Πρακτικά ζητήματα και προκλήσεις κατά την εκπόνηση μελέτης εκτίμησης αντικτύπου στην προστασία δεδομένων

Γρηγόρης Λαζαράκος

Αναπληρωτής Καθηγητής Συνταγματικού Δικαίου στη Στρατιωτική Σχολή Ευελπίδων

πρώην αν. μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Πιστοποιημένος νομικός εμπειρογνώμονας για την προστασία δεδομένων (CEPE L PS) σε ηλεκτρονικά προϊόντα και υπηρεσίες (IT based products and services) στο γερμανικό φορέα πιστοποίησης European Privacy Seal GmbH (EuroPriSe)

Παρουσίαση στην Επιστημονική εκδήλωση, που διοργανώνει το **Επιστημονικό Συμβούλιο της Κοινωνίας της Πληροφορίας** σε συνεργασία με την **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**
με θέμα:
«Γενικός Κανονισμός Προστασίας Δεδομένων: Ειδικά θέματα συμμόρφωσης»

Στόχος εισήγησης

- Παρουσίαση ζητημάτων που αναφύονται στην πράξη και αφορούν κυρίως στα **κριτήρια για να είναι αποδεκτή** μία DPIA.
- 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 **τρίτους (λ.χ. προγραμματιστές/developers)**
- Χρήση παραδειγμάτων από την πράξη.

Πότε μία επεξεργασία είναι υψηλού κινδύνου (οπότε απαιτείται DPIA);

Σε περίπτωση:

Συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών που βασίζεται σε αυτοματοποιημένη επεξεργασία (κατάρτιση προφίλ) και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα ή επηρεάζουν σημαντικά το φυσικό πρόσωπο

ή

Μεγάλης κλίμακας επεξεργασίας των ευαίσθητων δεδομένων του άρθρου 9 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10

ή

Συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

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)]

Αναλυτική περιγραφή πράξεων επεξεργασίας (1/6)

Αναγνωρίζουμε τις πράξεις επεξεργασίες που αποτελούν αντικείμενο της DPIA

- ✓ Ποια είναι η υπό εξέταση επεξεργασία;
- ✓ Ποια είναι τα εμπλεκόμενα μέρη (εκτελών/από κοινού υπεύθυνος, αποδέκτες);
- ✓ Υπάρχει εγκεκριμένος Κώδικας Δεοντολογίας;

Καταγραφή προσωπικών δεδομένων και υποκειμένων των δεδομένων

- ✓ Διάκριση μεταξύ απλών και ευαίσθητων
- ✓ Προσοχή στα δεδομένα που δεν αναγνωρίζονται εύκολα, όπως π.χ. usage data, payment data, log files, data for authorization)

Κύκλος ζωής των δεδομένων (data flow)

- ✓ Πηγή συλλογής, τυχόν αποδέκτες,
- ✓ περίοδος αποθήκευσης των δεδομένων

➢ **Προσδιορισμός στοιχείων του ενεργητικού, στα οποία εναποτίθενται τα δεδομένα (hardware, software, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων)**

Αναλυτική περιγραφή πράξεων επεξεργασίας (2/6)

<u>Παράδειγμα 1:</u>
DPIA του Ολλανδικού Υπουργείου Δικαιοσύνης: Επεξεργασία προσωπικών δεδομένων κατά τη χρήση του Microsoft Office από τους υπαλλήλους των δημοσίων υπηρεσιών της Χώρας (περίπου 300.000)
✓Περιγραφή επεξεργασίες: Σε 61 από τις 91 σελίδες γίνεται ανάλυση σημαντικών παραμέτρων της επεξεργασίας:

1) Τι εμπίπτει στο αντικείμενο επεξεργασίας;

'Διαγνωστικά δεδομένα', δηλαδή όλες οι πληροφορίες που αποθηκεύονται στα αρχεία καταγραφής συμβάντων σχετικά με τη συμπεριφορά των χρηστών των 4 εφαρμογών Word, Excel, Powerpoint, Outlook (συμπεριλαμβανομένου Calendar)

2) Τι <u>δεν</u> εμπίπτει στο αντικείμενο της DPIA ;

- ✓ Η επεξεργασία λειτουργικών δεδομένων και δεδομένων περιεχομένου

Αναλυτική περιγραφή (3/6)
Καταγραφή προσωπικών δεδομένων

Διαγνωστικά δεδομένα (παράδειγμα από audit data):

- CreationTime":"2018-06-04T14:11:30",
- "Id":"2d406d82-c282-4be7-a82c-08d5ca2511c8",
- "Operation":"FileAccessed",
- "OrganizationId":"b61b13fc-e936-4ada-b443 f663048afd59",
- "RecordType":6,
- "UserKey":"i:0h.f|membership| [xxxxxxxxxxxxxxx]@live.com",
- "Workload":"OneDrive",
- "ClientIP":"XX.XXX.XXX.XXX",
- "ObjectId":"https:\/\/[HOSTNAME]-my.sharepoint.com\/personal\/[NAME]_[HOSTNAME_nl\/Documents\/Gedeeld met iedereen\/Event 20180607\/PPT 06 Advies SLM.pptx",
- "UserId":"[NAME]@[HOSTNAME].nl ",
- "CorrelationId":"05d56d9e-a035-5000-b848-4c14733cf7ff",
- "EventSource":"SharePoint",
- "ItemType":"File",
- ……..

