



GDPR & Πιστοποίηση
Οι προβληματισμοί σχετικά με
την πρακτική εφαρμογή

Κώστας Στασινόπουλος

Δικηγόρος

LLM Information Technology & Telecoms

Αιτ Σκέψη 9: Η διαφορά ως προς τα επίπεδα προστασίας οφείλεται στην ύπαρξη αποκλίσεων κατά την εκτέλεση και εφαρμογή της οδηγίας 95/46/ΕΚ.

Αιτ Σκέψη 10: Για τη διασφάλιση συνεκτικής και υψηλού επιπέδου προστασίας το επίπεδο προστασίας θα πρέπει να είναι ισοδύναμο σε όλα τα κράτη μέλη και να διασφαλίζεται συνεκτική και ομοιόμορφη εφαρμογή των κανόνων σε ολόκληρη την Ένωση.

ΚΕΦΑΛΑΙΟ IV

Τμήμα 5

Κώδικες δεοντολογίας και πιστοποίηση

Άρθρα 40-43



ΓΚΠΔ - Πιστοποίηση (Άρθρο 42)

Μηχανισμοί πιστοποίησης - σφραγίδες - σήματα προστασίας δεδομένων

- ✓ **Εθελοντική** και διαθέσιμη μέσω διαφανούς διαδικασίας.
- ✓ **Κριτήρια** η εν λόγω αρμόδια εποπτική αρχή (αρ.58§3) ή το Συμβούλιο Προστασίας Δεδομένων (αρ 63)
- ✓ **ΔΕΝ** περιορίζει την ευθύνη του υπευθύνου ή του εκτελούντος και **ΔΕΝ** θίγει καθήκοντα και αρμοδιότητες εποπτικών αρχών
- ✓ **Ανανεώνεται**
- ✓ **Ανακαλείται**

ΓΚΠΔ - Πιστοποίηση (Άρθρο 42)

Σκοπός

42 § 1.: με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας.

42 § 2.:για τον σκοπό της απόδειξης ότι παρέχονται κατάλληλες εγγυήσεις στο πλαίσιο των διαβιβάσεων ΔΠΧ σε τρίτες χώρες ή διεθνείς οργανισμούς.

Αιτιολογική σκέψη 100: να μπορούν τα υποκείμενα των δεδομένων να αξιολογούν ταχέως το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων και υπηρεσιών.

Η Απόφαση για την Πιστοποίηση



ΠΙΣΤΟΠΟΙΗΣΗ

ΓΚΠΔ διατυπώνει και στις αιτιολογικές σκέψεις, 81, 98, 166-168 & 170 αλλά και στα άρθρα 24§3, 25§3, 28§5, 32§3

«...η προσχώρηση σε εγκεκριμένο κώδικα συμπεριφοράς/δεοντολογίας ή εγκεκριμένο μηχανισμό πιστοποίησης μπορεί να χρησιμοποιηθεί ως στοιχείο για να αποδειχθεί η συμμόρφωση...» του υπεύθυνου ή του εκτελούντα την επεξεργασία με τις υποχρεώσεις.

ΠΙΣΤΟΠΟΙΗΣΗ

Η συμμόρφωση στον ΓΚΠΔ είναι σφαιρική

Αναφέρεται στην συμμόρφωση με όλες τις πτυχές του ΓΚΠΔ

ΠΙΣΤΟΠΟΙΗΣΗ

1^η ενέργεια

- Αρχική εκτίμηση για το εάν η εταιρεία ανταποκρίνεται και σε ποιο βαθμό με τις απαιτήσεις του πιστοποιητικού

2^η ενέργεια

- Εξέταση της αποτελεσματικής λειτουργίας της εταιρείας και των συστημάτων και διαδικασιών επεξεργασίας των ΔΠΧ

3^η ενέργεια

- Μελέτη της αναγκαιότητας λήψης του πιστοποιητικού σύμφωνα με τα πορίσματα των προηγούμενων ενεργειών

