

Προσωπικά Δεδομένα & Analytics: «Μια δυναμική σχέση που αλλάζει την online επιχειρηματικότητα»

Ευάγγελος Καμαράκης
Δικηγόρος LLM, MBA, CIPP/E
Data & Privacy Legal
www.dplegal.gr

Γιατί μιλάμε για προσωπικά δεδομένα Τι είναι ο GDPR;

- General Data Protection Regulation 2016/679
- Αντικαθιστά την οδηγία EC 95/46 (N 2472/1997)
- Εκκίνηση εφαρμογής 25.5.2018 (Σχεδόν δυο χρόνια αφού θεσμοθετήθηκε)
- Ισχύει για όλες σχεδόν τις επιχειρήσεις, ανεξαρτήτως αν είναι ευρωπαϊκές.

Γιατί έχει τόση σημασία ο GDPR;

Ομοιόμορφη
εφαρμογή
Δικαίου
Προστασίας
Προσωπικών
Δεδομένων σε
ΕΕ.

Αρκετές και
σημαντικές
αλλαγές σε
σχέση με
το ισχύον
νομοθετικό
πλαίσιο.

Συνειδητοποίη
ση της
σημασίας της
διαχείρισης
προσωπικών
δεδομένων για
τον πολίτη και
την
επιχείρηση:

Δικαιώματα
πολιτών

Υποχρεώσεις
και ρίσκα για
τις
επιχειρήσεις

Αυξημένα
πρόστιμα -
ποινές

Τι είναι προσωπικά δεδομένα ;

Ορισμός : «δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου»

Τι είναι
προσωπικά
δεδομένα;
Παραδείγματα

Ο Μιχάλης Νικολάου (φανταστικό πρόσωπο)
είναι μέλος της εκκλησίας του Star Trek

Ο Μιχάλης Νικολάου έχει σκύλο

Ο ένοικος του 3ου ορόφου στην οδό
Δημοκρατίας 46 έχει σκύλο

Η διεύθυνση IP 192.168.254.264 αντιστοιχεί σε
νοικοκυριό που έχει σκύλο

Ανωνυμοποίηση -
Ψευδωνυμοποίηση

Με βάση την έρευνα που έγινε σε 100 ανθρώπους, ο ερωτηθείς Νο 56 έχει σκύλο, αλλά δεν ξέρουμε ποιος είναι αυτός

Ο MN/4/Δημ46 έχει σκύλο

Ο χρήστης 36A89 έχει σκύλο

Η διεύθυνση IP που έχει κωδικοποιηθεί ως 563AZ8 αντιστοιχεί σε νοικοκυριό που έχει σκύλο

Βασικές έννοιες της νομοθεσίας περί προσωπικών δεδομένων

- Επεξεργασία: ακόμα και η πιο απλή ενέργεια αν σχετίζεται με τα προσωπικά δεδομένα θεωρείται επεξεργασία
 - Η επεξεργασία χρειάζεται νομιμοποιητική βάση (Συνήθως, αλλά όχι αποκλειστικά, συναίνεση)
- Controller (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
- Processor (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

Μας αφορά
στα analytics η
νομοθεσία
περί
προσωπικών
δεδομένων;

Εφόσον επεξεργαζόμαστε δεδομένα που θεωρούνται προσωπικά δεδομένα γιατί μπορεί να είναι επιγραμμικά αναγνωριστικά ταυτότητας (online identifiers) όπως:

- IPs
- Geolocation data
- MAC Address (Media Access Control Address)
- IMEI (International Mobile Equipment Identity)
- IMSI (International Mobile Subscriber Identity)
- UDID (Unique Device ID-Apple)

Αλλαγές που επιφέρει ο GDPR και μας αφορούν

Συναίνεση

- Η συναίνεση πρέπει να είναι «ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια»
- Τα παλιές μέθοδοι opt ins δεν αρκούν (pre-ticked boxes, συνέχεια της χρήσης ισοδυναμεί με αποδοχή)
- Ειδικές κατηγορίες προσωπικών δεδομένων : ακόμα αυστηρότερες προϋποθέσεις

