L&L LAW FIRM

Η αξιολόγηση ηλεκτρονικών εφαρμογών σε σχέση με την προστασία των προσωπικών δεδομένων από το σχεδιασμό και εξ ορισμού ως ανταγωνιστικό πλεονέκτημα των παρόχων προϊόντων πληροφορικής στην αγορά

ΜΑΪΟΣ 2024

Παρουσίαση στο πλαίσιο του 9ου Data Privacy & Protection Conference

ΓΡΗΓΟΡΗΣ ΛΑΖΑΡΑΚΟΣ, L & L Managing Partner

Στόχος εισήγησης

- Σημασία και τρόπος προσέγγισης αλλά και διαφορές μίας Μελέτης (PIA) που εκπονείται από **εκτελούντες την επεξεργασία**.
- Σημασία και τρόπος προσέγγισης αλλά και διαφορές μίας Μελέτης (PIA) που εκπονείται από **κατασκευαστές προϊόντων πληροφορικής (λ.χ. προγραμματιστές/developers)**

Εισαγωγικά για ΕΑΔΠ

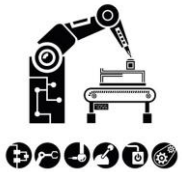
ΕΑΠΔ = «εργαλείο» λογοδοσίας του υπεύθυνου επεξεργασίας
ΕΑΠΔ = μέθοδος απόδειξης της συμμόρφωσης του υπεύθυνου επεξεργασίας

WP 248 αναθ. 01 κατευθυντήριες γραμμές ΕΣΠΔ: «Η ΕΑΠΔ αποτελεί σημαντικό εργαλείο για την πλήρωση της υποχρέωσης λογοδοσίας, καθώς παρέχει συνδρομή στους υπεύθυνους επεξεργασίας όχι μόνον προκειμένου να συμμορφώνονται με τις προδιαγραφές του ΓΚΠΔ, αλλά και για να αποδεικνύουν ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για τη διασφάλιση της συμμόρφωσης προς τον κανονισμό».

Χρηματικό πρόστιμο (έως 10 εκατ. ευρώ ή έως 2 % του τζίρου)

- Παράλειψη διενέργειας ΕΑΠΔ (άρθρο 35 παρ. 1-3)
- Διενέργεια ΕΑΠΔ με εσφαλμένο τρόπο (άρθρο 35 παρ 2 και 7-9)
- Μη διαβούλευση με ΑΠΔΠΧ [άρθρο 36 παρ. 3 στοιχείο ε)] μπορούν να επιφέρουν διοικητικό πρόστιμο ύψους, ανάλογα με το ποιο είναι υψηλότερο».
- Πρόσφατο παράδειγμα ΑΠΔΠΧ 13/2024 – Υπουργείο Μετανάστευσης

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA (1/2)



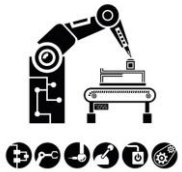
Ποιος οφείλει να διενεργεί DPIA; Υπεύθυνος επεξεργασίας

Εκτελών υλοποιεί -εν όλω ή εν μέρει- την επεξεργασία:

Άρθρο 28 παρ. 3 στοιχείο (στ) ΓΚΠΔ: Ο εκτελών θα πρέπει

- **να συνδράμει** τον υπεύθυνο επεξεργασίας στη διενέργεια της DPIA
- **να παρέχει** κάθε αναγκαία πληροφορία, λαμβανομένης υπόψη της φύσης της επεξεργασίας και των πληροφοριών που διαθέτει ο εκτελών την επεξεργασία.

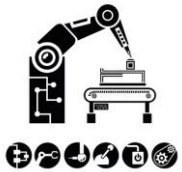
Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA (2/2)



Πάροχος/κατασκευαστής του προϊόντος (WP 248 ΟΕ 29):
Μπορεί να προσφέρει μεγάλη βοήθεια αν καταρτίσει τη δική του ΕΑΠΔ ενός τεχνολογικού προϊόντος σχετικά με την προστασία των δεδομένων, για παράδειγμα ενός λογισμικού, όταν αυτό ενδέχεται να χρησιμοποιηθεί από διαφορετικούς υπεύθυνους επεξεργασίας.

Ο υπεύθυνος επεξεργασίας που κάνει χρήση του προϊόντος παραμένει υποχρεωμένος να διενεργήσει τη δική του ΕΑΠΔ ως προς τη συγκεκριμένη εφαρμογή, ωστόσο, εάν ενδείκνυται, αυτή μπορεί να τεκμηριωθεί με χρήση της ΕΑΠΔ που έχει καταρτίσει ο πάροχος του προϊόντος.

