Εσωτερικό

Προσωπικά δεδομένα ως αντικείμενο της έρευνας

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

Δαμιανός Κοσμίδης *Head GDPR Services , GRC, Information Security Consultant, MSc Πληροφορική και Διοίκηση, DPO executive*

Περιεχόμενο

- Προσωπικά Δεδομένα & Επεξεργασία - Ορισμοί
- Οι Αρχές της Επεξεργασίας Προσωπικών Δεδομένων
- Τι ειδικό ισχύει για την έρευνα;
- Διεθνείς μεταβιβάσεις προσωπικών δεδομένων
- Τι είναι η παραβίαση προσωπικών δεδομένων…

Τι είναι ο ΓΚΠΔ (GDPR); - Άρθρο 1

1.Ο παρών κανονισμός θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα.

2.Ο παρών κανονισμός προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

3.Η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Επεξεργασία ΠΔ σημαίνει…

…κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή, ……

Προσωπικά Δεδομένα σημαίνει…

…κάθε πληροφορία που σχετίζεται με ένα ταυτοποιημένο ή που δύναται να ταυτοποιηθεί φυσικό πρόσωπο *(‘υποκείμενο των δεδομένων’)*

- **SOCIAL SECURITY NUMBER**
- **CONTACT INFORMATION** (email address, physical address, telephone and mobile numbers)
- **GOVERNMENT-ISSUED IDENTIFICATION** (driver’s license, passport, birth certificate, library card)
- **BIRTH DATE, BIRTH PLACE**
- **ONLINE INFORMATION** (Facebook, social media, passwords, PINs)
- **GEOLOCATION** (smartphone, GPS, camera)
- **VERIFICATION DATA** (mother’s maiden name, pets’ and kids’ names, high school, passwords)
- **MEDICAL RECORDS INFORMATION** (prescriptions, medical records, exams, images)
- **ACCOUNT NUMBERS** (bank, insurance, investments, credit cards)

Ειδικής κατηγορίας ή ευαίσθητα δεδομένα (άρθρο 9.1 GDPR)

- η φυλετική ή εθνοτική καταγωγή,
- τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- τη συμμετοχή σε συνδικαλιστική οργάνωση,
- η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου,
- δεδομένων που αφορούν την υγεία
- δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό

οι Αρχές της Επεξεργασίας Προσωπικών Δεδομένων (άρθρο 5)

1. **Νομιμότητα, αντικειμενικότητα και διαφάνεια**
2. **Περιορισμός του σκοπού**
3. **Ελαχιστοποίηση των δεδομένων**
4. **Ακρίβεια**
5. **Περιορισμός της περιόδου αποθήκευσης**
6. **Ακεραιότητα και εμπιστευτικότητα**
7. **Λογοδοσία**

1. Νομιμότητα, αντικειμενικότητα , διαφάνεια

Νομιμότητα (άρθρο 6(1) GDPR):
Επεξεργαζόμαστε προσωπικά δεδομένα μόνο όταν υπάρχει νομική βάση:
(α) Συγκατάθεση υποκειμένου των Δεδομένων

Αντικειμενικότητα : Ο σκοπός της επεξεργασίας πρέπει να είναι <u>ενεστώς σκοπός</u>, σαφής, κατανοητός από όλους, δίκαιος, νόμιμος , ηθικός …

Διαφάνεια: Ενημέρωση που να εξασφαλίζει ότι το φυσικό πρόσωπο «**γνωρίζει**» και «**έχει καταλάβει**» για τη χρήση των δεδομένων του και τα δικαιώματά του (άρθρα 13 & 14 του GDPR)

Τι γίνεται με τα ευαίσθητα δεδομένα; (άρθρο 9.2)

- Απαγορεύεται η επεξεργασία ευαίσθητων προσωπικών δεδομένων. Εκτός εάν :

(α) Υπάρχει ρητή συγκατάθεση του υποκειμένου των Δεδομένων

.....

