

Προετοιμασία για μια νέα σχέση με την Αρχή Προστασίας Δεδομένων

Η ενίσχυση των δικαιωμάτων στην πράξη & τα εργαλεία συμμόρφωσης για τη μετάβαση από το ν.2472/1997 στον ΓΚΠΔ

Γ: Προετοιμάζοντας τη συμμόρφωση σε 10 βήματα

Γεώργιος Ρουσόπουλος

Δρ. Μηχ. Η/Υ & Πληροφορικής

Ε.Ε.Π. - Α.Π.Δ.Π.Χ.

grousopoulos at dpa.gr

Κωνσταντίνος Λιμνιώτης

Δρ. Πληροφορικής & Τηλεπικοινωνιών

Ε.Ε.Π. - Α.Π.Δ.Π.Χ.

klimniotis at dpa.gr



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Προετοιμασία για τον ΓΚΠΔ

- Οι ακριβείς υποχρεώσεις για τον κάθε φορέα τελικά εξαρτώνται από διάφορους παράγοντες
 - Φύση της επεξεργασίας, εκτιμώμενοι κίνδυνοι,
- Ωστόσο, είναι σημαντικό ο κάθε φορέας να εντοπίσει έγκαιρα τις υποχρεώσεις του
- Συστηματικοποίηση των βασικών βημάτων που πρέπει να ακολουθηθούν από τους φορείς, για να είναι έτοιμοι για τον ΓΚΠΔ
 - Υπεύθυνοι επεξεργασίας
αλλά και
 - Εκτελούντες την επεξεργασία
- Στα βήματα εμπλέκονται:
 - Διοίκηση, Επιχειρησιακή λειτουργία, Νομικό τμήμα, Τμήμα Πληροφορικής κ.α.



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

1

Ενημέρωση – Ετοιμότητα



- Η συμμόρφωση με το ΓΚΠΔ θα πρέπει να αντιμετωπιστεί ως **μία συστηματική δράση**, με τον κατάλληλο σχεδιασμό
- Όλο το ανθρώπινο δυναμικό θα πρέπει να είναι ενήμερο για την αλλαγή του νομικού πλαισίου
 - Π.χ.: Περιστατικά παραβίασης δεδομένων ενδέχεται να υποπέσουν στην αντίληψη του οποιουδήποτε
- Τα **πρόσωπα-κλειδιά** του φορέα πρέπει να κατανοήσουν την αλλαγή στο νομικό πλαίσιο με τις συνέπειες που αυτή επιφέρει
 - : Ο ΓΠΚΔ μπορεί να επιφέρει αύξηση στο φόρτο εργασίας του φορέα
 - Π.χ. απλά και μόνο για την ικανοποίηση των δικαιωμάτων
 - Γρήγορη ανάθεση κατάλληλων ρόλων και αρμοδιοτήτων
 - Προετοιμασία εν όψει της 25/5/2018, διαρκής εφαρμογή στη συνέχεια
- Μία **πρώτη αποτίμηση σημαντικών «ελλείψεων»**, με εύρεση τρόπων αντιμετώπισής τους, είναι σημαντικό να γίνει έγκαιρα, γιατί θα διευκολύνει τα επόμενα βήματα





- **Αναγνώριση των δραστηριοτήτων**
 - **Προσοχή: Πολλές μπορεί να μην είναι άμεσα εμφανείς!**
 - Αρχείο εγγράφων, αρχείο προσωπικού, αρχείο πελατών, αρχεία από ηλεκτρονικές εφαρμογές, αρχεία επαφών για επικοινωνιακούς σκοπούς, αρχεία για σκοπούς ασφάλειας (π.χ. υλικό καμερών, καταγραφής προσβάσεων σε διαδικτυακές υπηρεσίες) κτλ.
 - Διαχωρισμός ανά σκοπό επεξεργασίας
- **Υπάρχει υποχρέωση καταγραφής αρχείων δραστηριοτήτων;**
 - Η επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα των προσώπων;
 - Η επεξεργασία αφορά ειδικές κατηγορίες δεδομένων ή δεδομένα αναφορικά με ποινικές καταδίκες;
 - Προσοχή: Οι ειδικές κατηγορίες («ευαίσθητα» δεδομένα) διευρύνονται στο ΓΚΠΔ
 - Ο φορέας απασχολεί περισσότερα από 250 άτομα;
- **Καταγραφή αρχείων δραστηριοτήτων**
 - Ποιος; Γιατί; Τι; Σε ποιόν; Διαβιβάσεις; Για πόσο; Πως;
- Η καταγραφή των αρχείων βαρύνει και τον εκτελούντα την επεξεργασία, για τις δραστηριότητες που πραγματοποιεί για λογαριασμό του υπευθύνου