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA



Παράδειγμα 1: Η σχέση μεταξύ κατασκευαστών ευφυών μετρητών και υπηρεσιών κοινής ωφελείας.

Παράδειγμα 2: Ηλεκτρονική εφαρμογή (πλατφόρμα) τηλεμετρίας, καταγραφής και διαχείρισης βιολογικών σημάτων και παραμέτρων υγείας και διασύνδεσης μεταξύ πολιτών με το νοσοκομείο, τον ιατρό ή άλλο επιστήμονα υγείας (π.χ. διατροφολόγο), καθώς και μεταξύ επαγγελματιών υγείας.

Υποχρεώσεις κατασκευαστών προϊόντων πληροφορικής (1/2)

Αιτιολογική σκέψη 78 ΓΚΠΔ: «Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, **οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των "τελευταίων εξελίξεων", να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων**».

Κατευθυντήριες Γραμμές 4/2019 ΕΣΠΔ: Παρότι δεν μνημονεύεται άμεσα στο άρθρο 25, […] **οι παραγωγοί αναγνωρίζονται επίσης ως βασικοί παράγοντες για την εφαρμογή της ΠΔΣΕΟ** και πρέπει να γνωρίζουν ότι οι υπεύθυνοι επεξεργασίας υποχρεούνται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μόνο με συστήματα και τεχνολογίες που διαθέτουν ενσωματωμένη προστασία δεδομένων.

Υποχρεώσεις κατασκευαστών προϊόντων πληροφορικής (2/2)

Κατευθυντήριες Γραμμές 4/2019 ΕΣΠΔ:

- «95. Κατά την [...] παροχή λύσεων σε υπευθύνους επεξεργασίας [...] οι παραγωγοί πρέπει να χρησιμοποιούν την τεχνογνωσία τους, **να εδραιώνουν σχέση εμπιστοσύνης με τους πελάτες τους, περιλαμβανομένων των ΜΜΕ, και να τους καθοδηγούν στον σχεδιασμό λύσεων που ενσωματώνουν την προστασία δεδομένων στη διαδικασία επεξεργασίας. Αυτό σημαίνει ότι ο σχεδιασμός των προϊόντων και υπηρεσιών πρέπει να διευκολύνει τις ανάγκες των υπευθύνων επεξεργασίας».**

- **Οι παραγωγοί και οι εκτελούντες την επεξεργασία πρέπει να επιδιώκουν τη διευκόλυνση της ΠΔΣΕΟ** προκειμένου να υποστηρίζουν την ικανότητα του υπεύθυνου επεξεργασίας να συμμορφώνεται προς τις απαιτήσεις του άρθρου 25. **Από την άλλη πλευρά, οι υπεύθυνοι επεξεργασίας δεν πρέπει να επιλέγουν παραγωγούς ή εκτελούντες την επεξεργασία που δεν προτείνουν συστήματα τα οποία επιτρέπουν στον υπεύθυνο επεξεργασίας ή τον υποστηρίζουν στο να συμμορφώνεται προς το άρθρο 25, διότι οι υπεύθυνοι επεξεργασίας θα λογοδοτούν σε περίπτωση μη εφαρμογής των διατάξεων του άρθρου».**

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA

Πως μπορεί ο κατασκευαστής προϊόντος να διευκολύνει τον υπεύθυνο επεξεργασίας κατά την εκπόνηση DPIA;

Καταγραφή σε χωριστό κείμενο των στοιχείων που σχετίζονται με την επεξεργασία προσωπικών δεδομένων (Product Privacy Impact Assessment/PPIA).

Σκοπός της PPIA είναι να ενημερώσει τον υπεύθυνο επεξεργασίας σε σχέση με πτυχές του προϊόντος που αφορούν σε προσωπικά δεδομένα και όχι να αποδείξει ότι το προϊόν βρίσκεται σε συμμόρφωση με τη νομοθεσία.

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA

Κατασκευαστής

❖ Δεν (οφείλει να) έχει επαρκείς γνώσεις και γι' αυτό δεν αξιολογεί ζητήματα (παράγοντες) που καθορίζει κυριαρχικά ο υπεύθυνος επεξεργασίας που αποκτά άδεια χρήσης της εφαρμογής, όπως λ.χ. η συγκεκριμένη παραμετροποίηση (τρόπος χρήσης) της εφαρμογής και ακολούθως, οι σκοποί που θα επιδιώξει μέσω αυτής, οι πολιτικές προστασίας δεδομένων που θα εφαρμόσει, το περιβάλλον που θα εγκαταστήσει την εφαρμογή, τα εξουσιοδοτημένα πρόσωπα που θα την διαχειρίζονται, τυχόν επιπλέον τεχνικά και οργανωτικά μέτρα που θα λάβει κ.ο.κ.

