Συμμόρφωση Οργανισμών με τον Κανονισμό GDPR για την Προστασία της Ιδιωτικότητας

ΛΑΓΟΥ ΠΑΝΑΓΙΩΤΑ

27/05/2019

Περιεχόμενα

- ΓΚΠΠΔ – Γενικές Αρχές
- Δικαιώματα Υποκειμένων
- Ευθύνες του Υπεύθυνου Επεξεργασίας
- ΓΚΠΠΔ σε αριθμούς
- Ερωτήσεις

ΓΚΠΠΔ – Γενικές Αρχές

Σημαντικές Αλλαγές

Αντικείμενο και Στόχοι (άρθρο 1)

- Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΠΔ) 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.

- Ο ΓΚΠΠΔ προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμα τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Πεδίο Εφαρμογής (άρθρο 3)

Όταν διεξάγεται επεξεργασία δεδομένων προσωπικού χαρακτήρα:

- Πολιτών της Ευρωπαϊκής Ένωσης
- Από Υπεύθυνο Επεξεργασίας ή Εκτελών την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα που είναι εγκαταστημένος στην Ευρωπαϊκή Ένωση

Σημαντικοί Ορισμοί (άρθρο 4) - Α

- **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,
- **Επεξεργασία:** κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, 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,

Σημαντικοί Ορισμοί (άρθρο 4) - Β

- **Υπεύθυνος επεξεργασίας (άρθρο 24)**: 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,
- **Εκτελών την επεξεργασία (άρθρο 28)**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας,

Ειδικές Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα (άρθρο 9)

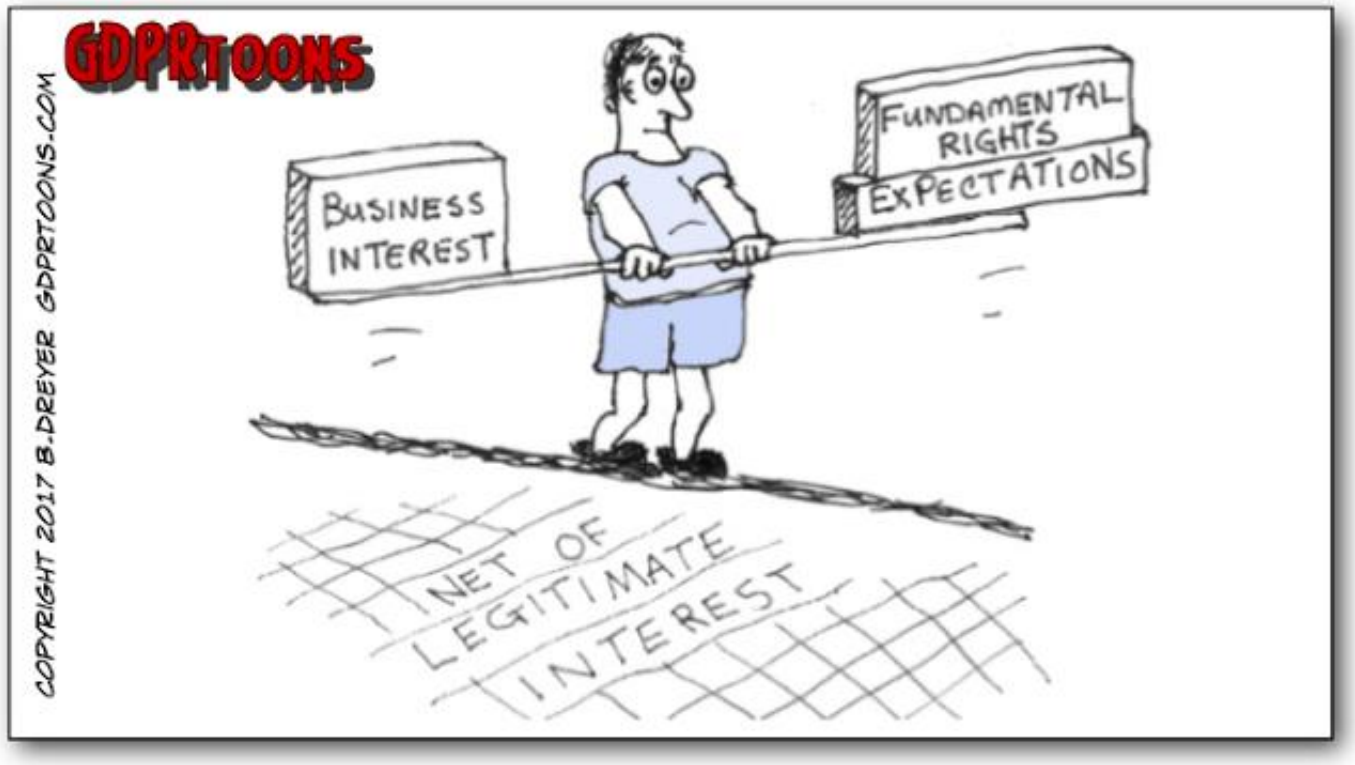
- **Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα**: Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη ***φυλετική ή εθνοτική καταγωγή***, τα ***πολιτικά φρονήματα***, τις ***θρησκευτικές ή φιλοσοφικές*** πεποιθήσεις ή τη συμμετοχή σε ***συνδικαλιστική*** οργάνωση, καθώς και η επεξεργασία ***γενετικών*** δεδομένων, ***βιομετρικών*** δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την ***υγεία*** ή δεδομένων που αφορούν τη ***σεξουαλική ζωή*** φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