4^η ενέργεια

- Υποβολή αιτήματος για πιστοποίηση

ΛΗΨΗ ΤΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

ΠΙΣΤΟΠΟΙΗΣΗ & ΤΥΠΟΠΟΙΗΣΗ

Πρότυπα

ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΙ ΤΥΠΟΠΟΙΗΣΗΣ

- Διεθνής Οργανισμός Τυποποίησης ISO (International Organization for Standardization)
- Διεθνής Ηλεκτροτεχνική Επιτροπή IEC (International Electrotechnical Commission)
- Διεθνής Ένωση Τηλεπικοινωνιών ITU (International Telecommunication Union)

ΕΥΡΩΠΑΪΚΟΙ ΟΡΓΑΝΙΣΜΟΙ ΤΥΠΟΠΟΙΗΣΗΣ

- Κοινός Ευρωπαϊκός Οργανισμός Τυποποίησης CEN/CENELEC (Joint European Standards Institution CEN/CENELEC)
- Ευρωπαϊκό Ινστιτούτο για τα Τηλεπικοινωνιακά Πρότυπα ETSI (European Telecommunications Standardization Institute)

ΕΘΝΙΚΟΙ ΟΡΓΑΝΙΣΜΟΙ ΤΥΠΟΠΟΙΗΣΗΣ

- Ελληνικός Οργανισμός Τυποποίησης - ΕΛΟΤ
- Γερμανικός Οργανισμός Τυποποίησης DIN (German Institute for Standardization)
- Βρετανικός Οργανισμός Τυποποίησης BSI (British Standards Institution)
- Γαλλικός Οργανισμός Τυποποίησης AFNOR (Association Francaise de Normalization)
- Αμερικάνικος Οργανισμός Τυποποίησης ANSI (American National Standards Institute)

Πρότυπα σχετικά με την Προστασία ΔΠΧ & Ιδιωτικότητας

Διεθνής Οργανισμός Τυποποίησης ISO

- ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29100:2011 Privacy framework
- ISO/IEC 29101:2013 Privacy architecture framework

CEN

- ❖ CWA 16113:2010 Personal Data Protection Good Practices

Βρετανικός Οργανισμός Τυποποίησης BSI (British Standards Institution)

- ❑ BS 10012:2009 Data protection. Specification for a personal information management system

Πρότυπα σχετικά με την Προστασία ΔΠΧ & Ιδιωτικότητας

ISO/IEC 27000

(family - Information **security** management systems)

Προδιαγραφές για σύστημα διαχείρισης της ασφάλειας πληροφοριών (ISMS)

Απαιτεί :

- Καθορισμό των κριτηρίων κινδύνου ασφάλειας πληροφοριών

- Περιοδικούς ελέγχους αξιολόγησης κινδύνων παράγουν συνεπή, έγκυρα και συγκρίσιμα αποτελέσματα

- Προσδιορισμό των κινδύνων που σχετίζονται με την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα

- Προσδιορισμό των πηγών αυτών των κινδύνων.

- Ανάλυση και αξιολόγηση των κινδύνων με διαφορετικά κριτήρια.

Πρότυπα σχετικά με την Προστασία ΔΠΧ & Ιδιωτικότητας

Διαφορετική ορολογία

ΓΚΠΔ	ISO 27701 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
Personal data-προσωπικά δεδομένα,	Personally Identifiable Information PII
Data controller-υπεύθυνος επεξεργασίας δεδομένων	PII controller
Data processor-εκτελών την επεξεργασία δεδομένων	PII processor
Data subject-υποκείμενο των δεδομένων	PII principal
Data protection by design-προστασία δεδομένων από το σχεδιασμό	Privacy by design
Data protection by default-προστασία δεδομένων εξ' ορισμού	Privacy by default

Το σχέδιο της Ευρωπαϊκής Επιτροπής για την τυποποίηση των Τεχνολογιών Πληροφορικής και Επικοινωνιών ΤΠΕ - ICT

Key enablers and security

- 5G
- Cloud computing
- Public sector information, open data and big data
- Internet of Things
- Cybersecurity / network and information security
- Electronic identification and trust services including e-signatures
- e-Privacy
- e-Infrastructures for research data and computing intensive science
- Broadband infrastructure mapping
- Accessibility of ICT products and services
- Artificial Intelligence
- European Global Navigation Satellite System (EGNSS)