Τα audit logs παρέχουν πληροφορίες ως προς το

- **Πότε** (creation time) και **ποιος** (E-mail address, name, IP-address) είχε πρόσβαση σε ένα έγγραφο, συμπεριλαμβανομένων των **γραμμών θέματος ηλεκτρονικού ταχυδρομείου** (subject line of a message).
- **Δραστηριότητα χρήστη** (π.χ. άνοιγμα αρχείου/e-mail activity) : (copy, create, softdelete and harddelete, message previewed or opened, moved to delete folder and Updateinboxrules).
- **Classified information**
- **Ειδικές κατηγορίες προσωπικών δεδομένων** (κατ' εξαίρεση)

Αναλυτική περιγραφή (4/6) πράξεων επεξεργασίας – Ρόλος εμπλεκόμενων μερών (Ολλανδική DPIA)

Microsoft:
Εκτελών την επεξεργασία

DPIA:
Ολλανδικό Δημόσιο και Microsoft **από κοινού υπεύθυνοι επεξεργασίας.**

Αιτιολογία: Microsoft ορίζει τους σκοπούς της επεξεργασίας (π.χ. ασφάλεια, επικαιροποίηση λογισμικού, διάγνωση δυσειτουργιών, ανάπτυξη λογισμικού με προσθήκη νέων υπηρεσιών).;

- Η Κυβέρνηση επιτρέπει στη Microsoft να επεξεργάζεται δεδομένα για αυτούς τους σκοπούς.
- Η Κυβέρνηση δεν δίνει τη δυνατότητα στο χρήστη/υπάλληλο να χρησιμοποιήσει άλλο λογισμικό.
- Κυβέρνηση και Microsoft έχουν την ιδιότητα του από κοινού υπεύθυνου επεξεργασίας.

Δημιουργεί αλυσιδωτές επιπτώσεις στην DPIA:
Σύναψη σύμβασης μεταξύ από κοινού υπεύθυνων σύμφωνα με τις διατάξεις του άρθρου 26 ΓΚΠΔ, στην οποία θα καθορίζονται με διαφανή τρόπο οι αντίστοιχες ευθύνες τους για συμμόρφωση προς τις υποχρεώσεις που απορρέουν από τον ΓΚΠΔ, ιδίως όσον αφορά την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων και τα αντίστοιχα καθήκοντά τους για να παρέχουν τις πληροφορίες που αναφέρονται στα άρθρα 13 και 14 ΓΚΠΔ.

Αναλυτική περιγραφή πράξεων επεξεργασίας- (5/6) Διάκριση μεταξύ απλών και ευαίσθητων

Παράδειγμα 2: Τεστ αξιολόγησης υποψηφίου (ψυχομετρικά τεστ)

Πληροφορίες:
Όνομα και επώνυμο, διεύθυνση ηλεκτρονικού ταχυδρομείου, ημερομηνία γέννησης, χώρα καταγωγής, εκπαίδευση, ιστορικό απασχόλησης

Τεχνικές πληροφορίες:
Διεύθυνση IP, ημερομηνία και ώρα σύνδεσης, στοιχεία ταυτότητας σύνδεσης, ρυθμίσεις προγράμματος περιήγησης, δραστηριότητα περιήγησης

Στο τεστ αξιολογούνται:

- **δεξιότητες των υποψηφίων** (γλωσσικός και/ή αριθμητικός συλλογισμός, επαγωγικός συλλογισμός, διαχείριση πληροφοριών, αγγλική γλώσσα)
- **στοιχεία της προσωπικότητάς τους**, που σχετίζονται με την επαγγελματική συμπεριφορά (προσωπικότητα, προσωπικότητα υπό συνθήκες πίεσης, αξίες και κίνητρα).

Συνήθως απλά. Αναλόγως όμως της εμβάθυνσης στην ψυχοσύνθεση του υποψηφίου, μπορεί να θεωρηθούν ευαίσθητα (π.χ. τεστ για πιλότους ή προσωπικό που φέρει οπλισμό).

Νομική Βάση: Έννομο συμφέρον (άρθρο 6.1.στ)

Αναλυτική περιγραφή (6/6) (dataflow)

Παράδειγμα:
Προϊόν πληροφορικής (IT-Product): επεξεργασία δεδομένων μέσω κινητής εφαρμογής (mobile app) που χρησιμοποιείται σε πρόγραμμα παροχής βοήθειας στο σπίτι (*περιλαμβάνεται και διαβίβαση δεδομένων σε ασφαλιστικές εταιρείες με σκοπό την ασφαλιστική κάλυψη της υπηρεσίας και, ακολούθως, την τιμολόγηση των υπηρεσιών*)

- **Υπεύθυνος επεξεργασίας:** Εταιρεία παροχής υπηρεσιών περίθαλψης
- **Αντικείμενο DPIA:** Επεξεργασία δεδομένων μέσω της εφαρμογής
- **Περιβάλλον επεξεργασίας:** π.χ. PDA hardware, DB στο διακομιστή (server), δίκτυο, firewall.
- **Προσωπικά Δεδομένα:**
  1) Δεδομένα υγείας ασθενούς,, ιατρικές νοσηλευτικές πράξεις,
  2) Δεδομένα νοσοκόμας (χρόνος παραμονής της στο σπίτι), log files.

