Ο Ρόλος των Ανεξάρτητων Φορέων Πιστοποίησης στην Εφαρμογή του Ευρωπαϊκού Κανονισμού για τα Προσωπικά Δεδομένα

ΗΜΕΡΙΔΑ ΙΣΑ

03 ΜΑΡΤΙΟΥ 2018

Κατσάπη Αγγελική
Διεθνής Επιθεωρήτρια Πιστοποιήσεων Υπηρ. Υγείας -
Διευθύνουσα Σύμβουλος
Swiss Approval Technische Bewertung

GENERAL
DATA
PROTECTION
REGULATION

Απαίτηση αναθεώρησης του υφιστάμενου νομικού πλαισίου και αντικατάστασή του από τον Κανονισμό 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (GDPR)

Λόγοι

- εξάπλωση της χρήσης του διαδικτύου σε παγκόσμιο επίπεδο,
- ολοένα και αυξανόμενη χρήση cloud services,
- προώθηση υπηρεσιών Big Data Analysis ,
- αύξηση κινδύνου διαρροής και ανέλεγκτης χρήσης και εκμετάλλευσης πληροφοριών
- ανάγκη εναρμόνισης των πολυεθνικών δραστηριοτήτων οργανισμών/ εταιρειών (διεθνών συνεργασιών εκτός Ευρώπης)

Ειδικής κατηγορίας δεδομένα

- γενετικά
- βιομετρικά δεδομένα – πληροφορίες που αποθηκεύονται σε ιατρικές συσκευές
- δεδομένα που αφορούν την κατάσταση υγείας του ατόμου

Ο Κανονισμός 2016/679 (GDPR) προβλέπει

- την έγκριση κωδίκων δεοντολογίας ("Κώδικες") και τη
- ***διαπίστευση πιστοποιήσεων, σφραγίδων και σημάτων*** για να βοηθήσει τους υπεύθυνους επεξεργασίας και τους επεξεργαστές να αποδείξουν τη συμμόρφωση και τις βέλτιστες πρακτικές

ΚΩΔΙΚΑΣ ΔΕΟΝΤΟΛΟΓΙΑΣ (CODE OF CONDUCT)

- Οι ενώσεις και οι αντιπροσωπευτικοί φορείς, (Ιατρικός Σύλλογος Αθηνών) μπορούν να καταρτίζουν κώδικες για έγκριση, καταχώριση και δημοσίευση από την εποπτική αρχή (Αρχή Προστασίας Δεδομένων)
- Η Ευρωπαϊκή Επιτροπή μπορεί να δηλώσει ότι οι κώδικες που συνιστά το EDPB (Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων) έχουν γενική εγκυρότητα εντός της ΕΕ.

Μοντέλο ‘’Semi self – regulating’’

- ***Κώδικας Δεοντολογίας από τις επαγγελματικές ή/και επιστημονικές ενώσεις***
- ***Δηλώσεις Συμμόρφωσης Φυσικών Προσώπων-Επαγγελματιών (****κατά τις Δηλώσεις CE Mark των κατασκευαστών προϊόντων προς απόδειξη εναρμόνισης με Ευρωπαϊκές Οδηγίες****) - Πιστοποίηση Νομικών Προσώπων***
- ***Η συμμόρφωση με τους Κώδικες θα υπόκειται σε παρακολούθηση, η οποία θα πρέπει να διεξάγεται από διαπιστευμένους οργανισμούς με τις κατάλληλες διαπιστεύσεις***.

Ο Ρόλος του Ιατρικού Συλλόγου – Αρχών Αδειοδότησης

- Ο σχετικός κώδικας μπορεί να προβλέπει αναστολή της συμμετοχής των παρόχων/ επαγγελματιών στον αντιπροσωπευτικό τους φορέα (Ιατρικό σύλλογο) και αναφορά στην Αρχή Προστασίας Προσωπικών Δεδομένων στην περίπτωση μη συμμόρφωσης
- ***Γνωστοποίηση δηλώσεων συμμόρφωσης και πιστοποιήσεων καθώς και των παραβιάσεων του Κώδικα- Ανακλήσεων των Πιστοποιητικών***

Πρόβλεψη Πιστοποίησης – Ενθάρρυνση για καθιέρωση της Πιστοποίησης Συμμόρφωσης ως βασικού μέσου για την

- *Απόδειξη εφαρμογής οργανωτικών, λειτουργικών και τεχνικών μέτρων για τη συμμόρφωση με τις απαιτήσεις του Κανονισμού*
- *Απόδειξη συμμόρφωσης για Εισαγωγείς δεδομένων εκτός ΕΕ/ΕΟΧ εφαρμόζουν επαρκείς διασφαλίσεις για το άρθρο 46 του Κανονισμού*
- *Απόδειξη ελέγχου από ένα Τρίτο Ανεξάρτητο Μέρος- Φορέα Πιστοποίησης* ***με επάρκεια για τον έλεγχο και την αξιολόγηση*** *της εφαρμογής των διατάξεων του Κανονισμού*