Societal challenges

- e-Health, healthy living and ageing
- e-Skills and e-Learning
- Emergency communications
- e-Government
- eCall Policy and legislation Policy objectives

Innovation for the digital single market

- E-Procurement pre- and post award
- e-Invoicing Policy and legislation Policy objectives
- Card, internet and mobile payments
- Preservation of digital cinema
- Fintech and Regtech Standardization
- Blockchain and Distributed Digital Ledger Technologies

Sustainable growth

- Smart grids and smart metering
- Smart cities / technologies and services for smart and efficient energy use
- ICT Environmental impact
- European Electronic Toll Service (EETS)
- Intelligent Transport Systems - Connected and Automated Mobility (ITS-CAM) and Electromobility
- Advanced manufacturing
- Robotics and autonomous systems
- Construction - building information modelling
- Common Information Sharing Environment (CISE) for the EU maritime domain
- Water Management Digitisation
- Single European Sky

Η Λήψη της Πιστοποίησης



ΓΚΠΔ - Φορείς πιστοποίησης - Διαπίστευση (Άρθρο 43)

**Χορηγούν και Ανανεώνουν πιστοποιήσεις Φορείς οι οποίοι είναι
διαπιστευμένοι:**

- α) Είτε από την αρμόδια Εποπτική αρχή (αρ 55,56)
- β) Είτε από τον Εθνικό οργανισμό διαπίστευσης κατά το πρότυπο EN-ISO/IEC 17065/2012.

Διαπίστευση βάσει κριτηρίων από εποπτική αρχή ή Συμβούλιο Προστασίας
Δεδομένων

Καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Άρθρο 70 § 1 , στ) εκτελεί τη διαπίστευση των φορέων πιστοποίησης και την
περιοδική επανεξέτασή της δυνάμει του άρθρου 43

Ν. 4624/2019 – άρθρο 37

Διαπίστευση φορέων πιστοποίησης και πιστοποίηση

1. 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.

2. Το Ε.ΣΥ.Δ. ανακαλεί διαπίστευση αν ενημερωθεί από την Αρχή ότι δεν πληρούνται πλέον οι απαιτήσεις διαπίστευσης ή ο φορέας πιστοποίησης παραβαίνει τον ΓΚΠΔ και τις διατάξεις του παρόντος.



Ανεξάρτητες εποπτικές αρχές



Α) Η Διαπίστευση των Φορέων Πιστοποίησης

Αρ 43 § 3

Η διαπίστευση βάσει των κριτηρίων που έχουν **εγκριθεί από:**

- ✓ την εποπτική αρχή που είναι αρμόδια δυνάμει του άρθρου 55 ή 56,
- ✓ ή από το ΕΣΠΔ δυνάμει του άρθρου 63 (Μηχανισμός συνεκτικότητας)

Άρθρο 63 – 65 Μηχανισμός συνεκτικότητας

- i. Αρμόδια Αρχή Υποβάλλει σχέδιο απόφασης στο ΕΣΠΔ (άρθρο 64 § 1 περ γ)
- ii. ΕΣΠΔ εάν ΔΕΝ έχει διατυπώσει γνώμη επί του ίδιου θέματος - εκδίδει γνώμη (άρθρο 64 § 3 περ γ)
- iii. Αρμόδια Αρχή ανακοινώνει κατά πόσο θα διατηρήσει ή θα τροποποιήσει το σχέδιο απόφασης (άρθρο 64 § 7)
- iv. Αρμόδια Αρχή εάν δεν ακολουθήσει γνώμη ΕΣΠΔ, στο σύνολό της ή εν μέρει, εφαρμόζεται το άρθρο 65 § 1. (άρθρο 64 § 8)
- v. Το ΕΣΠΔ εκδίδει δεσμευτική απόφαση εάν μια αρμόδια εποπτική αρχή δεν ζητήσει τη γνώμη του ή δεν ακολουθήσει τη γνώμη του που εκδίδεται δυνάμει του άρθρου 64 (άρθρο 65 § 1 περ γ)