Νομιμότητα της Επεξεργασίας (άρθρο 6) - Α

- Συγκατάθεση
- Σύμβαση
- Έννομη Υποχρέωση

Νομιμότητα της Επεξεργασίας (άρθρο 6) - Β

- Διαφύλαξη ζωτικού συμφέροντος του υποκειμένου
- Εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον
- Έννομο Συμφέρον



Δικαιώματα των Υποκειμένων

Δικαιώματα Των Υποκειμένων - Α

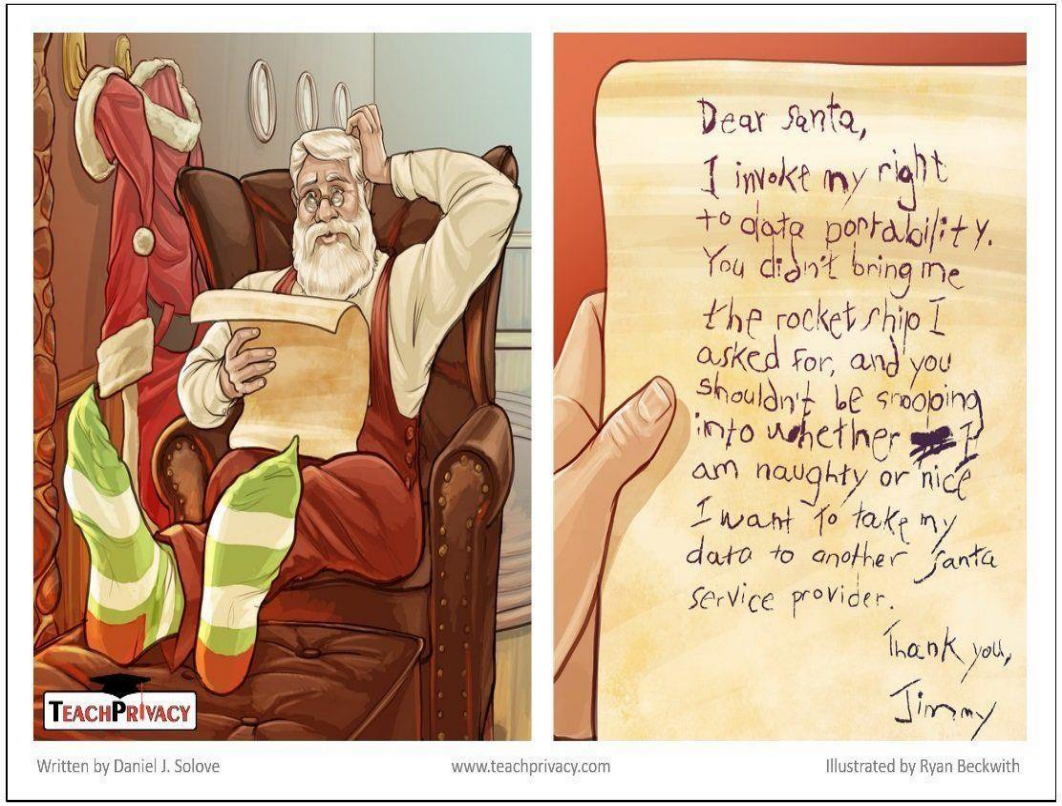
- **Διαφάνεια (άρθρο 12):** Ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση.
- **Δικαίωμα πρόσβασης (άρθρο 15):** Το υποκείμενο των δεδομένων έχει το δικαίωμα πρόσβασης στα δικά του δεδομένα προσωπικού χαρακτήρα