Πιστοποίηση Συμμόρφωσης κατά τις διατάξεις GDPR

Διαπίστευση κατά 17065

- *Οργανισμοί Διαπίστευσης – μέλη ΕΑ –IAF*
- *Ειδικά κριτήρια διαπίστευσης – πιστοποίησης (??)(πρόβλεψη από εθνικό νόμο)*
- *Ανάγκη ομογενοποίησης κριτηρίων για τη διασφάλιση ισοτιμίας των Πιστοποιητικών με Διαπίστευση από διαφορετικούς φορείς εντός ή και εκτός Ευρώπης (προδιαγραφές από EDPB, Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων ή εναρμόνιση προϋποθέσεων μεταξύ των εθνικών αρχών ΠΔ)* ***ΟΧΙ ΕΘΝΙΚΟ ΠΡΟΤΥΠΟ***

Ο προαιρετικός χαρακτήρας που προσδίδει ο Κανονισμός στην πιστοποίηση δεν αποκλείει ότι στο μέλλον δεν θα απαιτείται τόσο στις συναλλαγές με το Δημόσιο, όσο και στις συναλλαγές μεταξύ ιδιωτών η προσκόμιση πιστοποιητικού συμμόρφωσης με το GDPR, όπως έχει συμβεί στο παρελθόν με αρκετά πιστοποιητικά ποιότητας που απαιτούνται ρητώς στις συναλλαγές.

Π.χ.

- *Πιστοποίηση ΕΝ 15224 για την αδειοδότηση των μονάδων εξωσωματικής*
- *Πιστοποίηση διαγνωστικών εργαστηρίων και μονάδων Υγείας κατά ISO 9001, διαπίστευση εργαστηρίων κατά ISO 15189 για σύναψη σύμβασης με ΕΟΠΥΥ*
- *Πιστοποίηση εργολάβων δημοσίου με ISO 14001 για τη διατήρηση Συστημάτων Διαχείρισης Περιβαλλοντικών Επιπτώσεων κ.λπ.*

Πιστοποίηση Συμμόρφωσης κατά τις διατάξεις GDPR

Συσχετισμός Συμμόρφωσης GDPR με Πιστοποιημένα Συστήματα κατά ISO 9001 - 27001

ISO 9001:2015 και ISO 27001:2013 – μεθοδολογίες/ εργαλεία για την υποστήριξη της εφαρμογής των απαιτήσεων συμμόρφωσης

Data Mapping – Ροές διαχείρισης δεδομένων (βασίζονται στις τυποποιημένες διαδικασίες - Standardized Operational Procedures)

DPIA (Data Protection Impact Assessment) εντάσσεται στο ευρύτερο πλαίσιο του Risk-based thinking και Risk-assessment

Διαχείριση Προστασίας και Ασφάλειας των Δεδομένων/ Πληροφοριών μέσα από Διεθνή πρότυπα

Τα απαιτούμενα από τον GDPR μέτρα, πολιτικές και διαδικασίες ασφάλειας δεδομένων και επιχειρησιακής συνέχειας καθορίζονται από διεθνή πρότυπα και οδηγίες:

ISO 27001, το βασικό διεθνές πρότυπο για την ασφάλεια πληροφοριών

ISO 22301, το διεθνές πρότυπο για την επιχειρησιακή συνέχεια

PCI, το διεθνές πρότυπο για τις επιχειρήσεις που διαχειρίζονται δεδομένα καρτών πληρωμών

ISO 27018, οδηγία για την προστασία των προσωπικών δεδομένων στο cloud

ISO 27017, οδηγία για την ασφάλεια των δεδομένων στην παροχή υπηρεσιών μέσω cloud

ISO 27799, οδηγία για την ασφάλεια των δεδομένων υγείας

ISO 27011, οδηγία για την ασφάλεια των δεδομένων στους τηλεπικοινωνιακούς οργανισμούς

ISO 27015, οδηγία για την ασφάλεια δεδομένων στις οικονομικές υπηρεσίες.

ΣΥΜΠΕΡΑΣΜΑΤΑ

- **Ανάγκη ενίσχυσης τεχνογνωσίας και εμπειριών σε σχέση με την ασφάλεια διαχείρισης δεδομένων (εκπαίδευση προσωπικού IT, DPO, επιθεωρητών, αξιολογητών ΕΣΥΔ κ.λπ.)**
- **Ανάγκη διαβάθμισης των μέτρων συμμόρφωσης**
- **Ανάγκη ελέγχου της αγοράς Πιστοποίησης (proof of competence)**
- **Ανάγκη δημιουργίας πλαισίου πιστοποίησης ΔΙΑΣΦΑΛΙΖΟΝΤΑΣ ΤΗΝ ΙΣΟΤΙΜΗ ΑΝΑΓΝΩΡΙΣΗ των πιστοποιητικών**
- **Ανάγκη ελέγχου της αγοράς Πληροφορικής σε σχέση με τη συμμόρφωση των χρησιμοποιούμενων τεχνολογιών**

ΚΑΤΣΑΠΗ ΑΓΓΕΛΙΚΗ, CEO
SWISS APPROVAL TECHNISCHE BEWERTUNG
katsapi@swissapproval.ch
www.swissapproval.ch
Mob. +30 6932339017