Ευθύνη processors

- Πλέον ευθύνονται και αυτοί όταν:
 - ✓ Ενεργούν εκτός GDPR
 - ✓ Ενεργούν αντίθετα με όσα ορίζει η σύμβαση τους με controller, ή οι οδηγίες του controller
- Sub processors απαιτούνται:
 - ✓ γραπτές συμβάσεις που εγγυώνται την εφαρμογή GDPR- όπως για processors
 - ✓ γραπτή συγκατάθεση controller

Αλλαγές που επιφέρει ο GDPR και μας αφορούν

DPO (Υπεύθυνος προστασίας δεδομένων)

- Όλοι προαιρετικά
- Υποχρεωτικά:
 - ✓ δημόσια αρχή ή φορέας, εκτός από δικαστήρια
 - ✓ βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή
 - ✓ οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.

DPIA (Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων). Υποχρεωτικά όταν:

- «ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων»
- Ιδίως όταν:
 - ✓ profiling
 - ✓ μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων
 - ✓ Συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Αλλαγές που επιφέρει ο GDPR και μας αφορούν

Αρχή λογοδοσίας

- Ευθύνη Υπευθύνου επεξεργασίας να αποδείξει την τήρηση των παραπάνω αρχών
- Νέα υποχρέωση που εισάγει ο GDPR, με αυξημένες επιχειρησιακές απαιτήσεις και απαιτήσεις συμμόρφωσης για μια επιχείρηση

Νέα Δικαιώματα

- Δικαίωμα Διαγραφής (Erasure- right to be forgotten)
- Φορητότητα (Data Portability)
- Περιορισμός της Επεξεργασίας (πρώην blocking)

Data breach

- Ειδοποίηση της αντίστοιχης αρχής σε 72 ώρες
- Ειδοποίηση υποκειμένων των δεδομένων

Σχετική Νομοθεσία: E –privacy

- Οδηγία 2002/58 (όπως έχει τροποποιηθεί) Νόμος 3471/2006 (όπως έχει τροποποιηθεί)
- Αφορά στον τομέα τον ηλεκτρονικών επικοινωνιών και σε προσωπικά δεδομένα αλλά όχι μόνο
- Τεχνολογίες Cookies, Web beacons, & local storage «μαζεύουν» δεδομένα
- Προβλέπεται επίσης συναίνεση για πολλές κατηγορίες cookies αλλά όχι τόσο αυστηρή όπως στον GDPR
- Σύντομα θα έλθει ο κανονισμός E-Privacy
 - Rapporteur : Marju Lauristin
 - Τεράστια πολιτική μάχη
 - Προς το παρόν φαίνεται να κερδίζουν οι πλευρές που είναι pro-privacy

Analytics vs Marketing Cookies

Cookies από επιχειρήσεις analytics: Σχεδόν πάντα third party και επομένως χρειάζονται κάποιου είδους συναίνεση

1. Analytics cookies -> σχετικά πιο ασφαλή (δε χρειάζονται καν συναίνεση αν είναι first party)
2. Advertising/marketing cookies -> πιο επικίνδυνα (high risk)

Ενδεικτικά :content personalization, frequency capping, financial logging, ad affiliation, click fraud detection, research and market analysis.

GDPR καθιερώνει δικαίωμα εναντίωσης στο direct marketing και στο profiling

Τα cookies σήμερα: Μια λύση ανάγκης που δεν έχει δοκιμασθεί η αντοχή της



Χρησιμοποιώντας αυτόν τον ιστότοπο, συμφωνείτε με την χρήση των cookies. Περισσότερα εδώ

Ο κανόνας

OK



Secure | https://edps.europa.eu/about-edps/data-protection-edps_en

EUROPEAN DATA PROTECTION SUPERVISOR
The EU's independent data protection authority

English (en)

Home About Data Protection Press & Publications

> About > Data Protection within the EDPS

Data Protection within the EDPS

In this section, you will find information about our [Data Protection Officer](#) and [your rights](#) when the EDPS processes your personal data. For more information about how your personal data might be used when you visit this website, read our [data protection notice](#) page. For more information about cookies and our website, including how to opt-out, please go to our [cookies](#) page.

If you wish to opt-out or opt-in from our cookie service, please follow this [link](#).

Français Deutsch

Η εξαίρεση

We use cookies on our website to support technical features that enhance your user experience.
We also use analytics. To opt-out from analytics, click for more information.

[I've read it](#) [More information](#)

Opting out

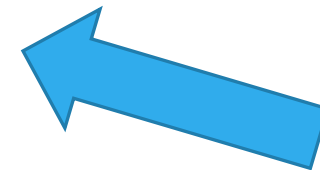
By default, the browsing experience of website visitors is tracked by Europa Analytics in order to produce anonymised statistics.

You may choose not to be tracked (opt-out). If you change your mind, you can choose to be tracked again (opt-in).

If you wish to opt-out (or opt-in back again) please click here:

You may choose not to have a unique web analytics cookie identification number assigned to your computer to avoid the aggregation and analysis of data collected on this website.
To make that choice, please click below to receive an opt-out cookie.

You are currently opted in. [Click here to opt out.](#)



We use cookies on our website to support technical features that enhance your user experience.
We also use analytics. To opt-out from analytics, click for more information.

[I've read it](#) [More information](#)

Η συναίνεση στο μέλλον σύμφωνα με GDPR & E-privacy regulation

- Το e-privacy regulation μάλλον θα ακολουθήσει την γραμμή του GDPR στο θέμα της συναίνεσης
- Πλέον η συναίνεση πολύ δύσκολο να αποκτηθεί, διατηρηθεί και να αποδειχθεί
- Η συναίνεση η μόνη νομιμοποιητική βάση έκτος από λίγα εργαλεία analytics «technically necessary for measuring the reach of an information society service requested by the user»
- GDPR+ Eprivacy reg : Η συναίνεση πρέπει να είναι «ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια»
 - Prechecked boxes, Cookie banner, Cookies walls, tracking μέσω ελεύθερων wifi/hotspots τέλος
 - Κάποιοι υποστηρίζουν soft opt in θεωρηθεί αποδεκτή λύση (αλλά ίσως και όχι)
 - Διαφορετικά opt ins , για διαφορετικές κατηγορίες επεξεργασίας (πχ marketing, analytics)
 - Συνεχώς δικαίωμα για opt out

Η Σχέση E-privacy - GDPR

- Η ύπαρξη του E privacy καθεστώτος, δε καθιστά το GDPR αυτομάτως μη εφαρμόσιμο στο σύνολό του. Οι διατάξεις αλληλοσυμπληρώνονται
- Ποιες διατάξεις εφαρμόζονται; Ποιο είναι το ειδικότερο νομικό καθεστώς (lex specialis);
- Η απάντηση «e-privacy» που δείχνει να επικρατεί είναι ευλογοφανής αλλά σέ περιβάλλον GDPR δεν είναι όσο αυτονόητη φαίνεται.
- Η αλληλεπίδραση E-Privacy & GDPR δεν έχει ρυθμιστεί πλήρως και θα απασχολήσει τη νομική επιστήμη και τη νομολογία.
- Νέα εποχή για τα cookies, ο GDPR είναι μόνο η αρχή, αλλάζει ριζικά το τοπίο για πολλούς επιχειρηματικούς κλάδους

Τι είναι καλό να κάνουν οι επιχειρήσεις analytics;

Συνειδητοποίηση

Επεξεργάζομαι δεδομένα; Τι είδους;

Τι τεχνολογίες χρησιμοποιώ; Που αποσκοπούν;

Processors ή Controllers; Έχω Sub-processors;

DPO ή DPIA; Με αφορούν;

Ασφάλεια δεδομένων (data breaches κλπ)

Καταγραφή συμμόρφωσης

Ετοιμότητα να ανταποκριθώ στις απαιτήσεις πελατών

Η νομοθεσία περί προσωπικών δεδομένων ως ευκαιρία

Σας ευχαριστώ!



ΕΥΑΓΓΕΛΟΣ ΚΑΜΑΡΑΚΗΣ & ΣΥΝΕΡΓΑΤΕΣ