Δικαιώματα Των Υποκειμένων - Β

- **Δικαίωμα Διόρθωσης (άρθρο 16):** Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν.
- **Δικαίωμα Διαγραφής (άρθρο 17):** Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Δικαιώματα Των Υποκειμένων - Γ

- **Δικαίωμα Φορητότητας (άρθρο 20):** Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα.
- **Αυτοματοποιημένη ατομική λήψη αποφάσεων (κατάρτιση προφίλ) (άρθρο 22):** Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο.



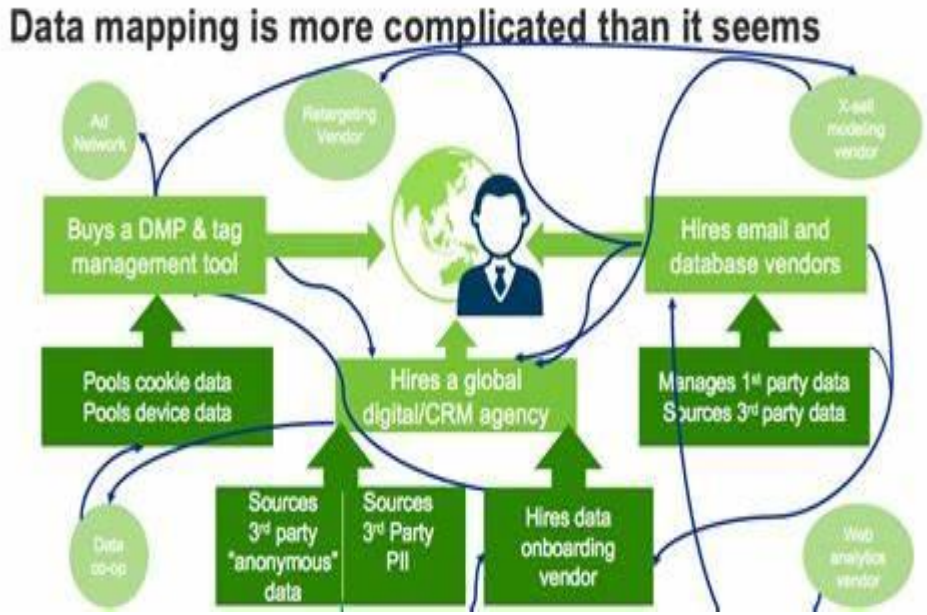
Ευθύνες του Υπεύθυνου Επεξεργασίας

Προστασία από το σχεδιασμό και εξ' ορισμού (άρθρο 25)

- **Προστασία από το σχεδιασμό και εξ' ορισμού (άρθρο 25):** Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

Αρχεία Δραστηριοτήτων Επεξεργασίας (άρθρο 30)

Κάθε υπεύθυνος επεξεργασίας και, κατά περίπτωση, ο εκπρόσωπός του, τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος.



Υπόδειγμα Αρχείου Δραστηριοτήτων Επεξεργασίας

Κωδ. Δραστηριότητας	**Υπεύθυνος Επεξεργασίας**	**Στοιχεία Επικοινωνίας Υπεύθυνου Επεξεργασίας**	**Από κοινού Υπεύθυνοι Επεξεργασίας**	**Εκπρόσωπος Υπεύθυνου Επεξεργασίας**	**Υπεύθυνος Προστασίας Δεδομένων**	**Σύντομη περιγραφή της εργασίας/διαδικασίας αναφορικά με την επεξεργασία των προσωπικών δεδομένων**	**Σκοπός Επεξεργασίας**	**Τρίτα μέρη στα οποία πραγματοποιείται μεταφορά δεδομένων**	**Εκτελών την Επεξεργασία**	**Μορφή διαβιβάσιμων δεδομένων στον Εκτελών την Επεξεργασία/ Τρίτα Μέρη**
1	XXXX ΑΕ	Διεύθυνση, Τηλ. Fax E-mail	Δ/Υ	Δ/Υ	Ονομα mail	Συλλογή, καταχώρηση, αναζήτηση, συνδυασμός, συσχέτιση, οργάνωση, χρήση, αποθήκευση και κοινολόγηση με διαβίβαση δεδομένων προσωπικού χαρακτήρα υπαλλήλων στο πλαίσιο υπολογισμού των μηνιαίων αποδοχών τους	Μισθοδοσία	Ενιαίος Φορέας Κοινωνικής Ασφάλισης Υπουργείο Εργασίας και Κοινωνικής Ασφάλισης Οργανισμός Απασχολήσεως Εργατικού Δυναμικού Ανεξάρτητη Αρχή Δημοσίων Εσόδων	Δ/Υ	Ηλεκτρονική

Υπόδειγμα Αρχείου Επεξεργασίας

Διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή σε διεθνή οργανισμό	**Περιγραφή των Υποκειμένων των Δεδομένων/ Αναφορά σε Ανήλικο**	**Φύση Προσωπικών Δεδομένων (απλά ή/και ευαίσθητα)**	**Τύπος Προσωπικών Δεδομένων**	**Μορφή Επεξεργασίας**	**Σχετικό Πληροφοριακό Σύστημα**	**Τμήματα που εμπλέκονται στην Επεξεργασία**	**Νομική Βάση**	**Περίοδος Διατήρησης Δεδομένων**	**Τεχνικά και Οργανωτικά Μέτρα**
Όχι	Υπάλληλοι	Απλά	Ονοματεπώνυμο Όνομα πατρός, μητρός Αριθμός μητρώου Φύλο Ημερομηνία γέννησης Διεύθυνση Στοιχεία ταυτότητας ΑΦΜ ΑΜΚΑ Ηλεκτρονική διεύθυνση Θέση εργασίας Μισθός Τραπεζικός λογαριασμός Οικογενειακή κατάσταση Προκαταβολές Οικονομικά στοιχεία Άδειες	Φυσική και Ηλεκτρονική	Σύστημα μισθοδοσίας E-mail File Server	Διεύθυνση Ανθρώπινου Δυναμικού Λογιστήριο	Σύμβαση	Επ' αόριστον	Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων Διαδικασίες διαχείρισης φυσικής και λογικής πρόσβασης χρηστών Μηχανισμοί αυθεντικοποίησης Συμβάσεις με τρίτους Κλειδωμένοι φωριαμοί Μέτρα για την προστασία της φυσικής ασφάλειας (φύλακες, κάμερες) Firewalls Antivirus Patching Αντίγραφα ασφαλείας συστημάτων Μηχανισμοί διαχείρισης αρχείων καταγραφής Μέτρα προστασίας που υλοποιούνται στους υπολογιστές των χρηστών Κρυπτογραφημένη απομακρυσμένη πρόσβαση

Ασφάλεια επεξεργασίας (άρθρο 32) (Α)

Τεχνικά και Οργανωτικά μέτρα:

- Ψευδωνυμοποίηση και κρυπτογράφηση:
  - Emails
  - File server
  - Βάσεις Δεδομένων
  - USBs
- Αποκατάσταση σε περίπτωση παραβίασης

"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."

Ασφάλεια επεξεργασίας (άρθρο 32) (Β)

Τεχνικά και Οργανωτικά μέτρα:

- Διασφάλιση απορρήτου, ακεραιότητας και διαθεσιμότητας
- Δοκιμές των τεχνικών και οργανωτικών μέτρων ασφάλειας

Μέτρα για τη Διασφάλιση Απορρήτου, Ακεραιότητας και Διαθεσιμότητας - Α

Πολιτικές, Διαδικασίες και Ρόλοι

- Πολιτική Ασφάλειας Πληροφοριών (Information Security Policy)
- Πολιτική Ιδιωτικότητας (Privacy Policy)
- Πολιτική Διακράτησης (Retention Policy)
- Διαδικασία διαχείρισης αλλαγών (Change Management):
  - Διαχωρισμός παραγωγικού και δοκιμαστικού περιβάλλοντος
  - Έγκριση του σχεδιασμού της αλλαγής και πριν την υλοποίηση
  - Δοκιμές
- Πλάνο Επιχειρησιακής Συνέχειας (Business Continuity Plan – BCP)

Μέτρα για τη Διασφάλιση Απορρήτου, Ακεραιότητας και Διαθεσιμότητας - Β

Πολιτικές, Διαδικασίες και Ρόλοι

- Διαδικασία αντιμετώπισης παραβιάσεων
- Διαχείριση τρίτων (συμβατικοί όροι για την ασφάλεια πληροφοριών και SLAs)
- Διαδικασία εσωτερικών ελέγχων
- Μεθοδολογία και διαδικασία αξιολόγησης κινδύνων
- Περιοδική αναθεώρηση ενεργών λογαριασμών σε δίκτυο και εφαρμογές
- Ενημέρωση και εκπαιδεύσεις
- Ρόλος Υπεύθυνου Ασφάλειας (Information Security Officer)