❖ Δεν πραγματοποιεί αξιολόγηση αναγκαιότητας και αναλογικότητας της επεξεργασίας [λ.χ. νομική βάση, τήρηση αρχής του σκοπού, της ελαχιστοποίησης, της ακρίβειας, της περιορισμένης αποθήκευσης].

❖Δεν αξιολογεί την επάρκεια των μέτρων που συμβάλλουν στη διαφύλαξη των δικαιωμάτων των ΥτΔ (πρόσβαση, φορητότητα, διόρθωση, διαγραφή, εναντίωση κλπ.).

❖Κατ' επέκταση δεν διενεργεί ΕΑΠΔ, κατ' άρθρο 35 ΓΚΠΔ.

Κριτήρια για μια αποδεκτή ΕΑΠΔ

(WP 248 ΟΕ άρθρου 29)

1) Συστηματική περιγραφή των πράξεων επεξεργασίας [άρθρο 35 παράγραφος 7 στοιχείο α)]

2) Εκτίμηση αναγκαιότητας και αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς
Προσδιορισμός μέτρων που συμβάλλουν στη διαφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων
[άρθρο 35 παράγραφος 7 στοιχείο β)]

3) Κίνδυνοι

- **Αξιολόγηση κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (απειλές, πηγές,, σοβαρότητα και πιθανότητα επέλευσης των κινδύνων, επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων)**
  [άρθρο 35 παράγραφος 7 στοιχείο γ)]

4) Μέτρα που συμβάλλουν στην αντιμετώπιση των κινδύνων
[άρθρο 35 παράγραφος 7 στοιχείο δ)]

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA

Κατασκευαστής πρϊόντος πληροφορικής **οφείλει** να μεταφέρει τη γνώση του για το προϊόν στον υπεύθυνο επεξεργασίας.

Η γνώση του περιορίζεται στο προϊόν και στις λειτουργίες του.

Καταλαμβάνει όμως και το ζήτημα των μέτρων που έχει λάβει για να προστατεύσει τα δεδομένα ήδη από το σχεδιασμό και εξ ορισμού (Privacy by design and default).

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και PPIA

Στην PPIA αποτυπώνεται ο τρόπος ενσωμάτωσης εκ μέρους του κατασκευαστή των αρχών Privacy by Design & Privacy by Default.

Περιγράφεται το προϊόν [π.χ. data flow overview, υποστηρικτικά στοιχεία της εφαρμογής]

Εντοπίζονται τυχόν αδυναμίες σε σχέση με την προστασία των προσωπικών δεδομένων, που μπορούν να οδηγήσουν σε συγκεκριμένους κινδύνους (π.χ. μη κρυπτογράφηση δεδομένων)

Αξιολογούνται οι πιθανοί κίνδυνοι ως προς τη σοβαρότητα και την πιθανότητα επέλευσής τους.

Εξηγούνται τα μέτρα που έχουν ληφθεί για να μειώσουν τους κινδύνους (από άποψη ασφάλειας και διευκόλυνσης της άσκησης των δικαιωμάτων από τα υποκείμενα)

Δίδονται συστάσεις στον υπεύθυνο επεξεργασίας σε σχέση με την αντιμετώπιση των κινδύνων.

Προστασία Δεδομένων από το Σχεδιασμό και εξ Ορισμού (privacy by design) (1/2)

Στο πλαίσιο της PPIA, ο κατασκευαστής θα πρέπει, μεταξύ άλλων να εξηγήσει:

- Πως έχουν ενσωματωθεί στην εφαρμογή τεχνικές ψευδωνυμοποίησης/κρυπτογράφησης ή τους λόγους για τους οποίους δεν μπορούν να εφαρμοστεί η ψευδωνυμοποίηση/κρυπτογράφηση των δεδομένων.

- Πως έχει ενσωματωθεί στην εφαρμογή η αρχή της ελαχιστοποίησης των δεδομένων (εξ ορισμού, υφίστανται επεξεργασία μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας) ή τους λόγους για τους οποίους δεν μπορεί να εφαρμοστεί η εν λόγω αρχή.

- Πως έχει ενσωματωθεί στην εφαρμογή η αρχή του περιορισμού της περιόδου αποθήκευσης ή τους λόγους για τους οποίους δεν μπορεί να εφαρμοστεί η εν λόγω αρχή (π.χ. αναφορά των προ-επιλεγμένων ρυθμίσεων σε σχέση με τους χρόνους τήρησης των δεδομένων και τη δυνατότητα αλλαγής/προσαρμογής των εν λόγω προεπιλεγμένων ρυθμίσεων).

