ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ – GENERAL DATA PROTECTION REGULATION (ΓΚΠΔ/GDPR)

Ευαγγελία Βαγενά, ΔΝ, DEA

Δικηγόρος, ΔΝ, DEA Droit et Informatique, CIPP/E

Ψηφιακή οικονομία:
η πολιτική εκτίμηση που οδηγεί στην νομική ρύθμιση

Challenges for the sector in the EU

- Two billion people are currently connected to the internet and by 2016, this number will exceed 3 billion – **almost half of the world's population.**
- Businesses that fail to get digitally connected will become excluded from the global market.
- The **huge potential of the digital economy is underexploited in Europe**, with 41% of enterprises being non-digital, and only two percent taking full advantage of digital opportunities.
- New digital opportunities create new business opportunities. Now that **youth unemployment** has risen to over 20% in the EU (and to over 55% in Spain and **Greece**), the growth prospects offered by the digital economy in Europe are promising.
- Other regions of the world are already ahead of the game. The digital economy now contributes up to **eight percent of the GDP of the G-20** major economies, powering growth and creating jobs.
- Over the last five years, the development of mobile applications alone has created nearly **500 000 new jobs in the US**, implying strong employment growth prospects. That type of growth is not seen across the EU. It is estimated **that 1.5 million additional jobs could be created in the EU** digital economy if it mirrors the performance of the US or Sweden.

Source: https://ec.europa.eu/growth/sectors/digital-economy/importance_en

Ψηφιακή οικονομία: η δημιουργία των κατάλληλων συνθηκών

«Ενίσχυση της εμπιστοσύνης και της **ασφάλειας** όσον αφορά τις ψηφιακές υπηρεσίες και τον χειρισμό των **δεδομένων προσωπικού χαρακτήρα**»

Ευρωπαϊκή Επιτροπή

- Γιατί αλλάζουμε τους κανόνες;
  - Είναι θέμα εμπιστοσύνης...
  - Η έλλειψη εμπιστοσύνης στους παλιούς κανόνες για την προστασία των δεδομένων ανέκοπτε την πορεία της ψηφιακής οικονομίας.
  - Μόνο το15% των ανθρώπων αισθάνονται ότι έχουν πλήρη έλεγχο των πληροφοριών που παρέχουν ηλεκτρονικά.
  - Το νέο σύστημα κρατάει τα έξοδα σε χαμηλά επίπεδα και θα συμβάλλει στην ανάπτυξη των επιχειρήσεων

Το νέο θεσμικό πλαίσιο "data reform package"

- Κανονισμός (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 Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων- **General Data Protection Regulation/ GDPR**).
- Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης **ποινικών αδικημάτων** ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.
- Οδηγία (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις **ονομάτων επιβατών (PNR)** για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων.
- Διαδικασία αναθεώρησης Οδηγίας **e- privacy** - (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες η οποία πλέον θα αντικατασταθεί από σχετικό Κανονισμό)

….με τα λόγια του νομοθέτη

- Ενώ οι στόχοι και οι αρχές της οδηγίας 95/46/ΕΚ παραμένουν ισχυροί, η οδηγία δεν κατόρθωσε να αποτρέψει τον κατακερματισμό της εφαρμογής της προστασίας των δεδομένων σε ολόκληρη την Ένωση, την ανασφάλεια δικαίου ή τη διαδεδομένη στο κοινό αντίληψη ότι υπάρχουν σημαντικοί κίνδυνοι για την προστασία των φυσικών προσώπων, ιδίως όσον αφορά την επιγραμμική δραστηριότητα. Διαφορές στο επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων, ιδίως του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα, όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στα κράτη μέλη, ενδέχεται να εμποδίζουν την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση. Επομένως, οι διαφορές αυτές μπορεί να συνιστούν εμπόδιο για την άσκηση οικονομικών δραστηριοτήτων στο επίπεδο της Ένωσης, να στρεβλώνουν τον ανταγωνισμό και να εμποδίζουν τις αρχές στην εκτέλεση των αρμοδιοτήτων τους, όπως αυτές απορρέουν από το δίκαιο της Ένωσης. Αυτή η διαφορά ως προς τα επίπεδα προστασίας οφείλεται στην ύπαρξη αποκλίσεων κατά την εκτέλεση και εφαρμογή της οδηγίας 95/46/ΕΚ.

Ας θυμηθούμε πρώτα όμως…..

Ποια δεδομένα χαρακτηρίζονται ως προσωπικά;

***κάθε* πληροφορία** κάθε πληροφορία που αναφέρεται στο “υποκείμενο των δεδομένων” , π.χ

- στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.)
- φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ)
- οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά)
- ενδιαφέροντα
- Δραστηριότητες
- Συνήθειες
- IP Address
- e-mail

- SOS: όχι στοιχεία εταιρειών και εν γένει νομικών προσώπων ΟΥΤΕ φυσικά ζώων ☺
- SOS: Δεν λογίζονται ως δεδομένα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιοριστούν τα υποκείμενα

Πώς αλλάζει ο ορισμός με τον GDPR?

- Διεύρυνση και εξειδίκευση
  - Δεδομένα θέσης, επιγραμμικά [on line] αναγνωριστικά στοιχεία ταυτότητας τα οποία παρέχονται από συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα τους και διευκολύνουν τον εντοπισμό του υποκειμένου [ip addresses ή εντοπισμός θέσης μέσω GPS, cookies, RFID

Ποια δεδομένα χαρακτηρίζονται ως ευαίσθητα;

Ευαίσθητα χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται:

- στη φυλετική ή εθνική του προέλευση
- στα πολιτικά του φρονήματα
- στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις
- στη συμμετοχή του σε συνδικαλιστική οργάνωση
- στην υγεία του, στην κοινωνική του πρόνοια
- στην ερωτική του ζωή
- τις ποινικές διώξεις και καταδίκες του
- καθώς και στη συμμετοχή του, σε συναφείς με τα ανωτέρω ενώσεις προσώπων

Ευαίσθητα= ειδικές κατηγορίες (GDPR)

- Ό,τι πριν ++
- «γενετικά δεδομένα»:τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου
- «βιομετρικά δεδομένα»:δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα,
- «δεδομένα που αφορούν την υγεία»:δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του,

Υποκείμενο δεδομένων

Το άτομο στο οποίο αφορούν

Το ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο

ΕΠΕΞΕΡΓΑΣΙΑ- έννοια

- Επεξεργασία: κάθε εργασία – με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων – που εφαρμόζεται σε δεδομένα όπως:
  - συλλογή
  - Καταχώριση
  - Οργάνωση
  - διατήρηση ή αποθήκευση
  - τροποποίηση
  - εξαγωγή
  - χρήση
  - διαβίβαση
  - διάδοση
  - συσχέτιση ή συνδυασμός
  - διασύνδεση
  - δέσμευση
  - διαγραφή
  - καταστροφή

ΕΠΕΞΕΡΓΑΣΙΑ- GDPR αρχές (preview)

- Αρχή νομιμότητας
- Αρχή αντικειμενικότητας
- Αρχή διαφάνειας
- Αρχή του σκοπού (και περιορισμού αυτού)
- Αρχή της ελαχιστοποίησης των δεδομένων
- Αρχή της ακρίβειας (δικαίωμα διόρθωσης ή διαγραφής)
- Αρχή του περιορισμού
- Αρχή της ακεραιότητας και εμπιστευτικότητας (ασφάλεια)
- Αρχή της λογοδοσίας

Υπεύθυνος επεξεργασίας

το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους

Υπεύθυνος επεξεργασίας

- Υποχρέωση Λογοδοσίας
- Ενημέρωση (awareness)
- Προστασία Ανηλίκων
- Συγκατάθεση
- Καταγραφή (διαδικασίες και συμβάντα)
- Εκτίμηση Επιπτώσεων
- Ανασχεδιασμός Διαδικασιών και Συστημάτων
- Υπεύθυνος Προστασίας Δεδομένων
- Πολιτικές Ασφαλείας
- Σεβασμός στα δικαιώματα
- Συνεργασία με τις Εποπτικές Αρχές
- Διαχείριση Παραβάσεων
- Ενημέρωση Αρχής και Υποκειμένων (γνωστοποίηση/ανακοίνωση)
- Διασυνοριακή Ροή (επάρκεια, δεσμευτικοί εταιρικοί κανόνες κλπ.

Εκτελών την επεξεργασία

το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

Data breach

«παραβίαση δεδομένων προσωπικού χαρακτήρα»:

η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία

THE GENERAL DATA PROTECTION REGULATION

GDPR

Ο νέος Κανονισμός

- Αντικαθιστά τη βασική Οδηγία 95/46/ΕΚ
- Έχει τεθεί σε ισχύ από τις 4.5.2016, θα τεθεί σε εφαρμογή από τις **25 Μαΐου 2018**
- Έως τότε οι εταιρείες θα πρέπει να εξασφαλίσουν ότι ανταποκρίνονται στις επιβαλλόμενες **νέες υποχρεώσεις**
- Θα βοηθηθούν από οδηγίες, γνωμοδοτήσεις, κατευθυντήριες γραμμές αρμόδιων αρχών

[173 εισαγωγικά σημεία προοιμίου, 99 άρθρα]

Ο νέος Κανονισμός

Ο κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα:

- α) στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης,
- β) από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ,
- γ) από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας,
- δ) από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

Article 29 Working Party

- ADOPTED GUIDELINES
  - Guidelines on the right to "data portability", wp242rev.01
  - Guidelines on Data Protection Officers ('DPOs'), wp243rev.01
  - Guidelines on The Lead Supervisory Authority, wp244rev.01
  - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01