Μέτρα για τη Διασφάλιση Απορρήτου, Ακεραιότητας και Διαθεσιμότητας - Γ

Τεχνικά Μέτρα

- Υλοποίηση προσωπικών λογαριασμών πρόσβασης
- Σύστημα εξουσιοδότησης
- Πολιτική κωδικών πρόσβασης
- Ενεργοποίηση καταγραφής κίνησης σε δικτυακό επίπεδο και σε επίπεδο εφαρμογών
- Χρήση εργαλείων αποθήκευσης και παρακολούθησης των αρχείων καταγραφής (SIEM – Security Information and Event Management)

Μέτρα για τη Διασφάλιση Απορρήτου, Ακεραιότητας και Διαθεσιμότητας - Δ

Τεχνικά Μέτρα

- Χρήση αντιϊκού εργαλείου (antivirus)
- Χρήση firewall
- Διαχείριση ασφάλειας εταιρικών συσκευών (MDM – Mobile Device Management)
- Περιορισμός δικαιωμάτων χρηστών στον εξοπλισμό:
  - Απενεργοποίηση θύρων USB
  - Απενεργοποίηση διαχειριστικών δικαιωμάτων των χρηστών στους υπολογιστές
- Περιοδική αξιολόγηση του δικτύου για ευάλωτα σημεία από δικτυακές απειλές (Cyber Security Assessment)

Μέτρα για τη Διασφάλιση Απορρήτου, Ακεραιότητας και Διαθεσιμότητας - Ε

Τεχνικά Μέτρα

- Χρήση αντιγράφων ασφαλείας
- Εφαρμογή συστημάτων πρόληψης, ανίχνευσης και περιορισμού παρεισδύσεων (IPS – Intrusion Prevention System / IDS – Intrusion Prevention System)
- Χρήση DLP (Data Leakage Prevention) εργαλείων
- Τακτική ενημέρωση συστημάτων (patch management)
- Προστασία καμερών που συνδέονται στο δίκτυο πληροφορικής

Μέτρα για τη Διασφάλιση Απορρήτου, Ακεραιότητας και Διαθεσιμότητας - Ζ

Τεχνικά Μέτρα

- Ειδοποίηση παρατυπίας ή επικίνδυνων συμπεριφορών
- Διαχείριση ευπαθειών
- Ασφαλή ανάπτυξη κώδικα εφαρμογών (secure coding)
- GRC εργαλεία (Governance, risk management, compliance)

Γνωστοποίηση Παραβίασης στην Εποπτική Αρχή (άρθρο 33)

- Εντός 72 ωρών
- Περιγραφή της φύσης της παραβίασης
- Όνομα και στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων
- Συνέπειες της παραβίασης
- Ανάλυση των μέτρων για την αντιμετώπιση της παραβίασης
- Ενημέρωση των υποκειμένων των δεδομένων στην περίπτωση που η παραβίαση θέτει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (άρθρο 34)

Παραδείγματα Παραβιάσεων - Α

- Νοσοκομείο στην Πορτογαλία – Παραβίαση της αρχής της ελαχιστοποίησης δεδομένων (data minimization)

https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/

- Knuddels – Έλλειψη κρυπτογράφησης προσωπικών δεδομένων χρηστών

https://www.itgovernance.eu/blog/en/chat-app-knuddels-fined-e20000-for-gdpr-breach

Παραδείγματα Παραβιάσεων - Β

- Marriott – μη εξουσιοδοτημένη πρόσβαση σε δεδομένα 500 εκατομμύρια πελατών και μη έγκαιρη ενημέρωση της Αρχής (μη συμμόρφωση με το χρονικό όριο των 72 ωρών)

https://www.compliancejunction.com/penalty-for-marriott-hotels-gdpr-breach-could-be-up-to-915/

- Facebook – παραβίαση δεδομένων προσωπικού χαρακτήρα 50 εκατομμύρια χρηστών

https://www.zdnet.com/article/facebook-discloses-network-breach-affecting-50-million-user-accounts/

- Google – παραβίαση της αρχής της διαφάνειας

https://www.businessinsider.com/france-fines-google-57-million-for-gdpr-breach-2019-1

Εκτίμηση Αντικτύπου (άρθρο 35)

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, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.

