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

APPROVAL
SWISS
Objectively True

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(διεθνών συνεργασιών εκτός Ευρώπης)

APPROVAL SWISS Objectively True

- **Προσωπικά Δεδομένα**

- Όνομα / ταυτότητα / δεδομένα τοποθεσίας
- Παράγοντες που προσδιορίζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του ατόμου

- **Ειδικής κατηγορίας δεδομένα**

- γενετικά - βιομετρικά δεδομένα (τηλεϊατρική)
- πληροφορία σε εικόνα/ κείμενο/ αριθμούς/ video
- δεδομένα που αφορούν στην κατάσταση υγείας- προγνωστικά κινδύνου ασφαλιστικών προγραμμάτων
- Φυλετικά, εθνοτικά, θρησκευτικά, πολιτικά δεδομένα

Ο Κανονισμός 2016/679 (GDPR) προβλέπει στο άρθρο 40

- Την εκπόνηση κωδίκων δεοντολογίας ("Κώδικες")

- Διαπίστευση πιστοποιήσεων, σφραγίδων και σημάτων

Μοντέλο ‘’Semi self – regulating’’

- *Κώδικας Δεοντολογίας από τις επαγγελματικές ή/και επιστημονικές ενώσεις*
- *Δηλώσεις Συμμόρφωσης Φυσικών Προσώπων*
- *Η συμμόρφωση με τους Κώδικες θα υπόκειται σε παρακολούθηση, η οποία θα πρέπει να διεξάγεται από διαπιστευμένους οργανισμούς με τις κατάλληλες διαπιστεύσεις.*
- *Γνωστοποίηση δηλώσεων συμμόρφωσης και πιστοποιήσεων καθώς και των παραβιάσεων του Κώδικα- Ανακλήσεων των Πιστοποιητικών*
- *Πιστοποίηση Νομικών Προσώπων*

Πιστοποίηση Συμμόρφωσης κατά τις διατάξεις GDPR

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 ελέγχου της εφαρμογής των διατάξεων του Κανονισμού*

APPROVAL
SWISS
Objectively True

- *Οργανισμοί Διαπίστευσης – μέλη ΕΑ –IAF*
- *Ειδικά κριτήρια διαπίστευσης – πιστοποίησης 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)*
- *Διεργασίες Πιστοποίησης και Διαπίστευσης Φορέων για GDPR COMPLIANCE – **Υπό Διαμόρφωση***

Πιστοποίηση Συμμόρφωσης κατά τις διατάξεις GDPR

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.*
- *Απαίτηση από ασφαλιστικούς οργανισμούς για εργολάβους- υπεργολάβους έργων, για υγειονομικούς παρόχους*
- *Απαίτηση από ταξιδιωτικούς πράκτορες για τη διακίνηση διεθνών τουριστών*

APPROVAL SWISS Objectively True

Συσχετισμός Συμμόρφωσης GDPR με Πιστοποιημένα Συστήματα κατά ISO 9001 - 27001

APPROVAL
SWISS
Objectively True


Clause/ Subclause: 8.4, 9.1.3, 9.3.2
RELATIONSHIP MANAGEMENT
Clause/Subclause: 4.4, 8.1
PROCESS APPROACH
LEADERSHIP
Clause/ Subclause: 5, 6.2, 6.2, 7.1.4
ISO 9001:2015
Principles Applicable to the Quality Management Standard
Clause/ Subclause: 7.1.5, 9.1.1, 9.1.3, 9.3
EVIDENCE BASED DECISION MAKING
CUSTOMER FOCUS
Clause/Subclause: 4.1, 4.2, 5.1, 8.2, 9.1.2, 9.3, 10.1
IMPROVEMENT
Clause/ Subclause: 4.4, 10.3
ENGAGEMENT OF PEOPLE
Clause/ Subclause: 5.3, 7.1.2, 7.1.6, 7.2, 7.3, 7.4

ISO 9001:2015

ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΟΙΟΤΗΤΑΣ:

Βασίζεται σε 8 αρχές ποιότητας:

Αρχή 1: Εστίαση στον Πελάτη

Αρχή 2: Ηγεσία (ρόλος της διοικήσης)

Αρχή 3: Συμμετοχή του Ανθρώπινου Δυναμικού

Αρχή 4: Διεργασιοκεντρική Προσέγγιση

Αρχή 5: Συστημική Προσέγγιση Διαχείρισης

Αρχή 6: Συνεχής Βελτίωση

Αρχή 7: Λήψη Αποφάσεων βασισμένη σε δεδομένα

Αρχή 8: Αμοιβαία ωφέλιμες σχέσεις με προμηθευτές

- **Πλαίσιο Οργάνωσης και ηγεσίας:**

- Καθορισμός των παραγόντων (εσωτερικών ή εξωτερικών) που δύναται να επηρεάσουν τα αποτελέσματα του Συστήματος Διαχείρισης Ποιότητας

