Γνώμη 34/2025 σχετικά με το σχέδιο απόφασης της ελληνικής εποπτικής αρχής όσον αφορά τα κριτήρια πιστοποίησης του Κ.Ε.Σ.Δ.

Εκδόθηκε στις 02 Δεκεμβρίου 2025

Εκδόθηκε

Πίνακας περιεχομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 63, το άρθρο 64 παράγραφος 1 στοιχείο γ) και το Άρθρο 42 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 (στο εξής: ΓΚΠΔ),

Έχοντας υπόψη τη συμφωνία για τον ΕΟΧ, και ιδίως το Παράρτημα XI και το Πρωτόκολλο 37, όπως τροποποιήθηκαν με την απόφαση αριθ. 154/2018 της Μεικτής Επιτροπής του ΕΟΧ, της 6ης Ιουλίου 2018[1],

Έχοντας υπόψη το Άρθρο 64 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ και τα Άρθρα 10 και 22 του εσωτερικού κανονισμού του,

Εκτιμώντας τα ακόλουθα:

1 Τα κράτη μέλη, οι εποπτικές αρχές, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (στο εξής: ΕΣΠΔ) και η Ευρωπαϊκή Επιτροπή ενθαρρύνουν, ιδίως σε επίπεδο Ένωσης, τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων (στο εξής: μηχανισμοί πιστοποίησης) και σφραγίδων και σημάτων προστασίας δεδομένων, για την απόδειξη της συμμόρφωσης με τον ΓΚΠΔ των πράξεων επεξεργασίας από υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία, λαμβανομένων υπόψη των ειδικών αναγκών των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων. Επιπλέον, η καθιέρωση πιστοποιήσεων μπορεί να ενισχύσει τη διαφάνεια και να παρέχει στα υποκείμενα των δεδομένων τη δυνατότητα να αξιολογούν το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων και υπηρεσιών.

2 Τα κριτήρια πιστοποίησης αποτελούν αναπόσπαστο μέρος κάθε μηχανισμού πιστοποίησης. Κατά συνέπεια, ο ΓΚΠΔ απαιτεί την έγκριση των εθνικών κριτηρίων πιστοποίησης ενός μηχανισμού πιστοποίησης από την αρμόδια εποπτική αρχή [Άρθρο 42 παράγραφος 5 και Άρθρο 43 παράγραφος 2 στοιχείο β) του ΓΚΠΔ] ή, στην περίπτωση ευρωπαϊκής σφραγίδας προστασίας δεδομένων, από το ΕΣΠΔ [Άρθρο 42 παράγραφος 5 και Άρθρο 70 παράγραφος 1 στοιχείο ιε) του ΓΚΠΔ].

3 Όταν εποπτική αρχή προτίθεται να εγκρίνει πιστοποίηση σύμφωνα με το Άρθρο 42 παράγραφος 5 του ΓΚΠΔ, ο κύριος ρόλος του ΕΣΠΔ είναι να διασφαλίσει τη συνεκτική εφαρμογή του ΓΚΠΔ, μέσω του μηχανισμού συνεκτικότητας που αναφέρεται στα Άρθρα 63, 64 και 65 του ΓΚΠΔ. Στο πλαίσιο αυτό, σύμφωνα με το Άρθρο 64 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ, το ΕΣΠΔ υποχρεούται να εκδώσει γνώμη σχετικά με το σχέδιο απόφασης της εποπτικής αρχής για την έγκριση των κριτηρίων πιστοποίησης.

4 Η παρούσα γνώμη αποσκοπεί στη διασφάλιση της συνεκτικής εφαρμογής του ΓΚΠΔ, μεταξύ άλλων από τις εποπτικές αρχές, τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία, με γνώμονα τα βασικά στοιχεία που πρέπει να αναπτύσσουν οι μηχανισμοί πιστοποίησης. Ειδικότερα, η αξιολόγηση του ΕΣΠΔ διενεργείται με βάση τις «Κατευθυντήριες γραμμές 1/2018 σχετικά με την πιστοποίηση και τον προσδιορισμό κριτηρίων πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 του Κανονισμού» (στο εξής: κατευθυντήριες γραμμές) και το Προσάρτημά τους, με τίτλο «Guidance on certification criteria assessment» (Καθοδήγηση σχετικά με την αξιολόγηση των κριτηρίων πιστοποίησης) (στο εξής: προσάρτημα).

[1] Οι αναφορές στα «κράτη μέλη» στο παρόν έγγραφο θα πρέπει να νοούνται ως αναφορές στα «κράτη μέλη του ΕΟΧ».

5 Σύμφωνα με τα ανωτέρω, το ΕΣΠΔ αναγνωρίζει ότι κάθε μηχανισμός πιστοποίησης θα πρέπει να εξετάζεται μεμονωμένα και με την επιφύλαξη της αξιολόγησης οποιουδήποτε άλλου μηχανισμού πιστοποίησης.

6 Οι μηχανισμοί πιστοποίησης θα πρέπει να παρέχουν τη δυνατότητα στους υπευθύνους επεξεργασίας και στους εκτελούντες την επεξεργασία να αποδεικνύουν τη συμμόρφωση με τον ΓΚΠΔ· ως εκ τούτου, τα κριτήρια πιστοποίησης θα πρέπει να αντικατοπτρίζουν δεόντως τις απαιτήσεις και τις αρχές σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα που ορίζονται στον ΓΚΠΔ και να συμβάλλουν στη συνεκτική εφαρμογή του.

7 Ταυτόχρονα, τα κριτήρια πιστοποίησης θα πρέπει να λαμβάνουν υπόψη και, κατά περίπτωση, να είναι διαλειτουργικά με άλλα πρότυπα, όπως τα πρότυπα ISO, και με άλλες πρακτικές πιστοποίησης.

8 Συνεπώς, οι πιστοποιήσεις θα πρέπει να προσθέτουν αξία σε έναν οργανισμό, συμβάλλοντας στην εφαρμογή τυποποιημένων και καθορισμένων οργανωτικών και τεχνικών μέτρων που αποδεδειγμένα διευκολύνουν και ενισχύουν τη συμμόρφωση των πράξεων επεξεργασίας, λαμβανομένων υπόψη των ειδικών ανά τομέα απαιτήσεων.