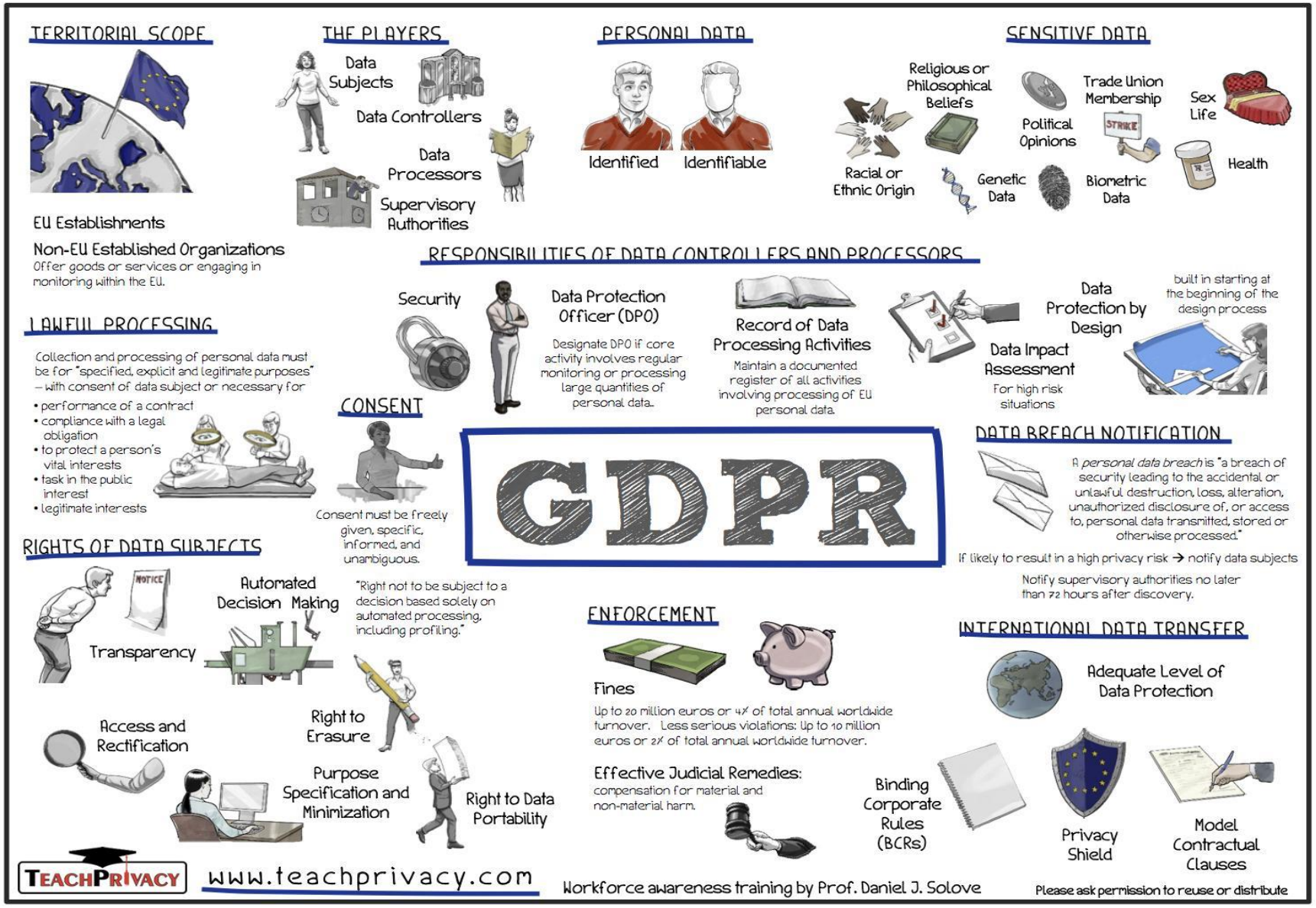
Ελληνική πραγματικότητα- νομοπαρασκευαστική επιτροπή

Αριθμ. 43519/ΦΕΚ Β 27.06.2016, Τ.1913

Σύσταση και συγκρότηση ειδικής νομοπαρασκευαστικής επιτροπής με αντικείμενο:

α) την κατάρτιση σχεδίου νόμου για την ενσωμάτωση στην εθνική έννομη τάξη της Οδηγίας 2016/680/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης - πλαίσιο 2008/977/ ΔΕΥ του Συμβουλίου», τη σύνταξη της σχετικής αιτιολογικής έκθεσης, της έκθεσης αξιολόγησης συνεπειών ρυθμίσεων και του πίνακα αντιστοίχισης των προτεινόμενων με το σχέδιο νόμου διατάξεων με τις διατάξεις της Οδηγίας και

β) την εξέταση του ενδεχόμενου λήψης νομοθετικών μέτρων για την εφαρμογή 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 (Γενικός Κανονισμός για την Προστασία Δεδομένων)»


TERRITORIAL SCOPE
EU Establishments
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.
THE PLAYERS
Data Subjects
Data Controllers
Data Processors
Supervisory Authorities
PERSONAL DATA
Identified
Identifiable
SENSITIVE DATA
Religious or Philosophical Beliefs
Political Opinions
Trade Union Membership
Sex Life
Racial or Ethnic Origin
Genetic Data
Biometric Data
Health
RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS
Security
Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.
Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.
Data Protection by Design
built in starting at the beginning of the design process
Data Impact Assessment
For high risk situations
LAWFUL PROCESSING
Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for
• performance of a contract
• compliance with a legal obligation
• to protect a person's vital interests
• task in the public interest
• legitimate interests
CONSENT
Consent must be freely given, specific, informed, and unambiguous.
GDPR
DATA BREACH NOTIFICATION
A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
If likely to result in a high privacy risk → notify data subjects
Notify supervisory authorities no later than 72 hours after discovery.
RIGHTS OF DATA SUBJECTS
NOTICE
Transparency
Automated Decision Making
"Right not to be subject to a decision based solely on automated processing, including profiling."
Right to Erasure
Access and Rectification
Purpose Specification and Minimization
Right to Data Portability
ENFORCEMENT
Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.
Effective Judicial Remedies:
compensation for material and non-material harm.
INTERNATIONAL DATA TRANSFER
Adequate Level of Data Protection
Binding Corporate Rules (BCRs)
Privacy Shield
Model Contractual Clauses
TEACHPRIVACY
www.teachprivacy.com
Workforce awareness training by Prof. Daniel J. Solove
Please ask permission to reuse or distribute

Τί αλλάζει κυρίως;

- Αρχή της λογοδοσίας ή υπευθυνότητας (accountability)
  - «Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει την συμμόρφωση …
  - Ακόμα και : «Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων ...»
  - ….«να αποδεικνύει»- «Αρχή - Ομπρέλα»
- Ευθύνη όχι μόνο του υπεύθυνου της επεξεργασίας αλλά και του εκτελούντα αυτήν π.χ.:
  - τήρηση αρχείου καταγραφής δραστηριοτήτων επεξεργασίας
  - λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων για την διασφάλιση της επεξεργασίας
- Κατάργηση γενικών γνωστοποιήσεων επεξεργασίας δεδομένων προς την εποπτική αρχή
- Εφαδικό Πεδίο εφαρμογής:
  - Δραστηριότητα εγκατάστασης υπευθύνου ή εκτελούντος την επεξεργασία στην Ε.Ε. ακόμη και εάν η επεξεργασία λαμβάνει σε χώρα εκτός Ε.Ε.
  - Δραστηριότητα εγκατάστασης υπευθύνου ή εκτελούντος την επεξεργασία εκτός Ε.Ε. αλλά η επεξεργασία αφορά υποκείμενα δεδομένων που βρίσκονται εντός Ε.Ε.

Τί αλλάζει κυρίως;

- Γνωστοποίηση παραβίασης δεδομένων στην εποπτική αρχή εντός 72 ωρών
- Ανακοίνωση παραβίασης δεδομένων στο υποκείμενο
- Διενέργεια εκτίμησης αντικτύπου (Privacy Impact Assessment) πριν από επικίνδυνη επεξεργασία
- Κώδικες Δεοντολογίας, μηχανισμοί πιστοποίησης, σφραγίδων και σημάτων προστασίας δεδομένων
- Περισσότερα και πιο σαφή δικαιώματα υποκειμένου
- Περιορισμός αδειοδοτήσεων από την εποπτική αρχή για την επεξεργασία ειδικών κατηγοριών δεδομένων
  - γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία
  - Όσων τυγχάνουν επεξεργασίας προς το δημόσιο συμφέρον, περιλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία».


GDPR
Privacy Impact Assessment
Protect by design
Data Protection Officer
Data Breach Notification
Right to be forgotten
Consent
Data Portability
Personal Data

Βασικές ρυθμίσεις νέου Κανονισμού- συγκατάθεση ενηλίκου

«συγκατάθεση» του υποκειμένου των δεδομένων:

κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν

Βασικές ρυθμίσεις νέου Κανονισμού- συγκατάθεση ενηλίκου

- 1.Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα.
- 2.Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Κάθε τμήμα της δήλωσης αυτής το οποίο συνιστά παράβαση του παρόντος κανονισμού δεν είναι δεσμευτικό.
- 3.Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.
- 4.Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

Βασικές ρυθμίσεις νέου Κανονισμού- συγκατάθεση ανηλίκου

Σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών (διαδίκτυο) απευθείας σε παιδί, η επεξεργασία δεδομένων προσωπικού χαρακτήρα παιδιού είναι σύννομη εάν το παιδί είναι **τουλάχιστον 16 χρονών.**

Εάν το παιδί είναι ηλικίας κάτω των 16 ετών, η επεξεργασία αυτή είναι σύννομη μόνο εάν και στον βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού. Τα κράτη μέλη δύνανται να προβλέπουν διά νόμου μικρότερη ηλικία για τους εν λόγω σκοπούς, υπό την προϋπόθεση ότι η εν λόγω μικρότερη ηλικία **δεν είναι κάτω από τα 13 έτη.**

Ο υπεύθυνος επεξεργασίας καταβάλλει εύλογες προσπάθειες για να επαληθεύσει στις περιπτώσεις αυτές ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία.

Βασικές ρυθμίσεις νέου Κανονισμού

- Ανανεωμένοι & νέοι ορισμοί, π.χ.:
  - Κατάρτιση προφίλ
  - Ψευδωνυμοποίηση
  - Γενετικά δεδομένα, βιομετρικά δεδομένα
- Ευαίσθητα: +**γενετικά, βιομετρικά**
- Ειδικές προϋποθέσεις για συγκατάθεση **παιδιού**
- Επαναδιατύπωση αρχών επεξεργασίας
- Νέα δικαιώματα «υποκειμένων»
  - Διαγραφής- **δικαίωμα λήθης** (Βλ. υπόθεση Costeja)
  - Φορητότητας δεδομένων
  - Εναντίωσης στην κατάρτιση προφίλ ή σε απόφαση βάσει αυτού
  - Πληροφόρησης για παραβίαση
- Τροποποίηση υποχρεώσεων υπεύθυνων επεξεργασίας
  - Κατάργηση υποχρέωσης γνωστοποίησης αρχείου
  - Privacy by design & privacy by default (κατά το σχεδιασμό και με προεπιλεγμένες ρυθμίσεις)
  - Διατήρηση αρχείων επεξεργασίας
  - Γνωστοποίηση εντός 72 ωρών παραβιάσεων
  - Impact assessment
- Νέος θεσμός **Data Protection Officer (DPO)-** υπεύθυνος προστασίας δεδομένων
- Νέες ρυθμίσεις για εποπτεύουσες αρχές
- Κυρώσεις για υπεύθυνους ή εκτελούντες την επεξεργασία

GDPR- Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Άρθρο 5 1.Τα δεδομένα προσωπικού χαρακτήρα:

- α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»),
- β) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»),
- γ) είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»),
- δ) είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»),
- ε) διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»),
- στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