- **Ανάλυση και Διαχείριση των Κινδύνων**

- Αναγνώριση των κινδύνων σχετικά με την λειτουργία, επιτυχία αναμενόμενων αποτελεσμάτων και συνεχής βελτίωση

- **Στόχοι, Μέτρηση και Διαχείριση Αλλαγών**

- Στόχοι σύμφωνοι με την πολιτική του οργανισμού, μετρήσιμοι και να σχετίζονται με τις απαιτήσεις πελατών και συμμόρφωση της υπηρεσίας

- **Επικοινωνία και Ευαισθητοποίηση**

- Ενήμεροι οι υπάλληλοι για πολιτική, στόχους και λειτουργία της εταιρείας

ISO 27001:2013

- **Ο επίσημος τίτλος του προτύπου είναι «Τεχνολογία Πληροφοριών- Τεχνικές Ασφαλείας - Απαιτήσεις των Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών»**

- Οι Οργανισμοί που πληρούν τις προδιαγραφές του προτύπου υποβάλλοντας αίτηση πιστοποίησης έχουν τη δυνατότητα μετά την επιτυχή ολοκλήρωση μιας αναλυτικής διαδικασίας ελέγχου να λάβουν επίσημα Πιστοποιητικό διασφάλισης συμμόρφωσης από το Διαπιστευμένο Φορέα μας για τον εν λόγω πρότυπο.

Συσχετισμός Συμμόρφωσης GDPR με Πιστοποιημένα Συστήματα κατά ISO 27001

Το **πρότυπο 27001:2013** περιλαμβάνει 10 συνοπτικές ενότητες, καθώς και ένα εξαιρετικά αναλυτικό παράρτημα:

- Πεδίο εφαρμογής του προτύπου
- Αναφορά εγγράφων
- Επαναχρησιμοποίηση των όρων και των ορισμών του προτύπου ISO / IEC 27000
- Οργανωτικό πλαίσιο και ενδιαφερόμενα μέρη
- Ηγεσία της Ασφάλειας της Πληροφορίας και υποστήριξη υψηλού επιπέδου για την εφαρμογή πολιτικών
- Σχεδιασμός ενός συστήματος διαχείρισης ασφάλειας πληροφοριών· αξιολόγηση κινδύνων· αντιμετώπιση κινδύνων
- Υποστήριξη του συστήματος διαχείρισης ασφάλειας πληροφοριών
- Δημιουργώντας ένα λειτουργικό επιχειρησιακό σύστημα διαχείρισης ασφάλειας πληροφοριών
- Επανεξέταση της απόδοσης του συστήματος
- Διορθωτικές ενέργειες