(ι) απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς

Τι ειδικό ισχύει για την έρευνα;

- για σκοπούς επιστημονικής έρευνας εφαρμόζονται οι όροι και οι εγγυήσεις του άρθρου 89 του GDPR και του άρθρου 30 του ν.4624/2019:

  Τεχνικά και οργανωτικά μέτρα (κρυπτογράφηση, έλεγχος πρόσβασης), ελαχιστοποίηση ψευδωνυμοποίηση, ανωνυμοποίηση, ορισμός ΔΠΟ

- Προοπτική μελέτη – ο ερευνητής συλλέγει άμεσα τα δεδομένα
- Αναδρομική μελέτη – τα δεδομένα έχουν ήδη συλλεγεί από τον υπεύθυνο επεξεργασίας. Ο σκοπός της επιστημονικής έρευνας είναι συμβατός με αυτόν της αρχικής συλλογής (άρθρο 5.1(β) GDPR)
- Μπορούν να περιοριστούν τα δικαιώματα πρόσβασης (15), διόρθωσης (16), περιορισμού της επεξεργασίας (18), εναντίωσης (21)
- Η υποχρέωση της ενημέρωσης είναι ανελαστική σε κάθε μελέτη. Σε περίπτωση δυσανάλογης προσπάθειας, τουλάχιστον οι πληροφορίες πρέπει να είναι διαθέσιμες στο κοινό (14.5(β))

νομικό πλαίσιο στον τομέα υγείας

Κώδικας Ιατρικής Δεοντολογίας (ΚΙΔ) - v.3418/2005

Έρευνα:

Κανονισμός 536/2014 κλινικές δοκιμές φαρμάκων

Κανονισμός 745/2017 ιατροτεχνολογικών προϊόντων για ανθρώπινη χρήση

Κανονισμός 746/2017 in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα για ανθρώπινη χρήση

Η έρευνα με άλλους συνεργάτες

- **από κοινού υπεύθυνοι επεξεργασίας (joint data controllers):** Όσοι μετέχουν αποφασιστικά στη διαμόρφωση του πρωτοκόλλου μελέτης (άρθρο 26).
- **Εκτελούντες την επεξεργασία (Data Processors):** επεξεργάζονται δεδομένα για λογαριασμό και κατ' εντολή του υπεύθυνου επεξεργασίας (άρθρο 28).
- Σε κάθε περίπτωση χρειάζεται γραπτή συμφωνία (πχ. Τυποποιημένες συμβατικές ρήτρες 2021/915 εντός ΕΕ)
- Σε ποια χώρα βρίσκεται ο συνεργάτης/partner;

Διαβιβάσεις ΠΔ προς τρίτες χώρες ή διεθνείς οργανισμούς

Είμαστε σίγουροι ότι δεν στέλνουμε προσωπικά Δεδομένα σε τρίτες χώρες;

- **Social media (facebook, Twitter, TikTok, Instagram, viber, youtube…)**
- **Cloud υπηρεσίες (dropbox, weTransfer, web ερωτηματολόγια..)**
- **Email (google, yahoo, Hotmail …)**

Η Διαφορά δωρεάν και επαγγελματικών υπηρεσιών cloud

Νομιμότητα διαβίβασης ΠΔ προς τρίτες χώρες ή διεθνείς οργανισμούς -

- Απόφαση Επάρκειας για την Τρίτη χώρα από την ΕΕ (adequacy decision)

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

- Εγκεκριμένες τυποποιημένες ρήτρες προστασίας δεδομένων (Τυποποιημένες συμβατικές ρήτρες 2021/914)
- Εγκεκριμένοι δεσμευτικοί εταιρικοί κανόνες

Διασφαλίζονται κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων στις τρίτες χώρες

Τι σημαίνει παραβίαση προσωπικών δεδομένων

- Κάποιος αποκτούσε πρόσβαση στα δεδομένα μας χωρίς να είναι ανάγκη
  - (απώλεια **Εμπιστευτικότητας**)
- Τα δεδομένα μας αλλοιώνονταν με μη εξουσιοδοτημένο τρόπο ή ακούσια
  - (απώλεια **Ακεραιότητας**)
- Δεν είχαμε πρόσβαση στα δεδομένα μας την στιγμή που χρειάζεται.
  - (απώλεια **Διαθεσιμότητας**)

- Πως αυτό θα επηρέαζε:
  - **τους συμμετέχοντες**
  - **τους εργαζόμενους**
  - τη φήμη
  - οικονομικά
  - **τη συμμόρφωση με τους νόμους**
  - την ικανότητα εκπλήρωσης των συμβατικών υποχρεώσεων
  - υγεία και Ασφάλεια