ΑΠΑΙΤΗΣΕΙΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΔΙΑΧΕΙΡΙΣΗΣ

ΠΑΡΑΡΤΗΜΑ Γ
ISO/IEC 27701:2019

ΠΡΟΣΘΕΤΕΣ ΠΛΗΡΟΦΟΡΙΕΣ / ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΗΝ ΕΠΙΘΕΩΡΗΣΗ

1. Η πιστοποίηση σύμφωνα με το πρότυπο ISO/IEC 27701 προϋποθέτει ότι ο Οργανισμός:
    a) Αιτείται ταυτόχρονα πιστοποίηση για το πρότυπο ISO/IEC 27001, ή
    b) Είναι ήδη πιστοποιημένος* ως προς το πρότυπο ISO/IEC 27001 και το πιστοποιητικό του είναι σε ισχύ.

    Σημείωση b): Πιστοποιημένος ως προς το πρότυπο ISO/IEC 27001 από την Q-CERT ή από άλλο διαπιστευμένο φορέα πιστοποίησης.

    Στην περίπτωση που αιτηθείτε επιθεώρηση πιστοποίησης μεμονωμένα για το πρότυπο ISO/IEC 27701 θα πρέπει να γνωρίζεται ότι θα απαιτηθεί επιπρόσθετος χρόνος για τον έλεγχο των κύριων στοιχείων διαχείρισης του συστήματος ISO/IEC 27001 που εφαρμόζετε.
2. Η διάρκεια ισχύος του πιστοποιητικού συνδέεται άρρητα και ακολουθεί αυτή του ISO/IEC 27001. Αυτό σημαίνει ότι εάν ένας Οργανισμός έχει σε ισχύ πιστοποιητικό ISO/IEC 27001 το οποίο λήγει για παράδειγμα σε ένα έτος και ο Οργανισμός αποφασίσει να πιστοποιηθεί και ως προς τις απαιτήσεις του ISO/IEC 27701, τότε στην περίπτωση της επιτυχούς κατάληξης της διαδικασίας πιστοποίησης το πιστοποιητικό που θα εκδοθεί θα έχει αρχική ημερομηνία την ημερομηνία λήψης της απόφασης πιστοποίησης και ημερομηνία λήξης ίδια με αυτή του πιστοποιητικού ISO/IEC 27001.
3. Σύμφωνα με το παραπάνω εάν για οποιοδήποτε λόγο ανασταλεί ή διακοπεί η ισχύς του πιστοποιητικού ISO/IEC 27001 του Οργανισμού τότε αυτομάτως αναστέλλεται ή διακόπτεται και η ισχύς του πιστοποιητικού του για το πρότυπο ISO/IEC 27701.
4. Το πεδίο εφαρμογής του συστήματος διαχείρισης του Οργανισμού για το πρότυπο ISO/IEC 27701 μπορεί να είναι διαφορετικό από αυτό του ISO/IEC 27001 δηλαδή να αφορά συγκεκριμένες υπηρεσίες / προϊόντα / διεργασίες υπό την προϋπόθεση όμως ότι τα προαναφερόμενα συμπεριλαμβάνονται στο πεδίο εφαρμογής του ISO/IEC 27001.
5. Ο Οργανισμός μπορεί να έχει μία κοινή «Δήλωση Εφαρμογής» (Statement of Applicability) που να καλύπτει και τα δύο πρότυπα ή δύο ξεχωριστές.
6. Η διάρκεια της επιθεώρησης και για τις δύο περιπτώσεις (συνδυασμένη για τα δύο πρότυπα ή ξεχωριστή για το ISO/IEC 27701) καθορίζεται από τα υποστηρικτικά προς αυτό πρότυπα και από τις απαιτήσεις του Φορέα Διαπίστευσης. Εξαρτάται δε από το ρόλο του Οργανισμού ως προς τη διαχείριση των Ιδιωτικών/Προσωπικών Δεδομένων (PII) δηλαδή εάν απλά επεξεργάζεται τις πληροφορίες αυτές ή εάν είναι ο ελεγκτής των πληροφοριών ή εάν ταυτόχρονα ελέγχει και επεξεργάζεται τις πληροφορίες.

Σημείωση: Το παρόν, σε συνδυασμό με τον κανονισμό πιστοποίησης αποτελούν μέρος των δεσμεύσεων που υπογράφει ότι αποδέχεται ο πελάτης μέσω της σύμβασης (F-2002) με το Φορέα.

7. Εάν κατά τη διάρκεια της επιθεώρησης ανιχνευτεί ότι ο ρόλος τον οποίο έχει δηλώσει ο Οργανισμός μέσω της αίτησής του δεν ανταποκρίνεται στην πραγματικότητα τότε ο χρόνος επιθεώρησης και αντίστοιχα το κόστος αυτής θα τροποποιηθεί (σε συνεννόηση με τα κεντρικά της Q-CERT).
8. Στην περίπτωση που η επιθεώρηση δεν είναι συνδυασμένη και για τα δύο πρότυπα, ο/οι επιθεωρητής(ες) θα πραγματοποιήσουν και έλεγχο σε βασικά στοιχεία του Συστήματος Διαχείρισης Ασφάλειας των Πληροφοριών (ISO/IEC 27001) όπως για παράδειγμα, εσωτερικές επιθεωρήσεις και διοικητική ανασκόπηση.