APPROVAL SWISS Objectively True

Οι Τεχνικές Επιθεώρησης ως εργαλεία του Data Protection Officer

APPROVAL
SWISS
Objectively True

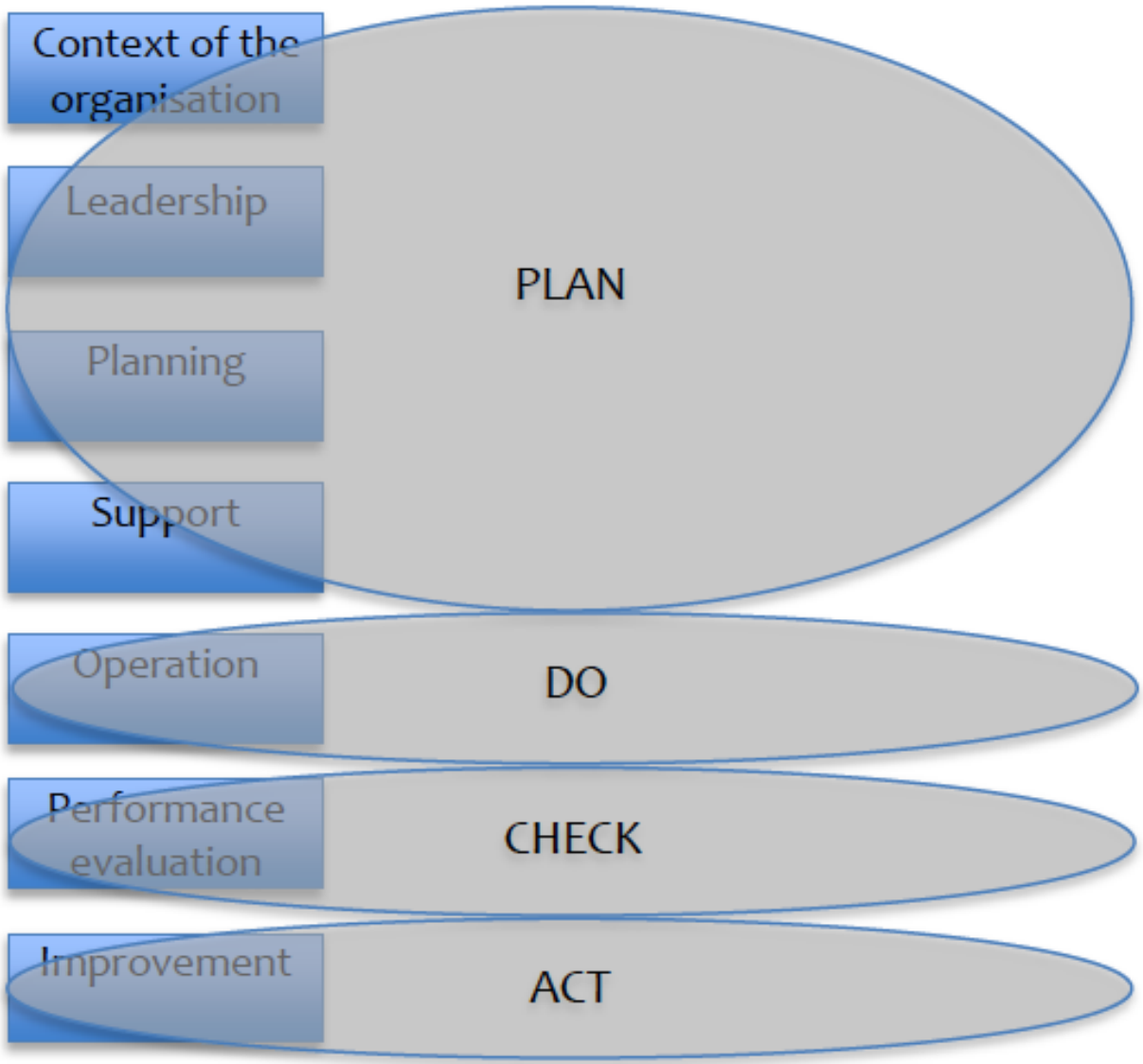

Figure 1: Link between PDCA and continuous improvement

Διεργασία Επιθεώρησης

Στάδια:

1.Προετοιμασία Επιθεώρησης (Πλάνο- Χρονοδιάγραμμα- Λίστα ελέγχου – Ενημέρωση τμημάτων- Ανασκόπηση συστήματος ελέγχου)

2. Εκτέλεση επιθεώρησης

3. Καταγραφή αποτελεσμάτων- Έκδοση αναφοράς

4. Αίτημα feedback

5. Αξιολόγηση ευρημάτων, Follow-up- Actions' Planning

Execution of Audit Rules

- Must be done according to timetable
- Only ask open, factual questions
- Verify answer through observation
- Follow an audit trail
- Do more listening than talking 2 ear 1 mouth; therefore listen 2/3 of the time
- Sampling – Random check sample (files, records)
- Remember to say often ---- 'SHOW ME'
- Check for documents, records, reports, data in computers etc
- Ensure auditees statements are cross checked by supporting evidence e.g. statements by other personnel with specified authority, records, documentary evidence, observed points e.t.c.
- Verifying conformity to SOP'S
- Select Objective evidence

Κάθετη Επιθεώρηση

- Έλεγχος όλων των επιμέρους φάσεων μιας διεργασίας για ένα συγκεκριμένο ‘δείγμα’/ περιστατικό
  - από το ανώτερο επίπεδο προς το κατώτερο
  - από το κατώτερο επίπεδο προς το ανώτερο
- Εύκολη διεργασία για έναν αρχάριο επιθεωρητή
- Εφαρμόζεται και στο πλαίσιο εκπαιδευτικών σκοπών
- Χρονοβόρα διαδικασία, δεν καλύπτονται όλες οι πτυχές της λίστας ελέγχου κάθε φορά

Οριζόντια επιθεώρηση

- Έλεγχος ενός και μόνο στοιχείου μιας διεργασίας για πολλαπλά περιστατικά/ δείγματα
- Χρησιμοποιείται κυρίως στις επαναληπτικές επιθεωρήσεις συνεπακόλουθα της κάθετης επιθεώρησης

Σύνθετη (αξιολογική) Επιθεώρηση

- Παρακολούθηση της διαδικασίας καθώς υλοποιείται και συσχετισμός/ σύγκρισή της με την αντίστοιχη πρότυπη καταγεγραμμένη διαδικασία SOP
- - έλεγχος της πρακτικής εφαρμογής και του ποσοστού compliance / συμμόρφωσης με τις καταγεγραμμένες διαδικασίες

- έλεγχος της κατανόησης του προσωπικού αναφορικά με τις εφαρμοζόμενες διαδικασίες και τις προδιαγραφές τους