- Λειτουργίες που επιτρέπουν στον Υπεύθυνο Επεξεργασίας να διαγράφει ή/και να ανωνυμοποιεί τα δεδομένα.

Προστασία Δεδομένων από το Σχεδιασμό και εξ Ορισμού(privacy by design) (2/2)

Στο πλαίσιο της PPIA, ο κατασκευαστής θα πρέπει, μεταξύ άλλων να εξηγήσει:

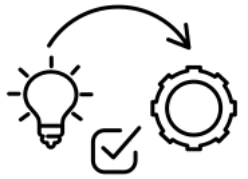
- Λειτουργίες που διασφαλίζουν ότι τα υποκείμενα των δεδομένων ασκούν ακώλυτα τα δικαιώματά τους σε σχέση με τα δεδομένα που τα αφορούν ή τα διευκολύνουν κατά την άσκηση των δικαιωμάτων τους.

- **Παράδειγμα:**
  - Δυνατότητα εξαγωγής φακέλων από το ίδιο το υποκείμενο των δεδομένων, ικανότητα αναζήτησης των προσωπικών δεδομένων που το αφορούν κλπ.
  - Δυνατότητα διαγραφής φακέλων/δεδομένων από το ίδιο το υποκείμενο των δεδομένων.

- Πως ελέγχεται η πρόσβαση ενός χρήστη στην εφαρμογή ή τους λόγους για τους οποίους δεν μπορεί να ελεγχθεί η πρόσβαση (π.χ. ύπαρξη προεπιλεγμένων χρηστών και κωδικών ασφαλείας).

- Ακεραιότητα/εμπιστευτικότητα: Χρήση των κατάλληλων τεχνικών και οργανωτικών μέτρων για την προστασία έναντι της άνευ εξουσιοδότησης και αθέμιτης επεξεργασίας, καθώς και έναντι της τυχαίας απώλειας, καταστροφής ή ζημίας.

Πρακτική εφαρμογή άρθρου 25 Γ.Κ.



Οι υπεύθυνοι επεξεργασίας δεν είναι σε πάντα σε θέση να ελέγχουν το σχεδιασμό των προϊόντων και υπηρεσιών (π.χ. λειτουργικά συστήματα, υλικό και λογισμικό).

- Αιτ. σκέψη (78) ΓΚ:
- Οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών πρέπει να ενθαρρύνονται να εφαρμόσουν την προστασία προσωπικών δεδομένων στο σχεδιασμό.
- Οι αρχές της προστασίας δεδομένων στο σχεδιασμό και εξ ορισμού να λαμβάνονται υπόψη στο πλαίσιο δημόσιων διαγωνισμών.
- Οι εξελίξεις της τεχνολογίας αλλάζουν διαρκώς: Πως μπορεί ο σχεδιασμός να παραμείνει φιλικός προς την ιδιωτικότητα;
- Αναβαθμίσεις υλικού και λογισμικού! Υποχρέωση παρόχου προϊόντος πληροφορικής, που θα πρέπει να προβλέπεται στη σύμβαση.

Σημασία ορθής εκτέλεσης PPIA (Product Privacy Impact Assessment)

Θα βοηθήσει τις επιχειρήσεις και τους οργανισμούς:

- να εντοπίσουν τις αδυναμίες των συστημάτων τους, με τη βοήθεια των οποίων επεξεργάζονται προσωπικά δεδομένα.
- να αποτρέψουν πιθανές παραβιάσεις της οικείας νομοθεσίας και, ακολούθως, να υποστούν τις αυστηρές –οικονομικής κυρίως φύσεως- κυρώσεις, που προβλέπει ο Κανονισμός σε περίπτωση παραβίασης των διατάξεών του.
- να προστατέψουν την αξιοπιστία τους και την εμπορική τους φήμη.
- να προχωρήσουν σε μεταγενέστερο στάδιο σε πιστοποίηση των επεξεργασιών βάσει του ΓΚΠΔ.
- Θα αποβεί εις όφελος των φυσικών προσώπων, τα προσωπικά δεδομένα των οποίων θα πρέπει ούτως ή άλλως, να αποτελούν αντικείμενο νόμιμης και θεμιτής επεξεργασίας

L&L

LAW FIRM

ΣΑΣ ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ

grigorios@lazarakos.gr

ΓΡΗΓΟΡΗΣ ΛΑΖΑΡΑΚΟΣ, L & L Managing Partner