Β) Η ΠΙΣΤΟΠΟΙΗΣΗ

Άρθρο 42 § 5 Πιστοποίηση από :

1. τους φορείς πιστοποίησης που αναφέρονται στο άρθρο 43 ή
2. από την αρμόδια εποπτική αρχή

Κριτήρια θα έχει εγκρίνει:

- η αρμόδια εποπτική αρχή δυνάμει του άρθρου 58 παράγραφος 3 ή
- το ΕΣΠΔ σύμφωνα με το άρθρο 63 (Ευρωπαϊκή Σφραγίδα Προστασίας Δεδομένων)

Η ΠΙΣΤΟΠΟΙΗΣΗ

Κατευθυντήριες Οδηγίες 1/2018 σχετικά με την πιστοποίηση και τον προσδιορισμό των κριτηρίων πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 ΓΚΠΔ

Ο ΓΚΠΔ επιφορτίζει την εποπτική αρχή με την έγκριση κριτηρίων πιστοποίησης, αλλά **όχι με ανάπτυξη κριτηρίων**.

Προκειμένου να εγκρίνει τα κριτήρια πιστοποίησης βάσει του άρθρου 42 §5, η εποπτική αρχή θα πρέπει να έχει σαφή εικόνα:

- ✓ όσον αφορά την απόδειξη της συμμόρφωσης με το ΓΚΠΔ και
- ✓ σε σχέση με το καθήκον να παρακολουθεί και να επιβάλλει την εφαρμογή του κανονισμού.

Το παράρτημα παρέχει οδηγίες για να διασφαλιστεί εναρμονισμένη προσέγγιση κατά την αξιολόγηση των κριτηρίων για το σκοπό της έγκρισης.

ΠΙΣΤΟΠΟΙΗΣΗ

Τα κριτήρια περιλαμβάνουν έλεγχο στα εξής σημεία:

- ✓ Την νομιμότητα της επεξεργασίας (άρθρο 6).
- ✓ Την τήρηση των αρχών της επεξεργασίας δεδομένων (άρθρο 5).
- ✓ Την διασφάλιση των δικαιωμάτων των υποκειμένων (άρθρα 12-23).
- ✓ Την ύπαρξη πλάνου για την αναφορά περιστατικών παραβιάσεων δεδομένων (άρθρο 33).
- ✓ Την τήρηση των υποχρεώσεων όσον αφορά την προστασία των δεδομένων από το σχεδιασμό ή από προεπιλογή (άρθρο 25).
- ✓ Κατά πόσον έχουν διεξαχθεί ΜΕΑΠΔ – DPIA και έχουν ληφθεί τεχνικά και οργανωτικά μέτρα σύμφωνα με το άρθρο 32.

CE Certification



Άρθρο 43 § 8 – 9 Πιστοποίηση

- Η Επιτροπή εξουσιοδοτείται να εκδίδει εκτελεστικές πράξεις, **με σκοπό τον προσδιορισμό των απαιτήσεων που πρέπει να λαμβάνονται υπόψη για τους μηχανισμούς πιστοποίησης**
- Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις σχετικά με τη θέσπιση τεχνικών προτύπων για μηχανισμούς πιστοποίησης, σφραγίδες και σήματα προστασίας δεδομένων, καθώς και μηχανισμούς για την προώθηση και την αναγνώριση των εν λόγω μηχανισμών πιστοποίησης, σφραγίδων και σημάτων.

Αιτιολογική σκέψη 166: Για την εκπλήρωση των στόχων του παρόντος κανονισμού, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σχετικά με τα κριτήρια και τις απαιτήσεις για τους μηχανισμούς πιστοποίησης, τις πληροφορίες που παρουσιάζονται με τυποποιημένα εικονίδια και τις διαδικασίες για την παροχή τέτοιων εικονιδίων.

**ΕΥΧΑΡΙΣΤΩ ΓΙΑ ΤΗΝ
ΠΡΟΣΟΧΗ ΣΑΣ**