Έλεγχος τήρησης συμμόρφωσης

- **Για κάθε έναν από τους σκοπούς επεξεργασίας:**

- Είναι ο σκοπός σαφής;
- Γίνεται επεξεργασία μόνο στο πλαίσιο αυτού του σκοπού;
- Πώς έχουν ληφθεί τα δεδομένα;
- Είναι τα απολύτως απαραίτητα δεδομένα για τον εν λόγω σκοπό;
- Πόσος χρόνος απαιτείται για την επεξεργασία των δεδομένων;

- Πόσο ασφαλής είναι η τήρηση και περαιτέρω επεξεργασία των δεδομένων;
 - Κρυπτογραφούνται; Ψευδωνυμοποιούνται;
 - Ποια πρόσωπα είναι αυτά που πρέπει να έχουν πρόσβαση;
 -
- Οι συνεργαζόμενες εταιρείες παρέχουν εγγυήσεις για τη συμμόρφωση με το ΓΚΠΔ;
- Ο έλεγχος ως προς το αν τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των προσώπων πρέπει να είναι **συνεχής**





Έλεγχος τήρησης συμμόρφωσης

- **Για κάθε έναν από τους σκοπούς επεξεργασίας:**
 - Γίνεται επεξεργασία αποκλειστικά πάνω στη βάση των καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας;
 - Επεξεργασία για άλλο σκοπό, με πρωτοβουλία του εκτελούντος, τον καθιστά υπεύθυνο επεξεργασίας και αποτελεί παράβαση
 - Τα πρόσωπα που είναι εξουσιοδοτημένα, έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας;
- Πόσο ασφαλής είναι η τήρηση και περαιτέρω επεξεργασία των δεδομένων;
 - Κρυπτογραφούνται; Ψευδωνυμοποιούνται;
 - Ποια πρόσωπα είναι αυτά που πρέπει να έχουν πρόσβαση;
 -
- Οι συνεργαζόμενες εταιρείες παρέχουν εγγυήσεις για τη συμμόρφωση με το ΓΚΠΔ;
 - Για την εν λόγω επεξεργασία, υπάρχει άδεια του υπευθύνου επεξεργασίας;
- Ο έλεγχος ως προς το αν τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των προσώπων πρέπει να είναι **συνεχής**





- **Αν η νομική βάση για την επεξεργασία προσωπικών δεδομένων είναι η συγκατάθεση**, ο υπεύθυνος επεξεργασίας πρέπει να μπορεί να αποδείξει ότι έχει λάβει τη συγκατάθεση των προσώπων
- Είναι η συγκατάθεση ελεύθερη;
- Είναι συγκεκριμένη και ρητή, **για σαφώς προσδιορισμένο σκοπό**;
- Έχει προέλθει με δήλωση / **με σαφή θετική ενέργεια**;
 - Π.χ. συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, επιλογή επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας της πληροφορίας
 - Η σιωπή, τα προ-συμπληρωμένα τετραγωνίδια ή η αδράνεια δεν πρέπει να εκλαμβάνονται ως συγκατάθεση.
- Για ανήλικους, εφόσον η επεξεργασία αφορά υπηρεσίας της κοινωνίας της πληροφορίας, η συγκατάθεση θεωρείται «έγκυρη» **όταν το παιδί είναι τουλάχιστον 16 ετών (*)**
 - Διαφορετικά, η συγκατάθεση πρέπει να δίνεται από το πρόσωπο που έχει τη γονική μέριμνα
 - Ο υπεύθυνος επεξεργασίας πρέπει να βρει την κατάλληλη μέθοδο