ΠΡΟΣΘΕΤΕΣ ΠΛΗΡΟΦΟΡΙΕΣ / ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΗΝ ΕΠΙΘΕΩΡΗΣΗ

Ο ρόλος του Οργανισμού (πελάτη) ως προς τη Διαχείριση Δεδομένων Ιδιωτικού/Προσωπικού Χαρακτήρα

Ο Οργανισμός (πελάτης) θα πρέπει να καθορίσει και να μας δηλώσει υπεύθυνα το «ρόλο» του σχετικά με τη Διαχείριση Ιδιωτικών/Προσωπικών Πληροφοριών, δηλαδή εάν:

- ✓ Απλά επεξεργάζεται τέτοιου είδους πληροφορίες (processor), ή
- ✓ Είναι ο ελεγκτής τέτοιων πληροφοριών (controller), ή
- ✓ Ελέγχει και επεξεργάζεται τέτοιες πληροφορίες (processor & controller).

Για να επιλέξετε το σωστό δίνονται οι ακόλουθες πληροφορίες / επεξηγήσεις:

1. ***«Επεξεργαστής» (processor):***

   Επεξεργάζεται ιδιωτικά/προσωπικά δεδομένα μόνο για λογαριασμό του «ελεγκτή». Άρα, ο υπεύθυνος επεξεργασίας δεδομένων δεν είναι «ιδιοκτήτης» των δεδομένων που επεξεργάζεται ούτε έχει τον έλεγχο αυτών.

   Αυτό σημαίνει ότι δεν μπορεί να αλλάξει τον σκοπό και τα μέσα στα οποία χρησιμοποιούνται τα δεδομένα. Ακολουθώντας το παραπάνω παράδειγμα, ο υπεύθυνος επεξεργασίας δεδομένων είναι η εταιρεία τρίτου μέρους που ο «ελεγκτής» των δεδομένων επέλεξε να χρησιμοποιήσει και να επεξεργαστεί τα δεδομένα.

   Οι υπεύθυνοι επεξεργασίας δεδομένων δεσμεύονται από τις οδηγίες που δίνονται από τον «ελεγκτή» των δεδομένων.

2. ***«Ελεγκτής» (controller):***

   Ο ελεγκτής καθορίζει τους σκοπούς για τους οποίους και τα μέσα με τα οποία υποβάλλονται σε επεξεργασία τα ιδιωτικά/προσωπικά δεδομένα. Οι ελεγκτές λαμβάνουν αποφάσεις σχετικά με τις δραστηριότητες επεξεργασίας, ασκούν τον συνολικό έλεγχο των ιδιωτικών/προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία και είναι τελικά υπεύθυνοι για αυτά και για την επεξεργασία αυτών.

3. ***«Επεξεργαστής & Ελεγκτής» (processor & controller):***

   Όταν οι δραστηριότητές του καλύπτουν και τις δύο παραπάνω περιπτώσεις.

Παράδειγμα:

Μία εταιρεία δημοσκοπήσεων (Α) η οποία πραγματοποιεί την όλη διαδικασία συλλογής δεδομένων έχει συνάψει σύμβαση με εταιρεία πληροφορικής (Β) στην οποία αναθέτει την ανάλυση των δεδομένων και την αποστολή τους στους ενδιαφερόμενους. Η (Α) καθορίζει τα δεδομένα που θα χρησιμοποιηθούν, την μορφή που θα πρέπει να έχουν τα αποτελέσματα της ανάλυσης και τον

Σημείωση: Το παρόν, σε συνδυασμό με τον κανονισμό πιστοποίησης αποτελούν μέρος των δεσμεύσεων που υπογράφει ότι αποδέχεται ο πελάτης μέσω της σύμβασης (F-2002) με το Φορέα.

τρόπο αποτύπωσής / παρουσίασής τους σε μία έκθεση με καθορισμένη μορφή, η (Β) αναλύει τα δεδομένα, τα αποθηκεύει στο σύστημά της, ετοιμάζει την έκθεση και τη στέλνει στον πελάτη όπως του έχει καθορίσει η (Α).

Στην περίπτωση αυτή η εταιρεία (Α) είναι ο «Ελεγκτής» και η (Β) ο «επεξεργαστής».

Προσοχή:

Πάροχοι εξειδικευμένων υπηρεσιών πχ λογιστές, θεωρούνται πάντα ως ελεγκτές. Ο λόγος που συμβαίνει αυτό είναι γιατί πρέπει να εργάζονται σύμφωνα με ορισμένα επαγγελματικά πρότυπα και υποχρεούνται να αναλαμβάνουν την ευθύνη για τυχόν προσωπικά δεδομένα που προσλαμβάνονται να επεξεργαστούν.

Για παράδειγμα, εάν ο λογιστής ανακαλύψει κάποια αθέμιτη πρακτική κατά τη συμπλήρωση των λογιστικών της εταιρείας, μπορεί να αναμένεται να αναφέρει αυτή την κακή πρακτική στην αστυνομία ή σε άλλες αρχές.

Εάν αναγκαστούν να προβούν σε αυτήν την ενέργεια, δεν θα ενεργούν πλέον σύμφωνα με τις οδηγίες του πελάτη τους, αλλά σύμφωνα με τις δικές τους επαγγελματικές υποχρεώσεις και επομένως ως ελεγκτές δεδομένων από μόνοι τους.

Οι ειδικοί πάροχοι υπηρεσιών που επεξεργάζονται δεδομένα σύμφωνα με τις δικές τους επαγγελματικές υποχρεώσεις θα ενεργούν πάντα ως ελεγκτές.

Σημείωση: Το παρόν, σε συνδυασμό με τον κανονισμό πιστοποίησης αποτελούν μέρος των δεσμεύσεων που υπογράφει ότι αποδέχεται ο πελάτης μέσω της σύμβασης (F-2002) με το Φορέα.

- REVISION HISTORY -

Revision No	Revision Date	Nature of Change	Review and Approval
0	June 5, 2023	Original Issue	VN / LDK