9 Το ΕΣΠΔ εκφράζει την ικανοποίησή του για τις προσπάθειες που καταβάλλουν οι ιδιοκτήτες συστημάτων να εκπονήσουν μηχανισμούς πιστοποίησης, οι οποίοι αποτελούν πρακτικά και δυνητικά οικονομικά αποδοτικά εργαλεία για τη διασφάλιση μεγαλύτερης συνεκτικότητας με τον ΓΚΠΔ και για την προώθηση του δικαιώματος στην προστασία της ιδιωτικής ζωής και την προστασία των δεδομένων των υποκειμένων των δεδομένων μέσω της αύξησης της διαφάνειας.

10 Το ΕΣΠΔ υπενθυμίζει ότι οι πιστοποιήσεις αποτελούν εθελοντικά εργαλεία λογοδοσίας και ότι η τήρηση μηχανισμού πιστοποίησης δεν μειώνει την ευθύνη των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία για συμμόρφωση με τον ΓΚΠΔ ούτε εμποδίζει τις εποπτικές αρχές να ασκούν τα καθήκοντα και τις εξουσίες τους σύμφωνα με τον ΓΚΠΔ και τη σχετική εθνική νομοθεσία.

11 Σύμφωνα με το Άρθρο 64 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ σε συνδυασμό με το Άρθρο 10 παράγραφος 2 του εσωτερικού κανονισμού του ΕΣΠΔ, η γνώμη του ΕΣΠΔ εκδίδεται εντός οκτώ εβδομάδων από την πρώτη εργάσιμη ημέρα αφότου η Πρόεδρος και η αρμόδια εποπτική αρχή αποφάσισαν ότι ο φάκελος είναι πλήρης. Με απόφαση της προέδρου, η προθεσμία αυτή μπορεί να παραταθεί κατά έξι ακόμη εβδομάδες, ανάλογα με την πολυπλοκότητα του θέματος.

12 Η γνώμη του EDBP επικεντρώνεται στα κριτήρια πιστοποίησης. Σε περίπτωση που το ΕΣΠΔ απαιτήσει πληροφορίες υψηλού επιπέδου σχετικά με τις μεθόδους αξιολόγησης προκειμένου να είναι σε θέση να εξετάσει διεξοδικά την ελεγξιμότητα του σχεδίου κριτηρίων πιστοποίησης στο πλαίσιο της γνώμης του, η γνώμη αυτή δεν περιλαμβάνει κανενός είδους έγκριση των εν λόγω μεθόδων αξιολόγησης.

Εξέδωσε την ακόλουθη γνώμη:

1 Σύνοψη των πραγματικών περιστατικών

13 Σύμφωνα με το Άρθρο 42 παράγραφος 5 του ΓΚΠΔ και τις κατευθυντήριες γραμμές, τα «ΚΡΙΤΗΡΙΑ ΓΙΑ ΤΗΝ ΠΙΣΤΟΠΟΙΗΣΗ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ ΠΡΑΞΕΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΑ ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ» (στο εξής: «σχέδιο κριτηρίων πιστοποίησης» ή «κριτήρια πιστοποίησης») καταρτίστηκαν από το ΚΕΝΤΡΟ ΕΥΡΩΠΑΪΚΟΥ ΣΥΝΤΑΓΜΑΤΙΚΟΥ ΔΙΚΑΙΟΥ (Κ.Ε.Σ.Δ.) — ΙΔΡΥΜΑ ΤΣΑΤΣΟΥ, νομικό πρόσωπο καταχωρισμένο στην Ελλάδα και υποβλήθηκαν στην ελληνική εποπτική αρχή.

14 Η ελληνική εποπτική αρχή υπέβαλε το οικείο σχέδιο απόφασης σχετικά με την έγκριση των κριτηρίων πιστοποίησης και ζήτησε τη γνώμη του ΕΣΠΔ σύμφωνα με το Άρθρο 64 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ στις 30 Σεπτεμβρίου 2025. Η απόφαση σχετικά με την πληρότητα του φακέλου ελήφθη στις 17 Νοεμβρίου 2025.

15 Το σχέδιο κριτηρίων πιστοποίησης έχει περιορισμένο πεδίο εφαρμογής και εφαρμόζεται μόνο σε συγκεκριμένες πράξεις επεξεργασίας. Καλύπτεται μόνο η πιστοποίηση των πράξεων επεξεργασίας που εκτελούνται από υπευθύνους επεξεργασίας, ενώ εξαιρείται η πιστοποίηση των πράξεων επεξεργασίας που διενεργούνται από εκτελούντες την επεξεργασία.

16 Το ΕΣΠΔ επισημαίνει ότι το περιορισμένο πεδίο εφαρμογής του σχεδίου κριτηρίων πιστοποίησης καλύπτει πράξεις επεξεργασίας που αφορούν δεδομένα εργαζομένων σε σχέση με ορισμένα θέματα (διαδικασίες πρόσληψης, παρακολούθηση του καθεστώτος απασχόλησης, μισθοδοσία, προγράμματα κατάρτισης, πειθαρχικές διαδικασίες, παρακολούθηση και αξιολόγηση της εκτελούμενης εργασίας, διαβιβάσεις δεδομένων εργαζομένων σε αρμόδιες αρχές σύμφωνα με τη νομοθεσία, διαβιβάσεις σε τρίτους — μη κρατικούς φορείς και διαχείριση συστημάτων βιντεοεπιτήρησης). Επιπλέον, το ΕΣΠΔ επισημαίνει ότι οι πράξεις επεξεργασίας στο πλαίσιο της τηλεργασίας των εργαζομένων δεν καλύπτονται από το πεδίο εφαρμογής του σχεδίου κριτηρίων πιστοποίησης (βλ. εξαιρέσεις στο σημείο Α.2). Το ΕΣΠΔ επισημαίνει επίσης την εξαίρεση που προβλέπεται στο σημείο Α.2 για τις «πράξεις επεξεργασίας στο πλαίσιο της εφαρμογής ειδικού κανονιστικού πλαισίου που προβλέπεται από τη νομοθεσία, όπως η διαχείριση εσωτερικών καταγγελιών για παρενόχληση στην εργασία, η αναφορά παραβάσεων (whistleblowing) κ.λπ.» από το πεδίο εφαρμογής του σχεδίου κριτηρίων πιστοποίησης.

17 Η πιστοποίηση των από κοινού υπευθύνων επεξεργασίας βάσει του Άρθρου 26 του ΓΚΠΔ εξαιρείται από το πεδίο εφαρμογής των κριτηρίων πιστοποίησης. Επιπλέον, η πιστοποίηση δεν είναι διαθέσιμη για εταιρείες που δεν διαθέτουν εγκατάσταση εντός του ΕΟΧ όταν διενεργούν επεξεργασία δεδομένων που υπόκειται στις υποχρεώσεις του ΓΚΠΔ σύμφωνα με το Άρθρο 3 παράγραφος 2.

18 Η παρούσα πιστοποίηση δεν αποτελεί πιστοποίηση σύμφωνα με το Άρθρο 46 παράγραφος 2 στοιχείο στ) του ΓΚΠΔ που προορίζεται για διεθνείς διαβιβάσεις δεδομένων προσωπικού χαρακτήρα και, ως εκ τούτου, δεν παρέχει κατάλληλες εγγυήσεις στο πλαίσιο των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς υπό τους όρους που αναφέρονται στο άρθρο 46 παράγραφος 2 στοιχείο στ). Κάθε διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό πραγματοποιείται μόνο εάν τηρούνται οι διατάξεις του κεφαλαίου V του ΓΚΠΔ.

2 Αξιολόγηση

19 Το ΕΣΠΔ διενήργησε την αξιολόγησή του σύμφωνα με τη δομή που προβλέπεται στο παράρτημα 2 των κατευθυντήριων γραμμών (στο εξής: παράρτημα) και στο προσάρτημά του. Όταν η παρούσα γνώμη σιωπά σχετικά με συγκεκριμένο τμήμα του σχεδίου κριτηρίων πιστοποίησης, θα πρέπει να θεωρείται ότι το ΕΣΠΔ δεν έχει παρατηρήσεις και δεν ζητεί από την ελληνική εποπτική αρχή να λάβει περαιτέρω μέτρα.

2.1 Γενικές παρατηρήσεις

20 Το ΕΣΠΔ επισημαίνει ότι σε διάφορα μέρη του σχεδίου κριτηρίων πιστοποίησης γίνεται αναφορά στον «νόμο 4624/2019» χωρίς να διευκρινίζεται τι συνεπάγεται η εν λόγω νομική πράξη. Ως εκ τούτου, το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να συμπεριλάβει ορισμό ή επεξηγηματική σημείωση που να περιγράφει τον εν λόγω νόμο, καθώς και ένδειξη σχετικά με το πού είναι δυνατή η δημόσια πρόσβαση σε αυτόν.

21 Επιπλέον, το ΕΣΠΔ επισημαίνει ότι δεν αναφέρεται σαφώς αν η στήλη «ΕΠΕΞΗΓΗΣΗ» συνιστά κανονιστική απαίτηση ή απλώς παρέχει καθοδήγηση που αναλύει ανεπισήμως τις δεσμευτικές διατάξεις που παρατίθενται στη στήλη «ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΚΡΙΤΗΡΙΟΥ». Ως εκ τούτου, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να αποσαφηνίσει την κανονιστική αξία του μέρους που αναφέρεται ως «επεξήγηση».

22 Κατά την άποψη του ΕΣΠΔ, η διατύπωση του σχεδίου κριτηρίων πιστοποίησης δεν είναι παντού συνεκτική, καθώς σε ορισμένα σημεία γίνεται αναφορά στα «δεδομένα προσωπικού χαρακτήρα των εργαζομένων» ενώ σε άλλα σημεία γίνεται αναφορά σε «πράξεις επεξεργασίας που εμπίπτουν στον στόχο της αξιολόγησης». Συνεπώς, το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να χρησιμοποιήσει συνεπή ορολογία σε ολόκληρο το έγγραφο και να αναφέρεται συστηματικά σε «πράξεις επεξεργασίας που εμπίπτουν στον στόχο της αξιολόγησης» κατά τη διατύπωση των απαιτήσεων.

23 Επιπλέον, σε διάφορα σημεία του σχεδίου κριτηρίων πιστοποίησης, το αντίστοιχο κριτήριο απαιτεί τη συμμόρφωση με τις κατευθυντήριες γραμμές που έχει εκδώσει το ΕΣΠΔ ή με τις εγκεκριμένες κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 (βλ., για παράδειγμα, τμήμα 1.1.5.1 όσον αφορά το ελάχιστο περιεχόμενο των εκτιμήσεων αντικτύπου σχετικά με την προστασία των δεδομένων ή τμήμα 1.1.9.5 όσον αφορά τις διαβιβάσεις κατά παρέκκλιση για ειδικές καταστάσεις). Το ΕΣΠΔ επισημαίνει ότι τα κριτήρια πιστοποίησης αποτελούν αυτοτελές έγγραφο, στο οποίο όλα τα κριτήρια αναλύονται επαρκώς και ειδικώς ώστε να διασφαλίζεται ότι είναι ελέγξιμα. Ως εκ τούτου, για λόγους πληρότητας και ελεγξιμότητας των κριτηρίων, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να αναπτύξει περαιτέρω συγκεκριμένα, ακριβή και ελέγξιμα κριτήρια και να αποφύγει γενικές αναφορές στην υποχρέωση συμμόρφωσης με τις κατευθυντήριες γραμμές που έχουν εκδοθεί από το ΕΣΠΔ ή τις εγκεκριμένες κατευθυντήριες γραμμές της ομάδας εργασίας του Άρθρου 29[2].

[2] Βλ. τη γνώμη 18/2024 του ΕΣΠΔ σχετικά με το σχέδιο απόφασης της αυστριακής εποπτικής αρχής όσον αφορά τα κριτήρια πιστοποίησης της DSGVO-zt GmbH (σημείο 22).

24 Όσον αφορά το τμήμα 1.1.10 του σχεδίου κριτηρίων πιστοποίησης σχετικά με τις «Επικαιροποιήσεις της νομοθεσίας», το ΕΣΠΔ θεωρεί ότι δεν είναι ρεαλιστικό να αναμένονται άμεσες αλλαγές πολιτικής μετά τις νομικές επικαιροποιήσεις, ούτε είναι δυνατόν κάτι τέτοιο να ελεγχθεί. Το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να τροποποιήσει το τμήμα 1.1.10 ώστε να αναμένονται επικαιροποιήσεις χωρίς αδικαιολόγητη καθυστέρηση, λαμβάνοντας παράλληλα υπόψη εύλογο χρονικό διάστημα (π.χ. 30 ή 90 ημέρες) για την αποκατάσταση.

2.2 Πεδίο εφαρμογής του μηχανισμού πιστοποίησης και στόχος της αξιολόγησης

25 Το ΕΣΠΔ επισημαίνει ότι, σύμφωνα με το σχέδιο του κριτηρίου πιστοποίησης Α.1.2, το εδαφικό πεδίο εφαρμογής είναι α) «το έδαφος της Ελληνικής Δημοκρατίας» και β) «το έδαφος οποιασδήποτε χώρας όπου πραγματοποιείται η επεξεργασία δεδομένων εργαζομένων που βρίσκονται στο έδαφος της Ελληνικής Δημοκρατίας και υπό την προϋπόθεση ότι οι δραστηριότητες επεξεργασίας αφορούν την παρακολούθηση της συμπεριφοράς τους ως εργαζομένων, η οποία λαμβάνει χώρα εντός της Ένωσης, ή την παροχή αγαθών ή υπηρεσιών σε αυτούς υπό την ιδιότητά τους ως εργαζομένων». Σύμφωνα με το ΕΣΠΔ, η χρήση της φράσης «οποιασδήποτε χώρας» μπορεί να οδηγήσει σε σύγχυση ως προς το πεδίο εφαρμογής του σχεδίου εθνικών κριτηρίων πιστοποίησης. Κατά συνέπεια, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να τροποποιήσει τα κριτήρια ώστε να διευκρινιστεί ότι το πεδίο εφαρμογής του συστήματος είναι εθνικό σύμφωνα με το άρθρο 42 παράγραφος 5 και το άρθρο 56 του ΓΚΠΔ.

26 Το ΕΣΠΔ επισημαίνει ότι οι όροι «μη κρατικοί φορείς» ή «μη κρατικά όργανα» μπορεί να οδηγήσουν σε σύγχυση και συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να ορίσει ή να αποσαφηνίσει τους όρους «μη κρατικοί φορείς» και «μη κρατικά όργανα».

27 Το ΕΣΠΔ επισημαίνει την εξαίρεση στο σημείο Α.2 των «πράξεων επεξεργασίας στις οποίες χρησιμοποιούνται προηγμένες τεχνολογίες, όπως συσκευές TLS, DLP (πρόληψη της απώλειας δεδομένων), τεχνολογία αλυσίδας συστοιχιών». Ωστόσο, το τμήμα 3 του σχεδίου κριτηρίων πιστοποίησης απαιτεί κρυπτογράφηση, ασφαλή πρωτόκολλα (TLS/HTTPS) και σύγχρονα μέτρα ασφάλειας. Το ΕΣΠΔ θεωρεί μη συνεκτική την εξαίρεση τεχνολογιών που είναι συχνά απαραίτητες για την εκπλήρωση των απαιτήσεων του άρθρου 32 του ΓΚΠΔ. Ως εκ τούτου, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος είτε να διαγράψει την εξαίρεση στο σημείο Α.2 ή να διευκρινίσει ότι η εξαίρεση ισχύει μόνο για την πιστοποίηση της ίδιας της προηγμένης τεχνολογίας (π.χ. πιστοποίηση προϊόντος) και όχι για τη χρήση των εν λόγω τεχνολογιών όταν αποσκοπούν στη διασφάλιση υψηλού επιπέδου ασφάλειας των δεδομένων προσωπικού χαρακτήρα.

2.3 Πράξη επεξεργασίας, άρθρο 42 παράγραφος 1

28 Όσον αφορά το τμήμα 1.1.3. του σχεδίου κριτηρίων πιστοποίησης σχετικά με τα «Δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε πράξεις επεξεργασίας», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να προσθέσει παραπομπή στο άρθρο 10 του ΓΚΠΔ στον τίτλο του τμήματος 1.1.3.

29 Επιπλέον, σύμφωνα με το τμήμα 1.1.3.4 του σχεδίου κριτηρίων πιστοποίησης σχετικά με τα «Δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα», το ΕΣΠΔ επισημαίνει ότι «ο αιτών αποδεικνύει ότι δεν επεξεργάζεται πλήρες ποινικό μητρώο» και ότι γίνεται αναφορά στο εφαρμοστέο εθνικό δίκαιο (δηλαδή στην οδηγία 115/2001 της ελληνικής ΑΠΔ). Το ΕΣΠΔ αντιλαμβάνεται ότι πρόκειται για την εφαρμογή των διατάξεων του άρθρου 10 του ΓΚΠΔ σχετικά με τις προϋποθέσεις υπό τις οποίες μπορεί να επιτραπεί η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα. Το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να προσδιορίσει περαιτέρω —εντός του κριτηρίου και σε σύνδεση με τις σχετικές διατάξεις του εφαρμοστέου εθνικού δικαίου— τις κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (π.χ. περιορισμός πρόσβασης, περίοδος διατήρησης, πιθανά εναλλακτικά αποδεικτικά στοιχεία) κατά την επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα βάσει του τμήματος 1.1.3.4.

30 Το ΕΣΠΔ επισημαίνει ότι δεν είναι σαφές αν το κριτήριο 2.2.1.5 πληροί τις απαιτήσεις των εθνικών διατάξεων που θεσπίζονται δυνάμει του Άρθρου 88 του ΓΚΠΔ, το οποίο επιτρέπει στην εθνική νομοθεσία ή στις συλλογικές συμβάσεις να προβλέπουν ειδικότερους κανόνες για τη διασφάλιση της προστασίας των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων στο πλαίσιο της απασχόλησης. Για παράδειγμα, το κριτήριο 2.2.1.5 σχετικά με την επεξεργασία βιομετρικών δεδομένων θα μπορούσε να οδηγήσει στην εσφαλμένη αντίληψη ότι η παρακολούθηση της εργασίας των εργαζομένων επιτρέπεται (βλ. εν προκειμένω τον στόχο της αξιολόγησης αριθ. 6) χωρίς ειδικούς περιορισμούς όσον αφορά τους νόμιμους επιδιωκόμενους σκοπούς, καθώς και χωρίς ρητές αναφορές στις ειδικές εγγυήσεις που απαιτούνται από το εθνικό δίκαιο, σύμφωνα με το Άρθρο 9 παράγραφος 2 στοιχείο β) και το Άρθρο 88 παράγραφος 2 του ΓΚΠΔ[3]. Το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να προσδιορίσει με ακρίβεια και να συμπεριλάβει παραπομπές στις νομικές απαιτήσεις που προβλέπονται από την εθνική νομοθεσία η οποία έχει θεσπιστεί σύμφωνα με το άρθρο 88 του ΓΚΠΔ.

31 Επιπλέον, το ΕΣΠΔ επισημαίνει ότι η επεξήγηση του κριτηρίου 1.1.5.1 σχετικά με την υποχρέωση διενέργειας εκτίμησης αντικτύπου για την προστασία δεδομένων (στο εξής: ΕΑΠΔ) αναφέρεται σε εκτενή κατάλογο πιθανών δραστηριοτήτων επεξεργασίας που ενδέχεται να μην είναι όλες εφαρμοστέες με βάση το πεδίο εφαρμογής (για παράδειγμα, ορισμένες πράξεις επεξεργασίας ενδέχεται να μην εκτελούνται καθόλου λόγω των απαιτήσεων που προβλέπονται στην εθνική νομοθεσία που έχει θεσπιστεί σύμφωνα με το Άρθρο 88 του ΓΚΠΔ). Ως εκ τούτου, το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να διαγράψει τις εν λόγω αναφορές από τις επεξηγήσεις, ώστε να αποφευχθούν τυχόν ασάφειες.

2.4 Νομιμότητα της επεξεργασίας

2.4.1 Νομική βάση

[3] Η γενική αναφορά στον τίτλο του κριτηρίου στο Άρθρο 9 παράγραφος 2 στοιχεία α) έως θ) φαίνεται να επιτρέπει την επεξεργασία των βιομετρικών δεδομένων των εργαζομένων για την παρακολούθηση και την αξιολόγηση της εργασιακής τους απόδοσης εκτός των ορίων που καθορίζονται στο Άρθρο 9 παράγραφος 2 στοιχείο β) και στο Άρθρο 88 του ΓΚΠΔ.

32 Το ΕΣΠΔ επισημαίνει ότι στο τμήμα 2.2 του σχεδίου κριτηρίων πιστοποίησης με τίτλο «Νομική βάση για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα», ο τίτλος των εν λόγω κριτηρίων παραπέμπει και αναλύει το Άρθρο 9 στοιχεία α) έως θ), αλλά παραλείπει τις αναφορές στο Άρθρο 9 στοιχεία δ), ε), η) και θ). Το ΕΣΠΔ θεωρεί ότι ο τίτλος αυτός μπορεί να είναι παραπλανητικός. Ως εκ τούτου, συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να τροποποιήσει τον τίτλο στο τμήμα 2.2, προκειμένου να συμπεριληφθούν οι διατάξεις του άρθρου 9 στοιχείο δ), ε), η) και θ).

33 Το ΕΣΠΔ σημειώνει το σχέδιο του κριτηρίου πιστοποίησης 2.1.1.1 σχετικά με την «Επεξεργασία βάσει συγκατάθεσης», το οποίο επί του παρόντος ορίζει ότι «ο αιτών πρέπει να αποδείξει ότι η συγκατάθεση του εργαζομένου για την επεξεργασία των δεδομένων του δόθηκε ελεύθερα, σύμφωνα με τους όρους του ΓΚΠΔ, όπως ορίζονται, ιδίως, στο Άρθρο 7, καθώς και στη σχετική διάταξη του Άρθρου 27 παράγραφος 2 του νόμου 4624/2019». Το ΕΣΠΔ υπενθυμίζει τη συνήθη ύπαρξη ανισορροπίας ισχύος στο πλαίσιο της απασχόλησης και σημειώνει ότι θεωρεί προβληματικό οι εργοδότες να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα των υφιστάμενων ή μελλοντικών εργαζομένων βάσει της συγκατάθεσής τους, καθώς είναι απίθανο αυτή να παρέχεται ελεύθερα[4]. Ως εκ τούτου, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να ορίζει ως βάση τη συγκατάθεση μόνο σε περιπτώσεις πραγματικά προαιρετικής, μη απαραίτητης επεξεργασίας, με σαφή και μη επιζήμια διαδρομή άρνησης.

2.5 Γενικές υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία

2.5.1 Υποχρέωση που εφαρμόζεται στους υπευθύνους επεξεργασίας

34 Όσον αφορά το σχέδιο κριτηρίου πιστοποίησης 1.1.8 για τους εκτελούντες την επεξεργασία δεδομένων, το ΕΣΠΔ επισημαίνει ότι η σύμβαση που περιέχει το ελάχιστο περιεχόμενο που απαιτείται βάσει του Άρθρου 28 παράγραφος 3 του ΓΚΠΔ πρέπει να είναι διαθέσιμη ή να υπογράφεται όχι μόνο κατά τον χρόνο του ελέγχου, αλλά ήδη κατά τον χρόνο ανάθεσης των δραστηριοτήτων επεξεργασίας στον εκτελούντα την επεξεργασία. Για τον σκοπό αυτό, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να τροποποιήσει τη διατύπωση του σχεδίου κριτηρίου πιστοποίησης 1.1.8, προκειμένου να διασφαλιστεί η πλήρης ευθυγράμμιση με τον ΓΚΠΔ.

[4] Κατευθυντήριες γραμμές 5/2020 του ΕΣΠΔ σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, έκδοση 1.1, οι οποίες εκδόθηκαν στις 4 Μαΐου 2020, σημείο 21.

35 Όσον αφορά το σχέδιο του κριτηρίου πιστοποίησης 2.5.3 σχετικά με τη γνωστοποίηση παραβίασης στο υποκείμενο των δεδομένων, το ΕΣΠΔ επισημαίνει ότι στο κριτήριο παρατίθενται μέτρα σύμφωνα με το Άρθρο 34 παράγραφος 3 του ΓΚΠΔ που προβλέπονται σε περίπτωση που «ο αιτών δεν αποδείξει τη γνωστοποίηση της παραβίασης στον εργαζόμενο που είναι το υποκείμενο των δεδομένων». Ειδικότερα, ο αιτών πρέπει να αποδείξει ότι η άμεση επικοινωνία με το υποκείμενο των δεδομένων θα συνεπαγόταν δυσανάλογες προσπάθειες. Ωστόσο, λαμβανομένου υπόψη του πεδίου εφαρμογής του κριτηρίου (δηλαδή τα δεδομένα του εργαζομένου), το ΕΣΠΔ θεωρεί ότι μια κατάσταση που συνεπάγεται τέτοιες δυσανάλογες προσπάθειες θα ήταν εξαιρετική. Για τον σκοπό αυτό, το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να αναπτύξει περαιτέρω τις καταστάσεις στις οποίες ενδέχεται να προκύψει η εν λόγω περίπτωση. Επιπλέον, το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να διευκρινίσει ότι η απόδειξη σχετικά με τις «δυσανάλογες προσπάθειες» —στο σχέδιο του κριτηρίου πιστοποίησης 2.5.3— πρέπει να υποβάλλεται στον οργανισμό πιστοποίησης.

2.6 Δικαιώματα των υποκειμένων των δεδομένων

36 Όσον αφορά το τμήμα 4.1.3 σχετικά με την «ταυτοποίηση του υποκειμένου των δεδομένων» (τμήμα επεξήγησης), το σχέδιο κριτηρίων πιστοποίησης αναφέρεται στην τεκμηρίωση που πρέπει να παρέχεται από το υποκείμενο των δεδομένων για την επαλήθευση της ταυτότητάς του κατά τρόπο που θα μπορούσε να θέσει σε κίνδυνο την αρχή της ελαχιστοποίησης των δεδομένων [5] . Προκειμένου να συμμορφωθεί με την αρχή της ελαχιστοποίησης των δεδομένων, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να τροποποιήσει την επεξήγηση του σχεδίου κριτηρίων στο τμήμα 4.1.3, ώστε να δηλώνεται σαφώς ότι η τεκμηρίωση πρέπει να ζητείται από το υποκείμενο των δεδομένων μόνο σε περίπτωση εύλογης αμφιβολίας.

37 Το ΕΣΠΔ επισημαίνει ότι, σύμφωνα με το επεξηγηματικό μέρος του σχεδίου κριτηρίου 4.1.3 (στο τμήμα 4.1 που αφορά τα δικαιώματα των υποκειμένων των δεδομένων), ο αιτών μπορεί να επιλέξει να χρησιμοποιήσει βιομετρικά δεδομένα ως μέθοδο ταυτοποίησης του υποκειμένου των δεδομένων. Στην περίπτωση αυτή, ο αιτών «τεκμηριώνει ότι πληρούνται οι προϋποθέσεις του κριτηρίου 2.2.1.5, ιδίως όσον αφορά τις ειδικές απαιτήσεις ασφάλειας που καθιστούν αναγκαία την επεξεργασία, και το γεγονός ότι η ταυτοποίηση δεν μπορεί να πραγματοποιηθεί αξιόπιστα με ηπιότερα μέσα». Το ΕΣΠΔ επισημαίνει ότι, καταρχήν, η χρήση βιομετρικών δεδομένων δεν θα ήταν αναγκαία και αναλογική για τον χειρισμό της άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων[6] και συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να αποκλείσει τη δυνατότητα χρήσης βιομετρικών δεδομένων για τον χειρισμό της άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων.

[5] Στην επεξήγηση του σχεδίου κριτηρίων πιστοποίησης αναφέρονται τα εξής: Α. Ο αιτών πρέπει να έχει θεσπίσει διαδικασία για την αξιόπιστη επαλήθευση της ταυτότητας των υποκειμένων των δεδομένων που ζητούν πρόσβαση στα δεδομένα τους και πληροφορίες σχετικά με αυτά και να καταγράφει το αποτέλεσμα της διαδικασίας αυτής στο αρχείο αιτημάτων εργαζομένων που τηρεί σύμφωνα με το κριτήριο 4.1.5: — αναγνωριστικά ταυτότητας όπως όνομα, επώνυμο και φωτογραφία— έγγραφα όπως δελτίο ταυτότητας, διαβατήριο, άδεια οδήγησης — επαλήθευση γνώσεων, με την παροχή πληροφοριών που είναι γνωστές μόνο στο υποκείμενο ή δεν είναι διαθέσιμες στο κοινό — ψηφιακή ταυτοποίηση, όπως αδειοπλαίσιο σύνδεσης και κωδικοί πρόσβασης που ενδέχεται να απαιτούνται για διαδικτυακά αιτήματα, όπως ορίζεται στο κριτήριο 4.1.5 — συνδυασμό των ανωτέρω.

[6] Βλ., για παράδειγμα, κατευθυντήριες γραμμές 01/2022 του ΕΣΠΔ σχετικά με τα δικαιώματα των υποκειμένων των δεδομένων — Δικαίωμα πρόσβασης, έκδοση 2.1, που εκδόθηκαν στις 28 Μαρτίου 2023, σημείο 68.

2.7 Κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων

38 Το ΕΣΠΔ εκφράζει την ικανοποίησή του για το σχέδιο των κριτηρίων 1.1.5.2 σχετικά με την «Εκτίμηση αντικτύπου για την προστασία των δεδομένων και προηγούμενη διαβούλευση», όπου τα κριτήρια προβλέπουν ότι «Ο αιτών πρέπει να αποδεικνύει (π.χ. μέσω του ROPA) ότι οι πράξεις επεξεργασίας που εκτελεί σε σχέση με δεδομένα προσωπικού χαρακτήρα των εργαζομένων του δεν συνεπάγονται αυξημένο κίνδυνο για τα δικαιώματα και τις ελευθερίες τους όσον αφορά τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς του, σύμφωνα με το Άρθρο 35 παράγραφος 1 του ΓΚΠΔ». Το ΕΣΠΔ κατανοεί από την επεξήγηση των εν λόγω κριτηρίων ότι ο αιτών περιλαμβάνει στο ROPA τις πληροφορίες σχετικά με το αν απαιτείται ΕΑΠΔ και το αν διενεργήθηκε σύμφωνα με την απαίτηση. Ωστόσο, ο τίτλος των κριτηρίων αυτών είναι «Μη υποχρέωση διεξαγωγής ΕΑΠΔ». Για λόγους σαφήνειας και ακρίβειας, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να αλλάξει τον τίτλο του κριτηρίου 1.1.5.2 ώστε να αντικατοπτρίζει την ουσία των κριτηρίων.

2.8 Τεχνικά και οργανωτικά μέτρα που εγγυώνται την προστασία

39 Το ΕΣΠΔ επισημαίνει ότι ο τρόπος με τον οποίο έχουν διαχωριστεί οι τεχνικές και οργανωτικές απαιτήσεις μεταξύ της στήλης «ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΚΡΙΤΗΡΙΟΥ» και της στήλης «ΕΠΕΞΗΓΗΣΗ» μπορεί να δημιουργήσει ασάφεια ως προς τη σχέση μεταξύ των απαιτήσεων που περιλαμβάνονται και στις δύο στήλες. Για παράδειγμα, όσον αφορά το κριτήριο 3.1.1.3, και οι δύο στήλες περιλαμβάνουν στοιχεία που πρέπει να καλύπτονται από την πολιτική ασφάλειας. Για λόγους ελεγξιμότητας, το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να αναδιοργανώσει το περιεχόμενο των στηλών.

40 Όσον αφορά το τμήμα 3.1.3.1 του σχεδίου κριτηρίων πιστοποίησης σχετικά με την «Αξιοπιστία των μηχανισμών καταγραφής», το ΕΣΠΔ επισημαίνει ότι τα κριτήρια, στην τρέχουσα έκδοσή τους, δεν είναι αρκετά ακριβή ως προς τις κατηγορίες δεδομένων που μπορούν να υποβληθούν σε επεξεργασία, δεδομένου ότι περιλαμβάνουν πεδία «ελεύθερου κειμένου» προς συμπλήρωση. Το ΕΣΠΔ είναι της γνώμης ότι αυτό ενδέχεται να θέσει σε κίνδυνο την αρχή της ελαχιστοποίησης των δεδομένων. Ως εκ τούτου, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να προβλέψει σαφείς και ακριβείς κατηγορίες δεδομένων στο πλαίσιο των κριτηρίων του τμήματος 3.1.3.1 και να καταργήσει τη δυνατότητα συμπλήρωσης πεδίων «ελεύθερου κειμένου».

41 Όσον αφορά το σχέδιο του κριτηρίου πιστοποίησης 3.2.1.1 για την κρυπτογράφηση, το ΕΣΠΔ επισημαίνει ότι η απαίτηση που προβλέπεται στη στήλη «ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΚΡΙΤΗΡΙΟΥ» — «Η κρυπτογράφηση είναι αποτελεσματική» — δεν περιλαμβάνει την επεξήγηση που παρέχεται για τα τεχνικά πρότυπα σε άλλα κριτήρια. Ως εκ τούτου, για λόγους ελεγξιμότητας και συνεκτικότητας, το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να παραπέμπει σε αναγνωρισμένα πρότυπα ή στο επεξηγηματικό μέρος για την περαιτέρω ανάπτυξη των κριτηρίων.

42 Όσον αφορά το τμήμα 3.1.2.5 του σχεδίου κριτηρίων πιστοποίησης σχετικά με την εναλλαγή και την εντροπία των κωδικών πρόσβασης, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να διασφαλίσει ότι οι αιτούντες λαμβάνουν υπόψη τις τελευταίες τεχνολογικές εξελίξεις, σύμφωνα με το Άρθρο 32 του ΓΚΠΔ, κατά τον καθορισμό της πολιτικής τους για τους κωδικούς πρόσβασης.

43 Το ΕΣΠΔ επισημαίνει ότι δεν υπάρχουν κριτήρια σχετικά με την κρυπτογράφηση των αδρανών δεδομένων, παρότι το κριτήριο 3.1.4.3 περιλαμβάνει την κρυπτογράφηση των υπό διαμετακόμιση δεδομένων. Το ΕΣΠΔ είναι της γνώμης ότι τα αδρανή δεδομένα θα πρέπει επίσης να υπόκεινται σε απαιτήσεις κρυπτογράφησης ώστε το σχέδιο κριτηρίων πιστοποίησης να είναι συνεκτικό, λαμβανομένων υπόψη των αποτελεσμάτων της ανάλυσης κινδύνου. Ως εκ τούτου, το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να τροποποιήσει τα κριτήρια, ώστε να διασφαλιστεί ότι καλύπτουν επίσης την κρυπτογράφηση των αδρανών δεδομένων.

44 Όσον αφορά το τμήμα 3.1.4.4 του σχεδίου πιστοποίησης σχετικά με τα εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου, το ΕΣΠΔ επισημαίνει ότι το κριτήριο καλύπτει μόνο τις υπηρεσίες ανταλλαγής αρχείων. Το ΕΣΠΔ επισημαίνει ότι υπάρχουν και άλλες μέθοδοι, όπως η κρυπτογράφηση των συνημμένων εγγράφων. Ως εκ τούτου, το ΕΣΠΔ ενθαρρύνει την ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος να τροποποιήσει το κριτήριο για τα εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου, ώστε να διασφαλιστεί η αποδοχή άλλων τεχνικών μηχανισμών, όπως η κρυπτογράφηση συνημμένων (π.χ. S/MIME, PGP ή κρυπτογραφημένα αρχεία) ή οι υπηρεσίες ανταλλαγής αρχείων (π.χ. υπηρεσίες ανταλλαγής με κρυπτογράφηση από την πλευρά του πελάτη), με τεκμηριωμένη διαχείριση κλειδιών και διαμοιρασμό μυστικού εκτός ζώνης.

3 Συμπεράσματα/Συστάσεις

45 Εν κατακλείδι, το ΕΣΠΔ θεωρεί ότι το παρόν σχέδιο κριτηρίων πιστοποίησης μπορεί να οδηγήσει σε μη συνεκτική εφαρμογή του ΓΚΠΔ και ότι πρέπει να επέλθουν οι ακόλουθες αλλαγές προκειμένου να πληρούνται οι απαιτήσεις που επιβάλλει το Άρθρο 42 του ΓΚΠΔ λαμβανομένων υπόψη των κατευθυντήριων γραμμών και του προσαρτήματος:

46 όσον αφορά τις «γενικές παρατηρήσεις», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος:

1. να αποσαφηνίσει την κανονιστική αξία του μέρους που αναφέρεται ως «επεξήγηση»·

2. να αναπτύξει περαιτέρω συγκεκριμένα, ακριβή και ελέγξιμα κριτήρια και να αποφύγει γενικές αναφορές στην υποχρέωση συμμόρφωσης με τις κατευθυντήριες γραμμές που έχουν εκδοθεί από το ΕΣΠΔ ή τις εγκεκριμένες κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29·

3. να τροποποιήσει το τμήμα 1.1.10 ώστε να αναμένονται επικαιροποιήσεις χωρίς αδικαιολόγητη καθυστέρηση, λαμβάνοντας παράλληλα υπόψη εύλογο χρονικό διάστημα (π.χ. 30 ή 90 ημέρες) για την αποκατάσταση·

47 όσον αφορά το «πεδίο εφαρμογής του μηχανισμού πιστοποίησης και τον στόχο της αξιολόγησης», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος:

1. να τροποποιήσει τα κριτήρια ώστε να διευκρινιστεί ότι το πεδίο εφαρμογής του συστήματος είναι εθνικό σύμφωνα με το Άρθρο 42 παράγραφος 5 και το Άρθρο 56 του ΓΚΠΔ·

2. να ορίσει ή να αποσαφηνίσει τους όρους «μη κρατικοί φορείς» και «μη κρατικά όργανα»·

3. είτε να διαγράψει την εξαίρεση στο σημείο Α.2 είτε να διευκρινίσει ότι η εξαίρεση ισχύει μόνο για την πιστοποίηση της ίδιας της προηγμένης τεχνολογίας (π.χ. πιστοποίηση προϊόντος) και όχι για τη χρήση των εν λόγω τεχνολογιών όταν αποσκοπούν στη διασφάλιση υψηλού επιπέδου ασφάλειας των δεδομένων προσωπικού χαρακτήρα·