Δικαιώματα υποκειμένου δεδομένων- GDPR

- Η αυστηροποίηση των γενικών προϋποθέσεων παροχής νόμιμης συγκατάθεσης ενηλίκων (άρ. 4 παρ. 11, 6-7) και των ανηλίκων (άρ. 8)
- Η παροχή των αιτηθέντων πληροφοριών στο υποκείμενο των δεδομένων εντός 1 μηνός (με δικαίωμα παράτασης 2 μηνών) ή ενημέρωση για τους λόγους τυχόν άρνησης (άρ. 12 παρ. 3)
- Το δικαίωμα πρόσβασης του υποκειμένου στα δεδομένα που τηρούνται σε σχέση με την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων - κατάρτισης προφίλ (άρ. 15 παρ. 1 εδ. η') και
- το δικαίωμα εναντίωσης του στην ανωτέρω επεξεργασία (αρ. 21-22), ιδίως για σκοπούς απευθείας εμπορικής προώθησης
- Το δικαίωμα στη φορητότητα των δεδομένων (άρ. 20)

Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

1.Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

α) τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν κατ' άλλο τρόπο σε επεξεργασία,

β) το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,

γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 2,

δ) τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,

ε) τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας,

στ) τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών που αναφέρονται στο άρθρο 8 παράγραφος 1. χάθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία (π.χ e commerce)

Αρχή της λογοδοσίας (accountability)

- Προκειμένου να μπορεί να αποδείξει συμμόρφωση προς τον παρόντα κανονισμό, ο υπεύθυνος επεξεργασίας θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τα οποία ανταποκρίνονται ειδικότερα στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού
- άρθρο 5 παρ. 2 του Κανονισμού «Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει την συμμόρφωση με την παράγραφο 1(«λογοδοσία»)».
- οφείλει να λαμβάνει τα απαραίτητα μέτρα ώστε ανά πάσα στιγμή να αποδεικνύει ότι εφάρμοσε τον Κανονισμό. Η αρχή της λογοδοσίας ως υποχρέωση διαρρέει τον Κανονισμό και την βρίσκουμε στις διατάξεις των άρθρων 12, 15 παρ. 3, 24, 25, 28, 30, 33, 35 και 39.
- Συμμόρφωση με τις αρχές που διέπουν την επεξεργασία + απόδειξη συμμόρφωσης

GDPR νομιμότητα επεξεργασίας απλών δεδομένων

Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Το στοιχείο στ) του πρώτου εδαφίου δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

GDPR νομιμότητα επεξεργασίας ειδικών κατηγοριών δεδομένων (ευαίσθητων)

Καταρχήν απαγορεύεται εκτός αν ισχύει ένα από τα ακόλουθα:

α) το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,

γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,

δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων,

ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,

στ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,

Εκτίμηση αντικτύπου – Data protection Impact Assesment (DPIA)- πότε;

«Όταν ένα είδος επεξεργασίας, ιδίως με τη χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους»

Όπως όταν υφίσταται:

- Συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών που βασίζεται σε αυτοματοποιημένη επεξεργασία (κατάρτιση προφίλ) και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα ή επηρεάζουν σημαντικά το φυσικό πρόσωπο.
- Μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών (ευαίσθητων) δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα.
- Συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Εκτίμηση αντικτύπου – Data protection Impact Assesment (DPIA)- Περιεχόμενο;

- Περιγραφή των προβλεπόμενων πράξεων και σκοπών επεξεργασίας.
- Εκτίμηση της αναγκαιότητας και αναλογικότητας των πράξεων σε συνάρτηση με τους σκοπούς.
- Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.
- Προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (συμπεριλαμβανομένων των μέτρων και μηχανισμών ασφάλειας).

αλλάζει ο κίνδυνος- αλλάζει & η εκτίμηση

Εκτίμηση αντικτύπου – Data protection Impact Assesment (DPIA)

- Πότε;
  - «όταν ενδέχεται να …**επιφέρει υψηλό κίνδυνο** για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων»
  - Ενδεικτικά κριτήρια στον κανονισμό
  - Κατάλογος πράξεων που εμπίπτουν από εποπτική αρχή
- Προκαθορισμένο ελάχιστο περιεχόμενο
- Προηγούμενη διαβούλευση με εποπτική αρχή & γνώμη υπεύθυνου προστασίας
  - Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη της εποπτικής αρχής πριν από την επεξεργασία, όταν η εκτίμηση αντικτύπου υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας.
  - Η εποπτική αρχή παρέχει γραπτώς συμβουλές εντός 8 εβδομάδων (δυνατή παράταση κατά 6 εβδομάδες) και δύναται να ασκήσει τις εξουσίες της όταν φρονεί ότι η επεξεργασία παραβαίνει τον παρόντα κανονισμό, ιδίως αν ο υπεύθυνος επεξεργασίας δεν έχει προσδιορίσει ή μετριάσει επαρκώς τον κίνδυνο.
  - Η διαβούλευση διενεργείται όταν η εκτίμηση αντικτύπου υποδεικνύει υψηλό κίνδυνο χωρίς διασφαλίσεις, μέτρα και μηχανισμούς ασφάλειας για να μετριαστεί ο κίνδυνος

Εκτίμηση αντικτύπου – Data protection Impact Assesment (DPIA) ΕΝΝΟΙΑ ΚΙΝΔΥΝΟΥ

- Ως «κίνδυνος» νοείται μια υπόθεση εργασίας που περιγράφει ένα συμβάν και τις επιπτώσεις του, που έχουν εκτιμηθεί με όρους σοβαρότητας και πιθανότητας επέλευσης.

- Ως «διαχείριση κινδύνου» μπορούν να νοηθούν οι συντονισμένες δραστηριότητες για την καθοδήγηση και τον έλεγχο ενός οργανισμού ως προς τον κίνδυνο.

Ανάλυση Κινδύνου-Εκτίμηση αντικτύπου/ Data protection Impact Assesment (DPIA)

- **Ανάλυση κινδύνου:**
  - **πιθανές απειλές (τεχνολογικά κενά, ελλιπείς διαδικασίες, ακόμα και … δυσαρεστημένοι υπάλληλοι)**
  - **κατηγοριοποίηση των δεδομένων ανάλογα με την κρισιμότητα τους**
  - **αποτελεσματικές διαδικασίες μείωσης του αντικτύπου (DPIA)**
- **Δραστηριότητες επεξεργασίας:**
  - **Υψηλού κινδύνου (DPIA, διαβούλευση, γνωστοποιήσεις άρθρου 33)**
  - **Κινδύνου (DPIA, γνωστοποιήσεις)**
  - **Χαμηλού κινδύνου (προαιρετικό DPIA, χωρίς υποχρέωση γνωστοποιήσεων)**

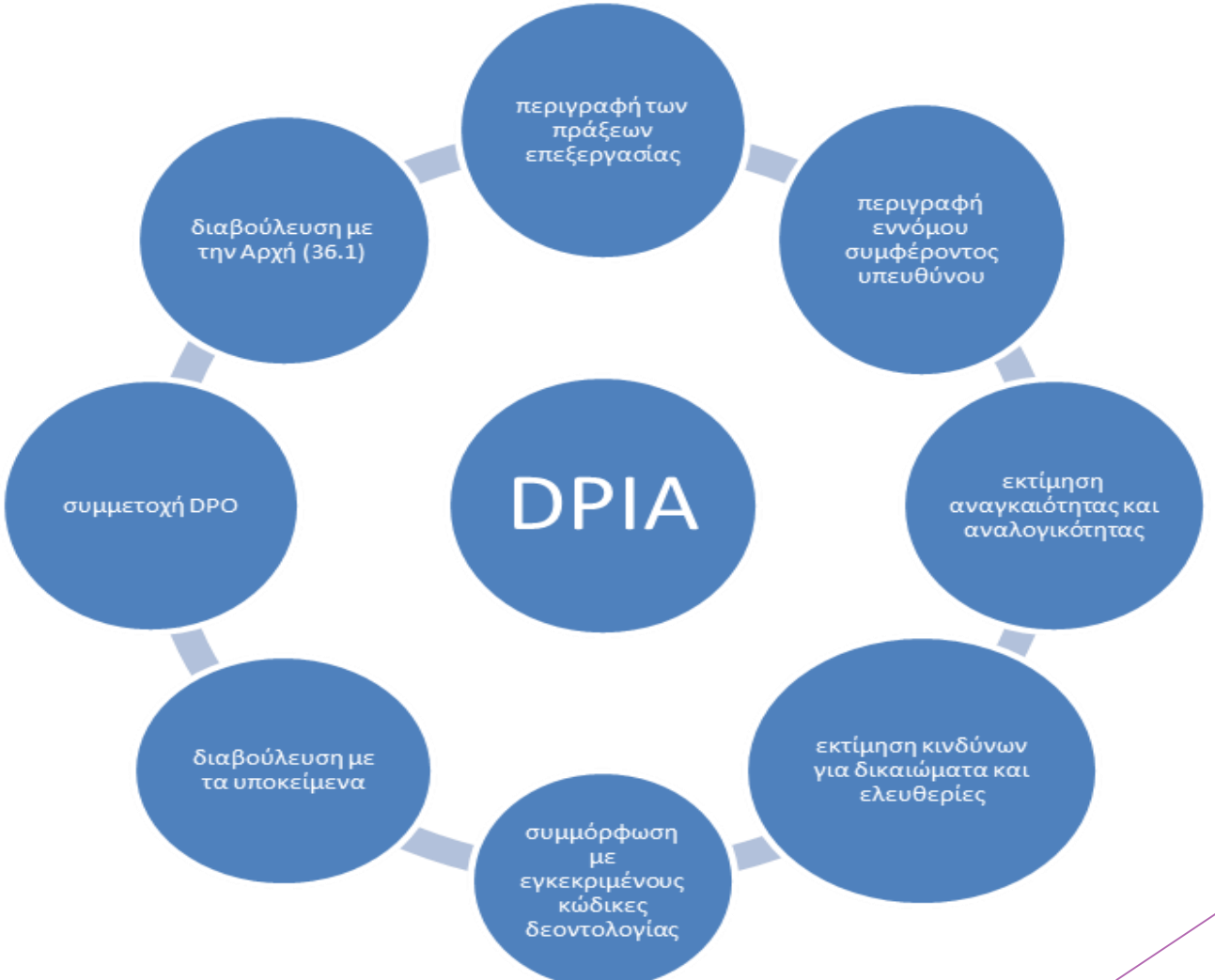
Εκτίμηση αντικτύπου – Data protection Impact Assesment (DPIA)

ΓΕΝΙΚΕΣ ΑΡΧΕΣ (Συνέχεια)

- **Σε ποια χρονική στιγμή θα πρέπει να πραγματοποιηθεί μια DPIA; *Πριν από την επεξεργασία.***
- **Ποιος είναι υποχρεωμένος να εκτελέσει την DPIA; *Ο υπεύθυνος επεξεργασίας, σε συνεργασία με τον DPO και τον εκτελούντα την επεξεργασία***
- **Ποια είναι η μεθοδολογία για την πραγματοποίηση μιας DPIA; *Διαφορετικές μεθοδολογίες αλλά κοινά κριτήρια.***
- **Πρέπει να δημοσιεύεται η Εκτίμηση Αντικτύπου; *Προτείνεται να δημοσιεύεται έστω και εν μέρει. Σε κάθε περίπτωση αν προηγήθηκε διαβούλευση με την Αρχή θα πρέπει να κοινοποιείται σε αυτή.***
- **Η DPIA είναι μια διαδικασία εμπέδωσης και απόδειξης της συμμόρφωσης (WP29).**
- **Η DPIA θα πρέπει να αντιμετωπίζεται ως εργαλείο που βοηθά στη λήψη αποφάσεων σε σχέση με την επεξεργασία.**