Process- oriented Audit

Examine by sample: Clinical audit of patients' files

- **Random dates (**less than 3 months old to ensure updated procedures and used forms**) and current date (**check EU records and pick up cases randomly**)**
- **Selection of patients' files (**3 – 5 inpatients' files, surgical cases, day care cases, at least 2 International Patients' files**)**
- **Verification of procedures (**compliance and fulfillment of SOPs**)**
- **Never take medical records' copies/ keep id data such as registration number of the patients but NO NAMES for your reporting**

Αναφορά Αποτελεσμάτων και Κατάρτιση Πλάνου Διορθωτικών Ενεργειών

- Τυποποιημένη φόρμα αναφοράς
- Επίσημη γλώσσα και ορολογία
- Καταγραφή και παράθεση τόσο των ευρημάτων μη συμμόρφωσης/ αποκλίσεων όσο και των θετικών!
- Εμπιστευτικότητα των αναφορών- Γνωστοποίηση σε προκαθορισμένους παραλήπτες
- Διαμόρφωση πλάνου ενεργειών (διορθωτικών- προληπτικών)
- Ανάθεση εργασιών
- Παρακολούθηση – Follow up

SWITZERLAND (Headquarters)
Via G. Corti 5, POLUS KOMPLEX, CH-6828 Balerna / Ticino
Tel.: +41 (0)91 682 0540 / (0)91 682 92 92
www.swissapproval.ch
e-mail: info@swissapproval.ch

UNITED KINGDOM
483 Green Lanes, Suite 50, London, N13 4BS
Tel.: +44 330 330 9047
www.swissapproval.ch
e-mail: uk@swissapproval.ch

SOUTH EASTERN MEDITERRANEAN SEA (SEMS)
Arch. Makariou 2-4, Capital Center, Nicosia
Tel.: +357 22680004
www.swissapproval.ch
e-mail: cyprus@swissapproval.ch

GREECE
Trapezountos & D. Akrita, 192 00 Elefsina, GR
Tel.: +30 2105562130
www.swissapproval.ch - www.swissapproval.gr
e-mail: greece@swissapproval.ch

UNITED ARAB EMIRATES
Oasis Center, Office No.59, 3rd Floor,Dubai, UAE
Tel: +971 4 3193001 - P.O.Box: 120685,
www.swissapproval.ch - e-mail: uae@swissapproval.ch
e-mail:uae.academy@swissapproval.com

ITALY
MILANO AREA: Via Canova 8, 21052, Busto Arsizio (VA)
ROMA AREA: Via Ancona 21, 00198, Roma
Tel: +39 0331 63 66 01 - 338 9755 249 -
www.swissapproval.ch
e-mail: italy@swissapproval.ch

ALBANIA
Rruga Sami Frasheri, Nd. 19, H.8, 1019 Tirana
Tel.: +355 44 30 9515, +355 69 707 3002
www.swissapproval.ch
e-mail: albania@swissapproval.ch

SERBIA
Bulevar Vojvode Stepe 59, 21000 Novi Sad, Serbia
Tel.: +381 216447947
www.swissapproval.rs & www.swissapproval.ch
e-mail: info@swissapproval.rs & serbia@swissapproval.ch

KINGDOM OF JORDAN
1803 Amman, 11947, Jordan
Tel: +962795474668
www.swissapproval.ch
e-mail: jordan@swissapproval.ch

PEOPLE'S REPUBLIC OF CHINA [PRC]
R 709, North Tower of Fortune 108 Plaza, No. 1839 Qixin RD,
Shanghai 201101, China. Tel: +86 021 609135 98
www.swisapproval.ch
e-mail: prc@swissapproval.ch

EGYPT
43 Masaken El Saudia st., El Sawah, Cairo,
Tel: +20 02 24 50 94 64
www.swissapproval.ch
e-mail: egypt@swissapproval.ch

KUWAIT
Ahmadi Indusltrial Area, Plots 63 & 84,
P.O.Box 24081, Safat, 13101, Kuwait
www.swissapproval.ch
e-mail: q8@swissapproval.ch

PAKISTAN
310, 3RD Floor, Jilani Tower,
M. A. Jinnah Road, Karachi, 74000,
Tel: +92 321 22 86 582
www.swissapproval.ch
e-mail: pakistan@swissapproval.ch

KOSOVA
Rr. Garibaldi, H-1, 10000, Pristina
www.swissapproval.ch
e-mail:kosova@swissapproval.ch

USA
CHICAGO, 150 N. Michigan Av., Ste 2800,
IL 60601Tel: +1 (312)291.4625
www.swissapproval.ch
e-mail: usa@swissapproval.ch

APPROVAL SWISS INTERNATIONAL Group of Companies


Thank You