48 όσον αφορά την «πράξη επεξεργασίας, Άρθρο 42 παράγραφος 1», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος:

1. να προσθέσει παραπομπή στο Άρθρο 10 του ΓΚΠΔ στην επικεφαλίδα του τμήματος 1.1.3·

2. να προσδιορίσει περαιτέρω —εντός του κριτηρίου και σε σύνδεση με τις σχετικές διατάξεις του εφαρμοστέου εθνικού δικαίου— τις κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (π.χ. περιορισμός πρόσβασης, περίοδος διατήρησης, πιθανά εναλλακτικά αποδεικτικά στοιχεία) κατά την επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα βάσει του τμήματος 1.1.3.4·

49 όσον αφορά τη «νομική βάση», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος:

1. να τροποποιήσει τον τίτλο στο τμήμα 2.2, προκειμένου να συμπεριληφθούν οι διατάξεις του Άρθρου 9 στοιχείο δ), ε), η) και θ)·

2. να ορίζει ως βάση τη συγκατάθεση μόνο σε περιπτώσεις πραγματικά προαιρετικής, μη απαραίτητης επεξεργασίας, με σαφή και μη επιζήμια διαδρομή άρνησης·

50 όσον αφορά τις «γενικές υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος:

να τροποποιήσει τη διατύπωση του σχεδίου του κριτηρίου πιστοποίησης 1.1.8 προκειμένου να διασφαλιστεί η πλήρης ευθυγράμμιση με τον ΓΚΠΔ·

51 όσον αφορά τα «δικαιώματα των υποκειμένων των δεδομένων», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος:

1. να τροποποιήσει την επεξήγηση του σχεδίου κριτηρίων στο τμήμα 4.1.3, ώστε να δηλώνεται σαφώς ότι η τεκμηρίωση πρέπει να ζητείται από το υποκείμενο των δεδομένων μόνο σε περίπτωση εύλογης αμφιβολίας·

2. να αποκλείσει τη δυνατότητα χρήσης βιομετρικών δεδομένων για τον χειρισμό της άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων·

52 όσον αφορά τους «κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος:

να αλλάξει τον τίτλο του κριτηρίου 1.1.5.2 ώστε να αντικατοπτρίζει την ουσία των κριτηρίων·

53 όσον αφορά τα «τεχνικά και οργανωτικά μέτρα που εγγυώνται την προστασία», το ΕΣΠΔ συνιστά στην ελληνική εποπτική αρχή να απαιτήσει από τον ιδιοκτήτη του συστήματος:

1. να προβλέψει σαφείς και ακριβείς κατηγορίες δεδομένων στο πλαίσιο των κριτηρίων του τμήματος 3.1.3.1 και να καταργήσει τη δυνατότητα συμπλήρωσης πεδίων «ελεύθερου κειμένου»·

2. να διασφαλίσει ότι οι αιτούντες λαμβάνουν υπόψη τις τελευταίες τεχνολογικές εξελίξεις, σύμφωνα με το Άρθρο 32 του ΓΚΠΔ, κατά τον καθορισμό της πολιτικής τους για τους κωδικούς πρόσβασης·

3. να τροποποιήσει τα κριτήρια, ώστε να διασφαλιστεί ότι καλύπτουν επίσης την κρυπτογράφηση των αδρανών δεδομένων.

54 Τέλος, σύμφωνα με τις κατευθυντήριες γραμμές, το ΕΣΠΔ υπενθυμίζει επίσης ότι, σε περίπτωση τροποποιήσεων των κριτηρίων συμμόρφωσης με τον ΓΚΠΔ πράξεων επεξεργασίας που αφορούν τα δεδομένα προσωπικού χαρακτήρα των εργαζομένων, που εκπόνησε το Κέντρο Ευρωπαϊκού Συνταγματικού Δικαίου (Κ.Ε.Σ.Δ.) — Ίδρυμα Τσάτσου, οι οποίες συνεπάγονται σημαντικές αλλαγές, η ελληνική εποπτική αρχή θα πρέπει να υποβάλει την τροποποιημένη έκδοση στο ΕΣΠΔ σύμφωνα με το Άρθρο 42 παράγραφος 5 και το Άρθρο 43 παράγραφος 2 στοιχείο β) του ΓΚΠΔ.

4 Τελικές παρατηρήσεις

55 Η παρούσα γνώμη απευθύνεται στην ελληνική εποπτική αρχή και θα δημοσιοποιηθεί σύμφωνα με το Άρθρο 64 παράγραφος 5 στοιχείο β) του ΓΚΠΔ.

56 Σύμφωνα με το Άρθρο 64 παράγραφοι 7 και 8 του ΓΚΠΔ, η εποπτική αρχή, εντός δύο εβδομάδων από την παραλαβή της γνώμης, ανακοινώνει στον πρόεδρο του ΕΣΠΔ με ηλεκτρονικά μέσα κατά πόσον θα τροποποιήσει ή θα διατηρήσει το σχέδιο απόφασής της. Εντός της ίδιας προθεσμίας, υποβάλλει το τροποποιημένο σχέδιο απόφασης ή, εάν δεν προτίθεται να ακολουθήσει τη γνώμη του ΕΣΠΔ, παρέχει τη σχετική αιτιολογία για την οποία δεν προτίθεται να ακολουθήσει τη γνώμη του, στο σύνολό της ή εν μέρει. Η εποπτική αρχή ανακοινώνει την τελική απόφαση στο ΕΣΠΔ προκειμένου να συμπεριληφθεί στο μητρώο αποφάσεων που εξετάστηκαν στο πλαίσιο του μηχανισμού συνεκτικότητας, σύμφωνα με το Άρθρο 70 παράγραφος 1 στοιχείο κε) του ΓΚΠΔ.

57 Το ΕΣΠΔ υπενθυμίζει ότι, σύμφωνα με το Άρθρο 43 παράγραφος 6 του ΓΚΠΔ, η ελληνική εποπτική αρχή δημοσιοποιεί τα «ΚΡΙΤΗΡΙΑ ΓΙΑ ΤΗΝ ΠΙΣΤΟΠΟΙΗΣΗ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ ΠΡΑΞΕΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΑ ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ» σε εύκολα προσβάσιμη μορφή και τα διαβιβάζει στο ΕΣΠΔ για να συμπεριληφθούν στο δημόσιο μητρώο μηχανισμών πιστοποίησης και σφραγίδων προστασίας δεδομένων, σύμφωνα με το Άρθρο 42 παράγραφος 8 του ΓΚΠΔ.

Για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η πρόεδρος

Anu Talus