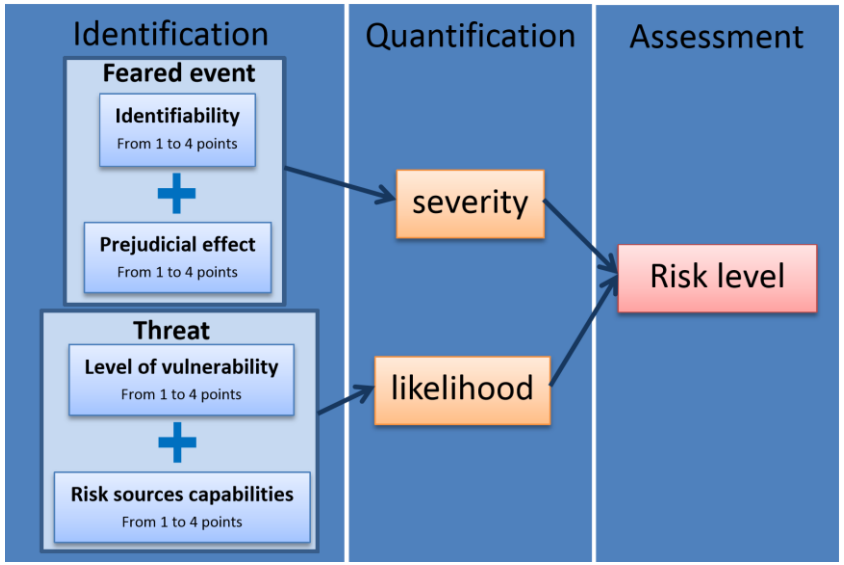
Εκτίμηση αντικτύπου – Data protection Impact Assesment (DPIA)

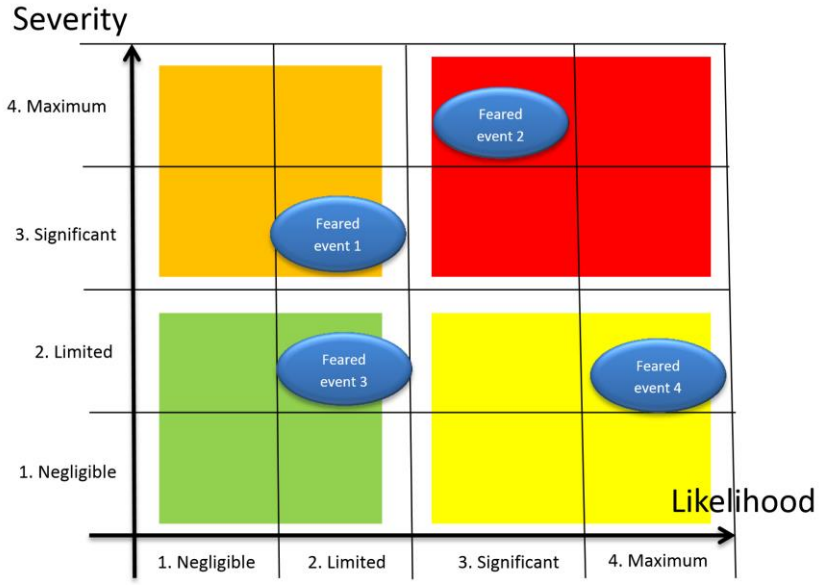
ΣΧΗΜΑΤΟΠΟΙΗΜΕΝΑ (Συνέχεια)



Εκτίμηση αντικτύπου – Data protection Impact Assesment (DPIA) (Συνέχεια)

- Βλ. Σύσταση της Επιτροπής της 10ης Οκτωβρίου 2014 σχετικά με το υπόδειγμα για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων όσον αφορά τα έξυπνα δίκτυα και τα έξυπνα συστήματα μέτρησης *(2014/724/ΕΕ)*





Source: https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf

Ασφάλεια & προστασία προσωπικών δεδομένων

«Λαμβάνοντας υπόψη … ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέσα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα

β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση

γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος

δ) της διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας **των τεχνικών και των οργανωτικών μέτρων** για τη διασφάλιση της ασφάλειας της επεξεργασίας.»

Παραβίαση ασφάλειας & υποχρέωση γνωστοποίησης της

- Στην εποπτική αρχή πάντα εφόσον υπάρχει κίνδυνος
- Στο υποκείμενο: αν ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων εκτός αν:
  - Υπάρχουν τεχνικά και οργανωτικά μέτρα που καθιστούν μη κατανοητά τα δεδομένα σε μη εξουσιοδοτημένα πρόσωπα (κρυπτογράφηση). •
  - Ληφθούν μέτρων που διασφαλίζουν ότι ο υψηλός κίνδυνος δεν μπορεί πλέον να προκύψει (εκ νέου εκτίμηση αντικτύπου).
  - Η γνωστοποίηση προϋποθέτει δυσανάλογες προσπάθειες.

Υπεύθυνος προστασίας δεδομένων – Data Protection Officer (DPO)

- Υποχρεωτικός διορισμός αν η επεξεργασία :
  - γίνεται από το Δημόσιο
  - γίνεται από τον υπεύθυνο στο πλαίσιο των βασικών του δραστηριοτήτων οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή
  - γίνεται από τον υπεύθυνο στο πλαίσιο των βασικών του δραστηριοτήτων οι οποίες προϋποθέτουν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα
- Σε όμιλο επιχειρήσεων μπορεί και 1

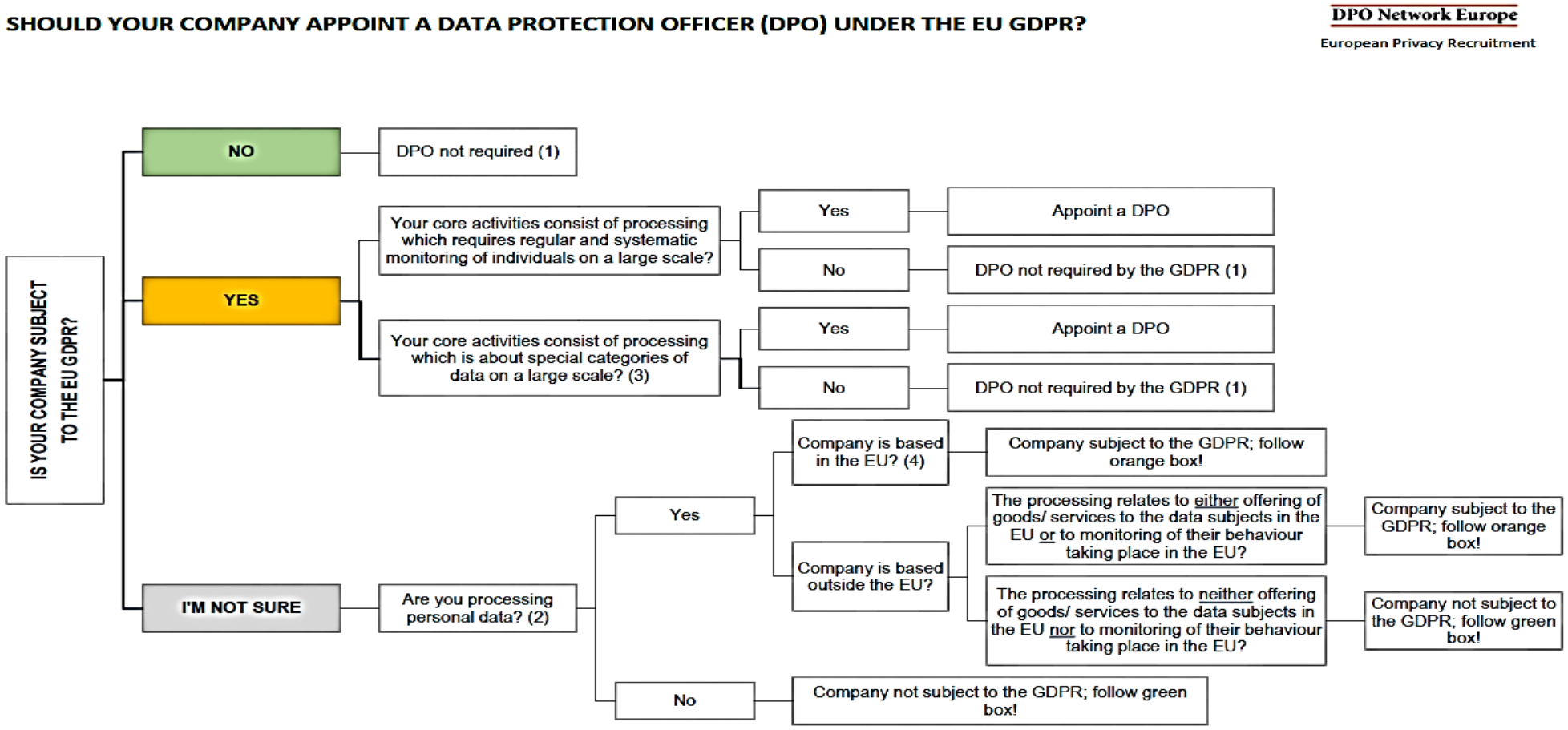
Υπεύθυνος προστασίας δεδομένων – Data Protection Officer (DPO) (Συνέχεια)

- Πώς εργάζεται:
  - Του παρέχονται οι απαραίτητοι πόροι για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόροι απαραίτητοι για τη διατήρηση της εμπειρογνωσίας του
  - Δεν λαμβάνει εντολές για την άσκηση των εν λόγω καθηκόντων
  - Δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του
  - Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία
  - Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας
  - Μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις (όχι όμως σύγκρουση συμφερόντων)
- Τι κάνει;
  - ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους σχετικά με την προστασία δεδομένων
  - παρακολουθεί τη συμμόρφωση με τη νομοθεσία για την προστασία δεδομένων και με τις πολιτικές της εταιρείας του, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων
  - παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντίκτυπου
  - συνεργάζεται με την εποπτική αρχή και ενεργεί ως σημείο επικοινωνίας με αυτήν

*π.χ. απόφαση Βαυαρικής ΑΠΔΠΧ 10/2016 επιβολή προστίμου 50.000Ε σε DPO – IT manager»

Πότε τελικά χρειάζεται μια εταιρεία DPO?

https://www.dponetwork.eu/



Υπεύθυνος προστασίας δεδομένων – Data Protection Officer (DPO) (Συνέχεια)

ΑΝΑΚΟΙΝΩΣΗ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 9-8-2017 Αρ. πρωτ.: Γ/ΕΞ/6007