Αναθεώρηση πολιτικών προστασίας δεδομένων και διαδικασιών



- Η υποχρέωση ενημέρωσης «διευρύνεται»
 - Αλλαγή πολιτικής προστασίας δεδομένων και ενημερωτικών εντύπων
- Σε σχέση με το νυν νομικό πλαίσιο, προστίθεται – μεταξύ άλλων – η υποχρέωση ενημέρωσης για:
 - τη νομική βάση για την επεξεργασία (που «δυσκολεύει» την ενημέρωση, καθώς προϋποθέτει νομική ανάλυση)
 - το χρονικό διάστημα επεξεργασίας/αποθήκευσης.
 - Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της δημιουργίας προφίλ, με πληροφορίες σχετικά με τη λογική που ακολουθείται και ενδεχόμενες συνέπειες
- Υποχρέωση ενημέρωσης ακόμα και όταν τα δεδομένα συλλέγονται από άλλες πηγές
 - Με χρονικά όρια εντός των οποίων αυτή πρέπει να γίνει
- Τα στοιχεία του υπεύθυνου προστασίας δεδομένων – όταν υπάρχει - πρέπει επίσης να δημοσιοποιούνται
- Αλλαγή/επικαιροποίηση διαδικασιών για την ικανοποίηση των αιτημάτων των υποκειμένων των δεδομένων, λόγω (και) των νέων δικαιωμάτων (όταν αυτά έχουν εφαρμογή)
 - Δικαίωμα στη λήθη - Δικαίωμα στη φορητότητα

Ενισχυμένη αρχή της Διαφάνειας





- Υπάρχει υποχρέωση εκπόνησης εκτίμησης αντικτύπου ως προς την προστασία δεδομένων (DPIA);
 - Έλεγχος ως προς το αν το είδος της επεξεργασίας καθιστά υποχρεωτική την εκτίμηση αντικτύπου
 - Η Αρχή οφείλει να εκδώσει κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται υποχρεωτικά στην απαίτηση για DPIA
 - DPIA μπορεί να γίνει ακόμα και πριν τις 25/5/2018 - είναι μια ορθή πρακτική και μπορεί να αποκαλύψει «ατέλειες»
- Πρέπει να **γίνεται με συστηματικό τρόπο**, λαμβάνοντας υπόψη τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα
 - Ποιος θα **πραγματοποιήσει** την DPIA;
 - Ποιοι **εργαζόμενοι**/τμήματα πρέπει να εμπλακούν;
 - Ποιος θα **αξιολογήσει** τα αποτελέσματα της DPIA;
- DPIA και για το Δημόσιο Τομέα
- Σε κάθε περίπτωση, αν μετά την εφαρμογή των μέτρων παραμένει υψηλός κίνδυνος για την προστασία δεδομένων, προβλέπεται **διαβούλευση με την Αρχή**.



7

Υπεύθυνος Προστασίας Δεδομένων



- Υπάρχει υποχρέωση ορισμού Υπεύθυνου Προστασίας Δεδομένων (DPO);
 - Ακόμα και χωρίς ρητή υποχρέωση μπορεί να ορισθεί
- Τα στοιχεία του γνωστοποιούνται στην εποπτική Αρχή
- Ο ρόλος του είναι **συμβουλευτικός**, όχι αποφασιστικός.
 - Οι τελικές αποφάσεις λαμβάνονται από τη Διοίκηση.
 - Ωστόσο, ο DPO πρέπει να αξιοποιείται **ουσιαστικά** από τον φορέα
 - Πρέπει να διασφαλίζεται ότι συμμετέχει δεόντως και εγκαίρως σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία προσωπικών δεδομένων
- Δύο ή περισσότεροι φορείς μπορούν να έχουν κοινό DPO
 - Αλλά πρέπει να μπορεί εύκολα κάποιος να απευθυνθεί στο DPO για κάθε φορέα.



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr





- Η ασφαλής επεξεργασία των προσωπικών δεδομένων, με κατάλληλα τεχνικά και οργανωτικά μέτρα, παραμένει ζητούμενο.

- Γνωστοποίηση του περιστατικού στην ΑΠΔΠΧ
 - Με συγκεκριμένες πληροφορίες επ' αυτού
 - Οι προθεσμίες είναι «πιεστικές»
- Ενημέρωση των προσώπων που αφορά το περιστατικό, όταν αυτό ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες τους

- 

Παραβιάσεις δεδομένων

- Η ασφαλής επεξεργασία των προσωπικών δεδομένων, με κατάλληλα τεχνικά και οργανωτικά μέτρα, παραμένει ζητούμενο.
 - Εμπιστευτικότητα – Ακεραιότητα – Διαθεσιμότητα των προσωπικών δεδομένων
- **Αναθεώρηση διαδικασιών** ώστε:
 - Να γίνεται έγκαιρη ανίχνευση και αξιολόγηση ενός περιστατικού παραβίασης δεδομένων, ώστε να **καταγράφεται εσωτερικά τεκμηρίωση αυτού**
 - Πρέπει να είναι σαφές τι συνιστά περιστατικό παραβίασης δεδομένων
 - Ενδεχομένως είναι πιο «ευρύς» ο όρος από ό,τι αρχικώς νομίζουμε
 - Χωρίς καθυστέρηση ενημέρωση του υπεύθυνου επεξεργασίας για το περιστατικό
 - Συνδρομή στον υπεύθυνο επεξεργασίας
- Οι κίνδυνοι για παραβίαση δεδομένων, από τυχαία ή εσκεμμένα αιτία, είναι πάντα πολύ πιθανοί – **Στόχος θα πρέπει να είναι η μέγιστη δυνατή ελαχιστοποίηση των κινδύνων**
 - Σωστά εφαρμοζόμενες τεχνικές κρυπτογράφησης ή/και ανωνυμοποίησης/ψευδωνυμοποίησης
 - Μία ορθά εκπονηθείσα DPIA αναμένεται να συμβάλλει σε μεγάλο βαθμό στην ελαχιστοποίηση των κινδύνων