9 Κριτήρια – Διεξαγωγή Εκτίμησης Αντικτύπου

1. Συστηματική αξιολόγηση (κατάρτιση προφίλ)
2. Λήψη αυτοματοποιημένων αποφάσεων
3. Παρεμπόδιση του υποκειμένου από την άσκηση των δικαιωμάτων του
4. Συστηματική επεξεργασία
5. Επεξεργασία σε μεγάλη κλίμακα
6. Ευαίσθητα δεδομένα προσωπικού χαρακτήρα
7. Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογιών
8. Συνδυασμός ή συσχέτιση δεδομένων
9. Ευάλωτα υποκείμενα

Περιεχόμενα της Εκτίμησης Αντικτύπου

- Περιγραφή της επεξεργασίας
- Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,
- Εκτίμηση των κινδύνων
- Μέτρα προστασίας

Υπεύθυνος Προστασίας Προσωπικών Δεδομένων (άρθρο 37)

Πότε απαιτείται:

- Η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα
- Όταν απαιτείται τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα
- Επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα (άρθρο 9)

Υπεύθυνος Προστασίας Προσωπικών Δεδομένων (άρθρο 39)

Καθήκοντα:

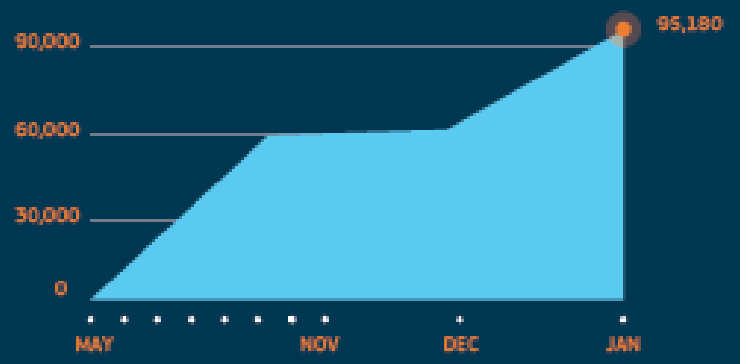
- Ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας και τους εκτελούντες την επεξεργασία αναφορικά με τις υποχρεώσεις με βάση των ΓΚΠΔ
- Παρακολουθεί τη συμμόρφωση με τον ΓΚΠΔ
- Παρέχει συμβουλές αναφορικά με την εκτίμηση αντικτύπου
- Συνεργάζεται και είναι σημείο επικοινωνίας με την Εποπτική Αρχή

ΓΚΠΠΔ σε Αριθμούς

ΓΚΠΠΔ σε Αριθμούς - Α

Number of complaints to Data Protection Authorities (DPAs) under the GDPR*

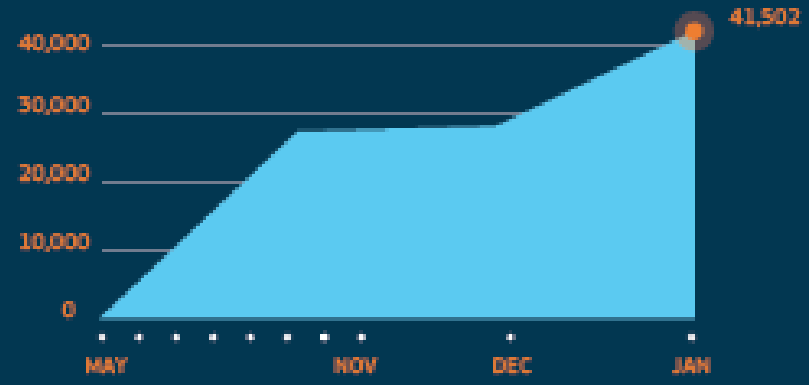
Complaints can come from any individual who believe their rights under GDPR have been violated, but the GDPR also introduced the possibility for an organisation mandated by individuals to introduce such complaints. This possibility has been used immediately after the entry into application of the GDPR.



Accumulated number over time.**
From all data protection authorities in Europe.

Number of data breach notifications*

When personal data for which a company is responsible is accidentally or unlawfully disclosed, that company is obliged to report this data breach to their national DPA within 72 hours after finding out about the breach.



Accumulated number over time.**
From all data protection authorities in Europe.

https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf

ΓΚΠΠΔ σε Αριθμούς - Β

https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf

Ερωτήσεις;