Η Αρχή συνεδρίασε για θέματα που αφορούν την πιστοποίηση επαγγελματικών προσόντων Υπευθύνων Προστασίας Δεδομένων (Data Protection Officers - DPOs), στο πλαίσιο εκπαιδευτικών προγραμμάτων που πραγματοποιούνται από διάφορους φορείς, και αποφάσισε να εκδώσει την ακόλουθη ανακοίνωση προς ενημέρωση των ενδιαφερομένων: Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαπιστώνει ότι, ενόψει της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) τον Μάϊο του 2018, προσφέρονται αρκετά εκπαιδευτικά προγράμματα/σεμινάρια για τον ρόλο του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO). Στο πλαίσιο της προώθησης των εκπαιδευτικών αυτών προγραμμάτων, υπάρχουν φορείς που υποστηρίζουν ότι η προσφερόμενη εκπαίδευση αποτελεί ένα προπαρασκευαστικό στάδιο που οδηγεί σε κάποιου τύπου πιστοποίηση DPO στην ελληνική επικράτεια. Η Αρχή, με στόχο την ενημέρωση των ενδιαφερομένων, επισημαίνει ότι: • Η δραστηριοποίηση αυτή της αγοράς είναι θετική, αφού συμβάλλει στη μεταφορά γνώσης και ενημέρωσης σε θέματα του ΓΚΠΔ, πρέπει όμως να τεθεί στην ορθή της διάσταση, αποφεύγοντας τη δημιουργία εσφαλμένων εντυπώσεων ως προς τις σχετικές απαιτήσεις του ΓΚΠΔ. • Ο ΓΚΠΔ, που θα τεθεί σε ισχύ τον Μάϊο του 2018, **δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του DPO, ούτε καν ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση. • Μέχρι σήμερα κανένας φορέας στην Ελλάδα δεν έχει διαπιστευθεί για να πιστοποιεί τα επαγγελματικά προσόντα/δεξιότητες ενός DPO. Συνεπώς, οι προτεινόμενες πιστοποιήσεις DPO δεν εμπίπτουν στην κατηγορία των υφιστάμενων επίσημων ελληνικών πιστοποιήσεων**. • Η ύλη των προσφερόμενων εκπαιδευτικών προγραμμάτων μπορεί μεν να χαρακτηριστεί γενικώς ως συναφής με τον ΓΚΠΔ και τη θέση του DPO, η επιλογή της όμως αποτελεί αποκλειστική ευθύνη των φορέων που τα παρέχουν.

Αρχεία των δραστηριοτήτων επεξεργασίας – Υπεύθυνος επεξεργασίας

- Κάθε **υπεύθυνος επεξεργασίας** και, κατά περίπτωση, ο εκπρόσωπός του, τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος.
- Το εν λόγω αρχείο περιλαμβάνει όλες τις ακόλουθες πληροφορίες:
- α) το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων,
- β) τους σκοπούς της επεξεργασίας,
- γ) περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,
- δ)τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,
- ε)όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού και, σε περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, της τεκμηρίωσης των κατάλληλων εγγυήσεων,
- στ) όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων,
- ζ) όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παράγραφος

Αρχεία των δραστηριοτήτων επεξεργασίας - εκτελών την επεξεργασία

- 1. 2.Κάθε **εκτελών την επεξεργασία** και, κατά περίπτωση, ο εκπρόσωπος του εκτελούντος την επεξεργασία τηρούν αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας που διεξάγονται εκ μέρους του υπευθύνου επεξεργασίας, το οποίο περιλαμβάνει τα εξής:
- α) το όνομα και τα στοιχεία επικοινωνίας του εκτελούντος ή των εκτελούντων την επεξεργασία και των υπευθύνων επεξεργασίας εκ μέρους των οποίων ενεργεί ο εκτελών και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, καθώς και του υπευθύνου προστασίας δεδομένων,
- β) τις κατηγορίες επεξεργασιών που διεξάγονται εκ μέρους κάθε υπευθύνου επεξεργασίας,
- γ)όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού και, σε περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, της τεκμηρίωσης των κατάλληλων εγγυήσεων,
- δ) όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παράγραφος
- 1. 3.Τα αρχεία που αναφέρονται στις παραγράφους 1 και 2 υφίστανται γραπτώς, μεταξύ άλλων σε ηλεκτρονική μορφή.
- 4.Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία και, κατά περίπτωση, ο εκπρόσωπος του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία θέτουν το αρχείο στη διάθεση της εποπτικής αρχής κατόπιν αιτήματος.

SIZE MATTERS?

- Για να ληφθεί υπόψη η ειδική κατάσταση των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων, ο παρών κανονισμός περιλαμβάνει παρέκκλιση για οργανισμούς που απασχολούν λιγότερα από 250 άτομα όσον αφορά την τήρηση αρχείων
- **Αρχεία των δραστηριοτήτων επεξεργασίας:** Οι υποχρεώσεις που αναφέρονται στις παραγράφους 1 και 2 δεν ισχύουν για επιχείρηση ή οργανισμό που απασχολεί λιγότερα από 250 άτομα, εκτός εάν η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, η επεξεργασία δεν είναι περιστασιακή ή η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων κατά το άρθρο 9 παράγραφος 1 ή επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

Άρθρο 27: Αντιπρόσωποι των ελεγκτών και επεξεργαστών που δεν εδρεύουν στην Ευρωπαϊκή Ένωση

- Όταν ο Υπεύθυνος ή ο Εκτελών την Επεξεργασία Προσωπικών Δεδομένων δεν εδρεύουν στην Ευρωπαϊκή Ένωση:
- Θα πρέπει να ορίζουν γραπτώς έναν αντιπρόσωπο στην Ευρωπαϊκή Ένωση
- Ο αντιπρόσωπος θα πρέπει να εδρεύει στον τόπο όπου η επεξεργασία δεδομένων ή η κατάρτιση προφίλ λαμβάνει χώρα
- Ο αντιπρόσωπος θα υπόκειται σε κάλεσμα από τις εποπτεύουσες αρχές και το υποκείμενο των δεδομένων για τους σκοπούς του Κανονισμού
- Ο καθορισμός των αντιπροσώπων δεν απαλλάσσει τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την Επεξεργασία από νομικές ευθύνες

Διαβιβάσεις προσωπικών δεδομένων προς τρίτες χώρες- βασικά σημεία

- Μπορούν να πραγματοποιηθούν άμεσα σε περίπτωση:
  - Απόφασης επάρκειας της Επιτροπής
    - χώρες με αναγνωρισμένο ικανοποιητικό επίπεδο προστασίας, Privacy Shield
  - Αν δεν υπάρχει παρόμοια απόφαση, αν παρέχονται κατάλληλες εγγυήσεις από τον υπεύθυνο ή εκτελούντα την επεξεργασία (ά. 46 παρ. 2), ιδίως νομικές δεσμεύσεις μεταξύ δημόσιων αρχών,
    - Δεσμευτικών εταιρικών κανόνων (BCRs, δηλ. επαρκών εγγυήσεων για διαβίβαση δεδομένων εκτός Ε.Ε. μεταξύ εταιρειών ίδιου ομίλου, είδος πολυμερούς σύμβασης)
    - τυποποιημένες ρήτρες προστασίας που εκδίδονται από την Επιτροπή ((Standard Contractual Clauses, όπου χρησιμοποιούνται πρότυπα με απόλυτη ακρίβεια, βλ. Αποφάσεις 67/2010, 148/2012 (άδειες ενημέρωσης δια του Τύπου σε Ford για διαβίβαση δεδομένων σε μητρική-εκτελούσα στις Η.Π.Α. και ανάθεση επεξεργασίας σε υπεργολάβο στις Η.Π.Α. βάσει συμβατικών ρητρών 2010/87/ΕΕ)
    - κώδικας δεοντολογίας ή μηχανισμός πιστοποίησης
- Με άδεια της εποπτικής Αρχής, αν παρέχονται κατάλληλες εγγυήσεις με τη μορφή:
  - Συμβατικών ρητών μεταξύ υπευθύνου ή εκτελούντος και υπευθύνου/εκτελούντος/αποδέκτη εκτός Ε.Ε.
  - διατάξεων προς συμπερίληψη σε διοικητικές ρυθμίσεις μεταξύ δημόσιων αρχών ή φορέων οι οποίες περιλαμβάνουν εκτελεστά και ουσιαστικά δικαιώματα υποκειμένων

BCRS- Binding corporate rules

- «δεσμευτικοί εταιρικοί κανόνες»:

οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβιβάσεις ή δέσμη διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα,

Διαβιβάσεις προσωπικών δεδομένων προς τρίτες χώρες- παρεκκλίσεις

- Ρητή συγκατάθεση υποκειμένου μετά από προηγούμενη ενημέρωση για πιθανούς κινδύνους διαβίβασης
- Εκτέλεση σύμβασης μεταξύ υποκειμένου – υπευθύνου ή λήψη προσυμβατικών μέτρων
- Σύναψη ή εκτέλεση σύμβασης προς όφελος υποκειμένου μεταξύ υπευθύνου και άλλου φυσικού ή νομικού προσώπου
- Σημαντικοί λόγοι δημόσιου συμφέροντος
- Θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων
- Προστασία ζωτικών συμφερόντων υποκειμένου ή άλλων προσώπων σε περίπτωση αδυναμίας για παροχή συγκατάθεσης
- Δημόσιο μητρώο

Π.χ Άδειες σε Αρχή Καταπολέμησης Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες & Χρηματοδότησης Τρομοκρατίας που δόθηκαν από ΑΔΠΔΧ βάσει ά. 9 παρ. 2γ΄ ν. 2472/1997 (για διαφύλαξη υπέρτερου δημόσιου συμφέροντος & σε εκτέλεση συμβάσεων συνεργασίας)

Διαβιβάσεις προσωπικών δεδομένων- ΗΠΑ

- Οκτώβριος 2015: Το Ευρωπαϊκό Δικαστήριο ανακοινώνει ότι ακυρώνεται η Αρχή Ασφαλούς Λιμένα (Safe Harbor Scheme)

- Απρίλιος 2015: Άρθρο 29 το Εργατικό Κόμμα αναγνωρίζει πολλά σοβαρά ελαττώματα
  - δεν πληροί τις προϋποθέσεις επάρκειας της Ε.Ε.
  - έλλειψη αρχής παρακράτησης δεδομένων
  - μαζική και αδιάκριτη συλλογή δεδομένων για τους σκοπούς της εθνικής ασφάλειας
  - ανεπάρκεια των έννομων διορθωτικών μέτρων

- Ιούλιος 2016: Συμφωνείται και τίθεται σε εφαρμογή η Ασπίδα Ιδιωτικότητας Ε.Ε. – Η.Π.Α.(Privacy Shield)

ΕΠΟΠΤΕΙΑ

- Το Κράτος Μέλος οφείλει να ορίσει μία ή περισσότερες ανεξάρτητες αρχές εποπτείας ικανές να επιτύχουν τα ακόλουθα:
  - Να επιτηρούν την εφαρμογή αυτού του Κανονισμού
  - Να συνεργάζονται με τις υπόλοιπες αρχές εποπτείας για να επιτύχουν της εφαρμογή του Κανονισμού σε όλη την Ε.Ε. με συνέπεια
- Το Κράτος Μέλος οφείλει να:
  - Καθορίσει την κυρίαρχη αρχή εποπτείας
  - Σχεδιάσει τον μηχανισμό που θα εξασφαλίζει συμμόρφωση για τις υπόλοιπες αρχές.