Δραστηριότητα σε περισσότερα Κράτη-Μέλη



- Εάν ο φορέας δραστηριοποιείται σε περισσότερα από ένα Κράτη-Μέλη, θα πρέπει να οριστεί το Κράτος της κύριας εγκατάστασης.
 - Η Αρχή αυτού του Κράτους-Μέλους είναι η επικεφαλής εποπτική Αρχή, με την οποία «συνομιλεί» ο φορέας
- Διερεύνηση:
 - Ποιος ο τόπος εγκατάστασης (έδρα);
 - Υπάρχουν άλλες εγκαταστάσεις εντός Ε.Ε.;
 - Ποιος ο τόπος που λαμβάνονται οι βασικές αποφάσεις για την επεξεργασία;
 - Είναι η έδρα;
 - Μήπως οι αποφάσεις λαμβάνονται και τίθενται σε εφαρμογή σε άλλη εγκατάσταση;
 - Υπάρχουν από κοινού υπεύθυνοι;



10

Διαβιβάσεις δεδομένων εκτός ΕΕ



- Θα πρέπει να συντρέχει κάποια εκ των προϋποθέσεων νόμιμης διαβίβασης (μηχανισμός διαβίβασης) – όπως ισχύει και τώρα
 - Δεσμευτικοί Εταιρικοί Κανόνες (BCRs)
 - Πρότυπες Συμβατικές Ρήτρες (SCCs)
 - Απόφαση επάρκειας
 - Προσχώρηση στην «ασπίδα ασφαλείας» (Privacy Shield) για τις Η.Π.Α.
 -
- Αξιολόγηση και επιλογή του κατάλληλου μηχανισμού διαβίβασης.
- «Διευρύνεται» η υποχρέωση ενημέρωσης στα πρόσωπα των οποίων τα δεδομένα διαβιβάζονται



Υλοποίηση των βημάτων

■ Επιχειρησιακά / Διαχειριστικά

■ Τεχνικά

- 1 Ενημέρωση - Ετοιμότητα
- 2 Καταγραφή επεξεργασιών
- 3 Έλεγχος συμμόρφωσης
- 4 Έλεγχος συγκατάθεσης
- 5 Αναθεώρηση πολιτικών
- 6 Εκτίμηση επιπτώσεων
- 7 Υπεύθυνος προστασίας δεδομένων
- 8 Παραβιάσεις δεδομένων
- 9 Δραστηριότητα σε πολλά ΚΜ
- 10 Διαβιβάσεις



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Συμπεράσματα

- Ο ΓΚΠΔ ενισχύει το θεμελιώδες δικαίωμα της προστασίας προσωπικών δεδομένων
- Ενσωματώνει την προστασία δεδομένων στις επιχειρησιακές διαδικασίες
 - «Μεταφέρει» το βάρος στους ίδιους φορείς στο να αυτο-συμμορφώνονται και να μπορούν να το αποδεικνύουν όποτε χρειαστεί
 - Καταργούνται «γραφειοκρατικές» διαδικασίες που δεν παρείχαν ουσιαστικό επίπεδο προστασίας
- Νέα δικαιώματα για τα φυσικά πρόσωπα
 - Νέες υποχρεώσεις για υπευθύνους και εκτελούντες
- Νέος ρόλος της Αρχής Προστασίας Προσωπικών Δεδομένων
- Η προστασία προσωπικών δεδομένων δεν θα πρέπει να εκλαμβάνεται ως «εμπόδιο» στις δράσεις των φορέων
 - Όλοι θα είναι ωφελημένοι από την ορθή προστασία του δικαιώματος αυτού
 - Ο ΓΚΠΔ πρέπει να εκληφθεί ως ένα πολύτιμο εργαλείο για όλους



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Ευχαριστούμε για την
προσοχή σας



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr