την Αρχή μέχρι την ολοκλήρωση της εν λόγω διαδικασίας.

Ο Πρόεδρος **Η Γραμματέας**

Κωνσταντίνος Μενουδάκος **Ειρήνη Παπαγεωργοπούλου**

.