ΕΠΟΠΤΕΙΑ

Οι αρχές εποπτείας οφείλουν να:

- επιτηρούν και επιβάλουν την εφαρμογή του Κανονισμού,
- προωθούν την ενημέρωση του κοινού και την κατανόηση των κινδύνων – οι δραστηριότητες που αφορούν ανήλικους οφείλουν να λαμβάνουν ειδικής προσοχής,
- συμβουλεύουν τους μετόχους σύμφωνα με τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων,
- προωθούν της ενημέρωση σχετικά με τις υποχρεώσεις των ελεγκτών και των επεξεργαστών,
- παρέχουν, έπειτα από αίτηση οποιουδήποτε υποκειμένου των δεδομένων, πληροφορίες σχετικά με την άσκηση των δικαιωμάτων τους.

ΕΠΟΠΤΕΙΑ

Άρθρο 55 Αρμοδιότητα

1. Κάθε εποπτική αρχή είναι αρμόδια να εκτελεί τα καθήκοντα και να ασκεί τις εξουσίες που της ανατίθενται σύμφωνα με τον παρόντα κανονισμό στο έδαφος του κράτους μέλους της

Άρθρο 56 Αρμοδιότητα της επικεφαλής εποπτικής αρχής

1. Με την επιφύλαξη του άρθρου 55, η εποπτική αρχή της κύριας ή της μόνης εγκατάστασης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία **είναι αρμόδια να ενεργεί ως επικεφαλής εποπτική αρχή για τις διασυνοριακές πράξεις επεξεργασίας** του εν λόγω υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σύμφωνα με τη διαδικασία που προβλέπεται στο άρθρο 60.
2. 2. Κατά παρέκκλιση από την παράγραφο 1, κάθε εποπτική αρχή είναι αρμόδια για την εξέταση υποβληθείσας καταγγελίας ή για την αντιμετώπιση ενδεχόμενης παραβίασης του παρόντος κανονισμού, εάν το αντικείμενο αφορά **μόνο εγκατάσταση στο οικείο κράτος μέλος ή επηρεάζει ουσιαστικώς υποκείμενα των δεδομένων μόνο στο οικείο κράτος μέλος**.

ΕΠΟΠΤΕΙΑ

Άρθρο 60: Συνεργασία μεταξύ της κυρίαρχης αρχής εποπτείας και των λοιπών σχετικών αρχών εποπτείας

- Συνεργασία
- Αλληλοβοήθεια
- Επικοινωνία
- μεταξύ της κυρίαρχης/επικεφαλής και των υπόλοιπων αρχών εποπτείας

ΕΠΟΠΤΕΙΑ

Άρθρο 68 Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

1. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων («Συμβούλιο Προστασίας Δεδομένων») συστήνεται ως όργανο της Ένωσης και διαθέτει νομική προσωπικότητα.

2. Το Συμβούλιο Προστασίας Δεδομένων εκπροσωπείται από τον Πρόεδρό του.

3. Το Συμβούλιο Προστασίας Δεδομένων απαρτίζεται από τον προϊστάμενο μίας εποπτικής αρχής κάθε κράτους μέλους και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων ή τους αντίστοιχους εκπροσώπους τους.

4. Εάν σε ένα κράτος μέλος υπάρχουν περισσότερες εποπτικές αρχές επιφορτισμένες με την παρακολούθηση της εφαρμογής των διατάξεων βάσει του παρόντος κανονισμού, ορίζεται κοινός εκπρόσωπος σύμφωνα με το δίκαιο του εν λόγω κράτους μέλους.

5. Η Επιτροπή δικαιούται να συμμετέχει χωρίς δικαίωμα ψήφου στις δραστηριότητες και στις συνεδριάσεις του Συμβουλίου Προστασίας Δεδομένων. Η Επιτροπή ορίζει τον εκπρόσωπό της. Ο Πρόεδρος του Συμβουλίου Προστασίας Δεδομένων ανακοινώνει στην Επιτροπή τις δραστηριότητες του Συμβουλίου Προστασίας Δεδομένων.

6. Στις περιπτώσεις που αναφέρονται στο άρθρο 65, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων έχει δικαίωμα ψήφου μόνο στις αποφάσεις που αφορούν τις αρχές και τους κανόνες που ισχύουν στα θεσμικά όργανα της Ένωσης, στους φορείς, στις υπηρεσίες και στους οργανισμούς που αντιστοιχούν κατ' ουσίαν προς εκείνους του παρόντος κανονισμού.

Γιατί να τα τηρήσει κανείς όλα αυτά;

«Παραβάσεις …επισύρουν, … **διοικητικά πρόστιμα έως**

20 000 000 EUR ή, σε περίπτωση επιχειρήσεων, **έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών** του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο»

Ενδεικτικά κριτήρια επιβολής προστίμου Ι

- Η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβάνοντας υπόψη τη φύση, την έκταση ή το σκοπό της σχετικής επεξεργασίας, καθώς και τον αριθμό των υποκειμένων των δεδομένων που έθιξε η παράβαση και το βαθμό ζημιάς που υπέστησαν
- Ο δόλος ή η αμέλεια που προκάλεσε την παράβαση
- Οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων
- Ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν
- Τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία
- Ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της

Ενδεικτικά κριτήρια επιβολής προστίμου ΙΙ (συνέχεια)

- Οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση
- Ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, ειδικότερα εάν και κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση
- Σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την πεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα
- Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης
- Κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση

Άρθρο 83: Γενικές συνθήκες για την επιβολή διοικητικών προστίμων

- Η επιβολή διοικητικών προστίμων θα είναι σε κάθε περίπτωση αποτελεσματική, αναλογική και αποθαρρυντική.
- Διοικητικά πρόστιμα που επιβάλλονται επιπρόσθετα, ή έναντι, των διορθωτικών δυνατοτήτων της αρχής εποπτείας σύμφωνα με το Άρθρο 58(2):
  - Έκδοση προειδοποιήσεων
  - Έκδοση επιπλήξεων
  - Διαταγή συμμόρφωσης με τις απαιτήσεις του Υποκείμενου των Δεδομένων
  - Αναφορά της παραβίασης Προσωπικών Δεδομένων απευθείας στο Υποκείμενο των Δεδομένων

- € 10,000,000 ή, σε περίπτωση ανάληψης υποχρέωσης, 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (όποιο εκ των δύο είναι μεγαλύτερο)
- Άρθρα
- 8: Συγκατάθεση ανηλίκου
- 11: επεξεργασία χωρίς αναγνώριση
- 25: προστασία δεδομένων λόγω σχεδιασμού και εξ' ορισμού (Privacy by Design and Privacy By Default)
- 26: Κοινοί Εκτελούντες την Επεξεργασία
- 27: αντιπρόσωποι Υπευθύνων Επεξεργασίας που δεν εδρεύουν στην Ε.Ε.
- 26 – 29 & 30: επεξεργασία
- 31: συνεργασία με την αρχή εποπτείας
- 32: ασφάλεια δεδομένων
- 33: αναφορά παραβιάσεων στην αρχή εποπτείας
- 34: ενημέρωση των κατόχων δεδομένων για παραβιάσεις
- 35: εκτίμηση επιπτώσεων προστασίας δεδομένων
- 36: πρότερη διαβούλευση
- 37-39: Υπάλληλοι Προστασίας Δεδομένων (DPOs)
- 41(4): επίβλεψη του αποδεκτού κώδικα δεοντολογίας
- 42: πιστοποίηση
- 43: σώμα πιστοποίησης

Άρθρο 83: Γενικές συνθήκες για την επιβολή διοικητικών προστίμων

- € 20,000,000 ή, σε περίπτωση ανάληψης υποχρέωσης, 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (όποιο εκ των δύο είναι μεγαλύτερο)
- Άρθρα
- 5: αρχές που σχετίζονται με την επεξεργασία προσωπικών δεδομένων
- 6: νομιμότητα της επεξεργασίας
- 7: συνθήκες συναίνεσης
- 9: επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων (πχ ευαίσθητα προσωπικά δεδομένα)
- 12-22: Δικαιώματα των υποκειμένων των δεδομένων στην ενημέρωση, πρόσβαση, διόρθωση, διαγραφή, περιορισμό στην επεξεργασία, φορητότητα δεδομένων, αντικείμενο και κατάρτιση προφίλ (profiling activities)
- 44-49: μεταφορές προσωπικών δεδομένων σε τρίτες χώρες
- 58(1): Προϋπόθεση να παρέχεται πρόσβαση στην εποπτεύουσα αρχή
- 58(2): Εντολές / περιορισμοί στην επεξεργασία ή διακοπή της ροής δεδομένων


GDPR Fines: 4% of global turnover
Privacy Budget: 0.0004% of global turnover
Written by Daniel J. Solove
www.teachprivacy.com
Illustrated by Ryan Beckwith

Έννομη προστασία- καταγγελίες, προσφυγές

- *Άρθρο 77*

Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή

*«…καταγγελία σε εποπτική αρχή, ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη **διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης** παράβασης, εάν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβαίνει τον παρόντα κανονισμό.»*

- *Άρθρο 78*

Δικαίωμα πραγματικής δικαστικής προσφυγής κατά αρχής ελέγχου

«…κατά νομικά δεσμευτικής απόφασης εποπτικής αρχής που το αφορά.»

- *Άρθρο 79*

Δικαίωμα πραγματικής δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία

*«…ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο ο υπεύθυνος επεξεργασίας ή ο **εκτελών την επεξεργασία έχουν εγκατάσταση**. Εναλλακτικά, ..ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο το υποκείμενο των δεδομένων έχει τη συνήθη διαμονή του, εκτός εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσια αρχή κράτους μέλους η οποία ενεργεί κατά την άσκηση των δημόσιων εξουσιών της.»*

Άρθρο 77: Το δικαίωμα να κατατεθεί παράπονο/προσφυγή με μια Εθνική αρχή Προστασίας Προσωπικών Δεδομένων (Αρχή Εποπτείας)

- Κάθε υποκείμενο δεδομένων έχει το δικαίωμα να καταθέσει παράπονο με μια αρχή εποπτείας
- Στο Κράτος Μέλος μόνιμης κατοικίας του
- Στον τόπο εργασίας του
- Στον τόπο όπου η υποτιθέμενη παράβαση έλαβε χώρα

- Η αρχή εποπτείας θα ενημερώνει τον καταγγέλλοντα για την πρόοδο, συμπεριλαμβανομένης της πιθανότητας δικαστικής αποζημίωσης

Αποζημιώσεις, Ευθύνες και Πρόστιμα

Άρθρο 78: Το δικαίωμα σε αποτελεσματική δικαστική αποζημίωση έναντι Αρχής Εποπτείας

- Το δικαίωμα σε δικαστική αποζημίωση έναντι νομικά δεσμευτικής απόφασης (σ.σ. τελεσίδικης απόφασης)
- Το δικαίωμα σε δικαστική αποζημίωση όπου η αρχή εποπτείας δεν χειρίζεται το παράπονο ή δεν ενημερώνει το υποκείμενο των δεδομένων για την πρόοδο ή το αποτέλεσμα
- Η δικαστική αποζημίωση θα αιτηθεί από δικαστήρια του Κράτους Μέλους όπου εδρεύει η αρχή εποπτείας
- Η αρχή εποπτείας πρέπει να παρέχει την άποψη ή απόφαση του Συμβουλίου στο δικαστήριο

Αποζημιώσεις, Ευθύνες και Πρόστιμα

Άρθρο 79: Το δικαίωμα σε αποτελεσματική δικαστική αποζημίωση έναντι Υπευθύνου Επεξεργασίας ή/και Υπεύθυνου Επεξεργασίας

- Το δικαίωμα σε δικαστική αποζημίωση όταν τα δικαιώματά τους έχουν παραβιαστεί ως αποτέλεσμα της επεξεργασίας των προσωπικών τους δεδομένων
- Οι νομικές διαδικασίες θα λάβουν χώρα στα δικαστήρια του Κράτους Μέλους όπου εδρεύει ο ελεγκτής ή ο επεξεργαστής
- Οι νομικές διαδικασίες δύναται να λάβουν χώρα στα δικαστήρια του Κράτους Μέλους όπου το υποκείμενο των δεδομένων δηλώνει μόνιμη κατοικία

Έννομη προστασία- Actio popularis

Άρθρο 80

Εκπροσώπηση υποκειμένων των δεδομένων

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να αναθέσει σε **μη κερδοσκοπικό φορέα, οργάνωση ή ένωση** που έχει συσταθεί δεόντως σύμφωνα με το δίκαιο κράτους μέλους, διαθέτει καταστατικούς σκοπούς που είναι γενικού συμφέροντος και δραστηριοποιείται στον τομέα της προστασίας των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σε σχέση με την προστασία των δεδομένων τους προσωπικού χαρακτήρα να **υποβάλει την καταγγελία για λογαριασμό του** και να ασκήσει τα δικαιώματα που αναφέρονται στα άρθρα 77, 78 και 79 για λογαριασμό του **και να ασκήσει το δικαίωμα αποζημίωσης** που αναφέρεται στο άρθρο 82 εξ ονόματός του, εφόσον προβλέπεται από το δίκαιο του κράτους μέλους.

2. Τα κράτη μέλη μπορούν να προβλέπουν ότι κάθε φορέας, οργάνωση ή ένωση που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου έχει το δικαίωμα, ανεξάρτητα από τυχόν ανάθεση του υποκειμένου των δεδομένων, να υποβάλει στο εν λόγω κράτος μέλος καταγγελία στην εποπτική αρχή που είναι αρμόδια δυνάμει του άρθρου 77 και να ασκήσει τα δικαιώματα που αναφέρονται στα άρθρα 78 και 79, εφόσον θεωρεί ότι τα δικαιώματα του υποκειμένου των δεδομένων δυνάμει του παρόντος κανονισμού παραβιάστηκαν ως αποτέλεσμα της επεξεργασίας.

Έννομη προστασία-αποζημίωση

Άρθρο 82 -**Δικαίωμα αποζημίωσης και ευθύνη**

1. Κάθε πρόσωπο το οποίο υπέστη υλική ή μη υλική ζημία ως αποτέλεσμα παραβίασης του παρόντος κανονισμού δικαιούται **αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα** την επεξεργασία για τη ζημία που υπέστη.

2. **Κάθε υπεύθυνος επεξεργασίας** που συμμετέχει στην επεξεργασία είναι υπεύθυνος για τη ζημία που προκάλεσε η εκ μέρους του επεξεργασία που παραβαίνει τον παρόντα κανονισμό. Ο εκτελών την επεξεργασία ευθύνεται για τη ζημία που προκάλεσε η επεξεργασία μόνο εφόσον δεν ανταποκρίθηκε στις υποχρεώσεις του παρόντος κανονισμού που αφορούν ειδικότερα τους εκτελούντες την επεξεργασία ή υπερέβη ή ενήργησε αντίθετα προς τις νόμιμες εντολές του υπευθύνου επεξεργασίας.

3. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία απαλλάσσεται από την ευθύνη που έχουν δυνάμει της παραγράφου 2, εάν αποδεικνύει ότι δεν φέρει καμία ευθύνη για το γενεσιουργό γεγονός της ζημίας.

4. Εάν περισσότεροι του ενός υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία ή αμφότεροι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εμπλέκονται στην ίδια επεξεργασία και, εάν δυνάμει των παραγράφων 2 και 3 είναι υπεύθυνοι για τυχόν ζημία που προκάλεσε η επεξεργασία, κάθε υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία ευθύνεται για τη συνολική ζημία, προκειμένου να διασφαλιστεί αποτελεσματική αποζημίωση του υποκειμένου των δεδομένων.

5. Εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει καταβάλει, σύμφωνα με την παράγραφο 4, πλήρη αποζημίωση για τη ζημία που προκάλεσε, ο εν λόγω υπεύθυνος ή εκτελών την επεξεργασία δικαιούται να ζητήσει από τους άλλους υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία που εμπλέκονται στην ίδια επεξεργασία την ανάκτηση μέρους της αποζημίωσης που αντιστοιχεί στο μέρος της ευθύνης τους λόγω της ζημίας που προκλήθηκε σύμφωνα με τις προϋποθέσεις της παραγράφου 2.[…]

- **Άρθρο 82: Το δικαίωμα σε αποζημίωση και απόδοση ευθυνών**

- Οποιοδήποτε πρόσωπο που έχει υποστεί υλική, ή μη υλική, βλάβη θα έχει το δικαίωμα να λάβει αποζημίωση από τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία .
- Ο εκτελών την επεξεργασία που σχετίζεται με την επεξεργασία θα είναι υπεύθυνος για βλάβες που έχουν προκληθεί από την επεξεργασία.
- Ο υπεύθυνος επεξεργασίας έχει ευθύνη μόνο για βλάβες που προκαλούνται από την επεξεργασία ή σε περίπτωση που ενήργησε αντίθετα με τις νόμιμες οδηγίες του ελεγκτή.
- Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία και ο επεξεργαστής εξαιρούνται για τις περιπτώσεις που δεν είναι υπεύθυνοι.
- Κοινή και εις ολόκληρον απόδοση ευθυνών για να διασφαλισθεί αποτελεσματική αποζημίωση
- Πρόβλεψη ρήτρας επανάκτησης αποζημίωσης

ΠΡΟΕΤΟΙΜΑΣΤΕΙΤΕ ΜΕ ΑΠΛΑ ΒΗΜΑΤΑ
[ΦΥΛΛΑΔΙΟ ΑΔΠΔΧ & ΕΝΠ]

- **ΕΓΡΗΓΟΡΣΗ:** Ενημερώστε το προσωπικό του οργανισμού σας για τις επερχόμενες μεταβολές υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων. Αξιολογήστε τους πιθανούς κινδύνους για τα προσωπικά δεδομένα που συλλέγετε ή/και επεξεργάζεστε. Διαμορφώστε στρατηγική αντιμετώπισης των πιθανών κινδύνων.
- **ΚΑΤΑΓΡΑΦΗ:** Καταγράψτε ενδελεχώς τα δεδομένα που τηρείτε και μεταβιβάζετε, τις επεξεργασίες στις οποίες προβαίνετε, το σκοπό τους και τη νομική βάση. Οι υπάρχουσες διαδικασίες ικανοποιούν τις απαιτήσεις του Κανονισμού; Οφείλετε να τηρείτε ειδικά αρχεία καταγραφής; Θα απαιτηθεί ένα είδος εσωτερικού πληροφορικού ελέγχου.
- **ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ:** Θα πρέπει να είστε σε θέση να εκτιμήσετε ποιοι κίνδυνοι υπάρχουν, από πού προέρχονται και ποιο είναι το είδος της βλάβης: Επίκειται μόνον οικονομική ζημία ή τίθεται σε κίνδυνο η ασφάλεια και τα ατομικά δικαιώματα των Υποκειμένων;
- **ΑΝΑΣΧΕΔΙΑΣΜΟΣ ΔΙΑΔΙΚΑΣΙΩΝ:** Αναπτύξτε στρατηγικής διαχείρισης των πιθανών απειλών: Ίσως θα πρέπει να εφαρμόσετε τεχνικά μέτρα που διασφαλίζουν την ακεραιότητα των δεδομένων, όπως η ψευδωνυμοποίηση και η κρυπτογράφηση, και μεθόδους περισσότερο φιλικές για τον χρήστη, όπως η προστασία *κατά το σχεδιασμό* και *εξ ορισμού*.
- **ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ:** Ο ορισμός Υπευθύνου δεν είναι πάντοτε υποχρεωτικός. Εξαρτάται από το μέγεθος της εταιρείας, τον τύπο και τον αριθμό των δεδομένων που συλλέγετε, αν η επεξεργασία κύρια επιχειρηματική δραστηριότητα και αν πραγματοποιείται σε μεγάλη κλίμακα.
- **ΚΕΙΜΕΝΑ ΠΟΛΙΤΙΚΗΣ:** Επικαιροποιήστε τη στρατηγική σας, τα κείμενα πολιτικής και τις ενημερώσεις προς τους ενδιαφερόμενους με βάση το νέο Κανονισμό.
- **ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΠΟΛΙΤΩΝ:** Επικαιροποιήστε τις διαδικασίες για τον χειρισμό των αιτημάτων και την ικανοποίηση των δικαιωμάτων των πολιτών, ιδίως ως προς την διαγραφή δεδομένων (δικαίωμα στη λήθη) ή την παροχή τους σε αναγνώσιμο ηλεκτρονικό μορφότυπο (φορητότητα δεδομένων).
- **ΣΥΓΚΑΤΑΘΕΣΗ**: Καταγράψτε και αναθεωρήστε τις μεθόδους για αναζήτηση, εξασφάλιση και καταγραφή ρητής συγκατάθεσης για κάθε επιδιωκόμενο σκοπό επεξεργασίας. Ειδικά για τους ανηλίκους, πρέπει να έχετε εξασφαλίσει τη συγκατάθεση των προσώπων που έχουν τη γονική μέριμνα, ενώ είναι απαραίτητο να διαθέτετε μεθόδους για την επαλήθευση της ηλικίας.
- **ΠΑΡΑΒΙΑΣΕΙΣ**: Υιοθετήστε μεθόδους για τον εντοπισμό, την καταγραφή και την διερεύνηση περιστατικών παραβιάσεων. Διαθέτετε διαδικασία για τις γνωστοποιήσεις παραβιάσεων προς την Αρχή και τα Υποκείμενα;
- **ΣΥΝΕΡΓΑΣΙΑ ΜΕΤΑΞΥ ΤΩΝ ΕΠΟΠΤΙΚΩΝ ΑΡΧΩΝ**: Εφ' όσον προβαίνετε σε διασυνοριακή επεξεργασία δεδομένων εντός ΕΕ πρέπει, στο πλαίσιο του μηχανισμού συνεργασίας και συνεκτικότητας, να ορίσετε το κράτος μέλος της κύριας εγκατάστασης η εποπτεύουσα Αρχή του οποίου θα είναι αρμόδια ως επικεφαλής Αρχή, για την εποπτεία της νομιμότητας της επεξεργασίας εντός της Ένωσης.
- **ΔΙΑΣΥΝΟΡΙΑΚΕΣ ΡΟΕΣ ΔΕΔΟΜΕΝΩΝ:** Αν διαβιβάζετε δεδομένα και σε τρίτες χώρες μπορεί να απαιτηθεί να χρησιμοποιήσετε δεσμευτικούς εταιρικούς κανόνες (BCRs) ή / και τυποποιημένες συμβατικές ρήτρες (SCCs) όταν συνάπτετε συμφωνίες με τους συνεργάτες σας.

1837 2017 YEARS
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
Νομική Σχολή
Εργαστήριο Νομικής Πληροφορικής

Ασφαλιστική κάλυψη για κινδύνους από κυβερνοέγκλημα ή διαρροή προσωπικών δεδομένων;

Κατάρτιση κωδίκων δεοντολογίας

- Δυνητική εκπόνηση
- Έγκριση από Εποπτική Αρχή και δημοσίευσή του
- Αν αφορά επεξεργασία σε περισσότερα κ-μ γνωμοδοτεί το Συμβούλιο Προστασίας δεδομένων και εγκρίνονται από την Ευρωπαϊκή Επιτροπή ότι έχουν γενική ισχύ
- Παρακολούθηση τήρησης από διαπιστευμένο φορέα

Κατάρτιση κωδίκων δεοντολογίας

Οι κώδικες δεοντολογίας είναι διαθέσιμοι σε εθνικό και Ευρωπαϊκό επίπεδο.

Σε Ομοσπονδίες και άλλα αντιπροσωπευτικά σώματα σε σχέση με:

- δίκαιη και με διαφάνεια επεξεργασία
- τα έννομα συμφέροντα που επιδιώκουν οι ελεγκτές σε ειδικά πλαίσια. Π.χ. τη συλλογή προσωπικών δεδομένων
- τη χρήση ψευδωνύμων στα προσωπικά δεδομένα
- τις πληροφορίες που παρέχονται στο κοινό και στα υποκείμενα των δεδομένων
- την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων
- την προστασία ανηλίκων
- τα μέτρα που εξασφαλίζουν ασφάλεια στην επεξεργασία
- την ενημέρωση της αρχής εποπτείας για παραβιάσεις προσωπικών δεδομένων
- την ενημέρωση των υποκειμένων των δεδομένων για παραβιάσεις προσωπικών δεδομένων
- τη μεταφορά προσωπικών δεδομένων σε τρίτες χώρες ή σε διεθνείς οργανισμούς, ή
- την επίλυση διαφωνιών χωρίς προκατάληψη για τα δικαιώματα των υποκειμένων των δεδομένων.

Πιστοποιήσεις – business opportunities?

- α. 42 GDPR
  - Παροτρύνουν […]τη θέσπιση **μηχανισμών πιστοποίησης** προστασίας δεδομένων και **σφραγίδων και σημάτων προστασίας δεδομένων**, με σκοπό την απόδειξη της συμμόρφωσης
  - **Εθελοντική** πιστοποίηση μέσω διαφανούς διαδικασίας
  - Όταν τα κριτήρια εγκρίνονται από το Συμβούλιο Προστασίας Δεδομένων, αυτό μπορεί να οδηγήσει σε κοινή πιστοποίηση, την **Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων**
  - Μέγιστη διάρκεια ισχύος **3 ετών**
  - **Μητρώο** Συμβουλίου Προστασίας Δεδομένων

Άρθρο 42 Πιστοποίηση

1. Τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή παροτρύνουν, ιδίως σε ενωσιακό επίπεδο, τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό **των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία**. Λαμβάνονται υπόψη οι ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων.
2. 3. Η πιστοποίηση είναι εθελοντική και διαθέσιμη μέσω διαφανούς διαδικασίας.
   4. Η πιστοποίηση σύμφωνα με το παρόν άρθρο δεν περιορίζει την ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία για συμμόρφωση προς τον παρόντα κανονισμό και δεν θίγει τα καθήκοντα και τις αρμοδιότητες των εποπτικών αρχών που είναι αρμόδιες σύμφωνα με το άρθρο 55 ή 56.

Πιστοποιήσεις για ιστοσελίδες, διαδικτυακές υπηρεσίες ή προϊόντα

Πιστοποιήσεις για οργανισμούς και επιχειρήσεις

(ενδεικτικά):

- ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements

- ISO/IEC 27018: Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- PCI/DSS: Proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB.

Πιστοποιήσεις για επαγγελματίες

(για ασφάλεια ενδεικτικά):

- (ISC)²: CISSP® Certified Information Systems Security Professional; SSCP® Systems Security Certified Practitioner
- ISACA: CISA® Certified Information Systems Auditor® An ISACA® Certification; CISM® Certified Information Security Manager® An ISACA® Certification
- EC-Council: C|EH Certified Ethical Hacker; ECSA EC-Council Certified Security Analyst
- CompTIA: CompTIA Security+
- GIAC: GSEC
- ISO/IEC: International Organization for Standardization; ISO 27001 Lead Auditor

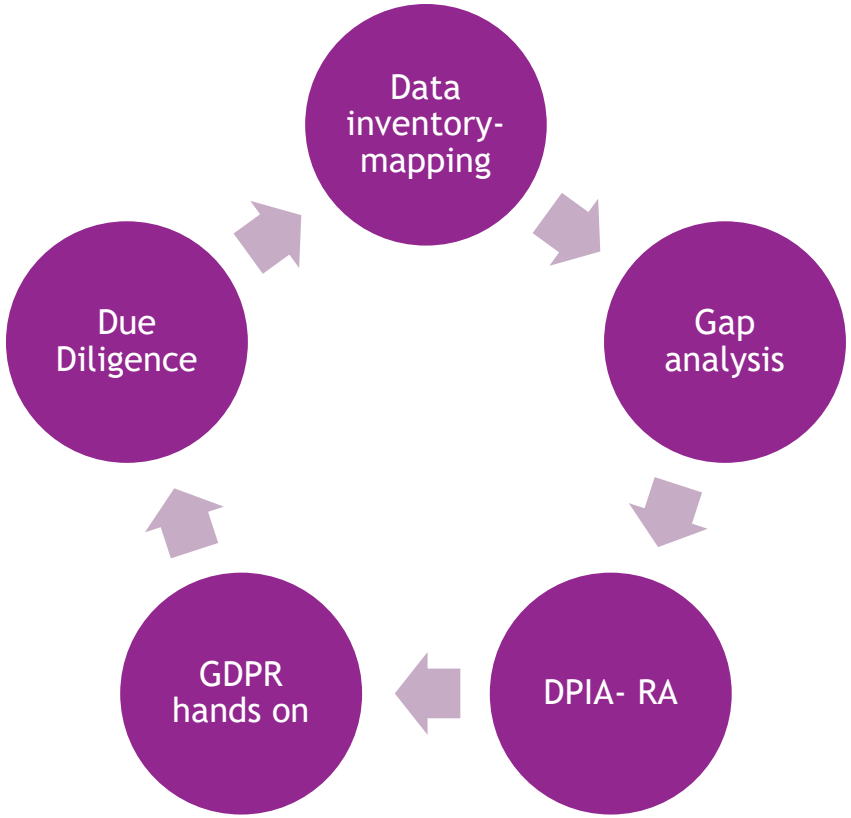
Πιστοποιήσεις για επαγγελματίες II (ενδεικτικά):

- Asia (CIPP/A)
- Canada (CIPP/C)
- Europe (CIPP/E)
- U.S. Government (CIPP/G)
- U.S. private-sector (CIPP/US)

Θεσμοί συνεργασίας ειδικών

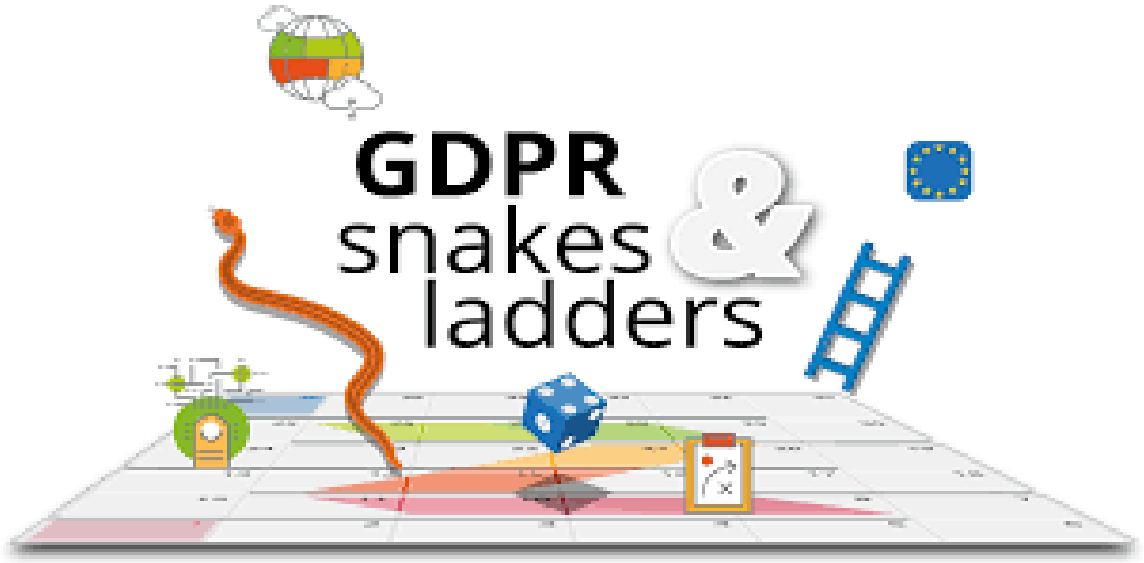
- **IPEN - Internet Privacy Engineering Network**
  https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN

Common steps for compliance



Basic step

Εν κατακλείδι




ON YOUR MARK
GET READY
ANY TIME NOW
REALLY SOON...
GDPR

Ερωτήσεις;