Αναγκαιότητα και αναλογικότητα [άρθρο 35 παράγραφος 7 στοιχείο β)]

Ενδεικτικές ερωτήσεις

- ✓ Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;
- ✓ Τηρείται η αρχή της ελαχιστοποίησης των δεδομένων;
- ✓ Ποια είναι η νομική βάση που καθιστά την επεξεργασία νόμιμη;
- ✓ Τα προσωπικά δεδομένα που συλλέγονται είναι επαρκή, συναφή και περιορίζονται σε όσα είναι απαραίτητα σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία;
- ✓ Είναι τα δεδομένα ακριβή και ενημερωμένα;
- ✓ Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;

Μέτρα που συμβάλλουν στη διαφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων

Ενδεικτικά:

- ✓ Πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρθρα 12, 13 και 14)
- ✓ Δικαίωμα πρόσβασης και δικαίωμα στη φορητότητα των δεδομένων (άρθρα 15 και 20)
- ✓ Δικαίωμα διόρθωσης και διαγραφής (άρθρα 16, 17 και 19)
- ✓ Δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρθρα 18, 19 και 21)
- ✓ Σχέσεις με τους εκτελούντες την επεξεργασία (άρθρο 28)
- ✓ Εγγυήσεις για διεθνείς διαβιβάσεις (Κεφάλαιο V)
- ✓ Προηγούμενη διαβούλευση (άρθρο 36).

Εκτίμηση κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων και Μέτρα αντιμετώπισης

- Αναλύονται:
  - πηγές κινδύνου (π.χ. εργαζόμενος, αποδέκτες δεδομένων, hackers, φυσικοί παράγοντες / φωτιά, πλημμύρα κ.ά.)
  - Αδυναμίες στα μέτρα ασφάλειας
  - Κίνδυνοι που αφορούν στην ιδιωτική ζωή
    1. Αθέμιτη πρόσβαση σε προσωπικά δεδομένα (εμπιστευτικότητα)
    2. Ανεπιθύμητη τροποποίηση των προσωπικών δεδομένων (ακεραιότητα)
    3. Μη διάθεση των προσωπικών δεδομένων (διαθεσιμότητα)
- Επιπτώσεις στα υποκείμενα (σε περίπτωση επέλευσης), π.χ. αίσθημα παραβίασης ιδιωτικότητας, προσωπικά ή επαγγελματικά προβλήματα.
- Εκτίμηση επιπτώσεων
- Πιθανότητες επέλευσης

Εκτίμηση κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων και Μέτρα αντιμετώπισης

Βαθμός αντικτύπου

1. **Αμελητέος**
Τα υποκείμενα των δεδομένων δεν θα επηρεαστούν καθόλου ή μπορεί να αντιμετωπίσουν κάποια μειονεκτήματα, τα οποία θα ξεπεράσουν χωρίς κανένα πρόβλημα

2. **Περιορισμένος**-
Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν κάποια ζητήματα, τα οποία θα καταφέρουν να ξεπεράσουν με ορισμένες δυσκολίες, π.χ. μικρό κόστος, άρνηση σύναψης σύμβαση

3. **Σημαντικός** -
σοβαρές συνέπειες που αντιμετωπίζονται με μεγάλες δυσκολίες όπως πρόκληση ζημιάς - (παραβίαση τραπεζικού απορρήτου μπορεί να επηρεάσει την εικόνα του ατόμου, πχ. αν γίνουν γνωστά ετήσια έσοδα ή κοινωνικά επιδόματα, μπορεί το υποκείμενο να πέσει θύμα εκβιασμού)

4. **Πολύ σημαντικός** -
Τα υποκείμενα των δεδομένων ενδέχεται να έχουν σημαντικές ή ακόμα και ανεπανόρθωτες επιπτώσεις, όπως πρόκληση ασθένειας - (η αποκάλυψη ή αλλαγή ή απώλεια της πληροφορίας που αφορά στην υγεία του υποκειμένου μπορεί να θέσει σε κίνδυνο τη ίδια τη ζωή του ατόμου)

Εκτίμηση της πιθανότητας επέλευσης των απειλών που σχετίζονται με κάθε κίνδυνο

1. **Αμελητέα** - π.χ. κλοπή εγγράφων που φυλάσσονται σε χώρο ελεγχόμενης πρόσβασης , με κάρτα, κωδικό πρόσβασης και κάμερα ασφαλείας.

2. **Περιορισμένη** - π.χ. κλοπή εγγράφων σε χώρο ελεγχόμενης πρόσβασης μόνο από κάρτα.

3. **Σημαντική** - κλοπή εγγράφων από γραφεία, στα οποία επιτρέπεται η πρόσβαση μόνον μετά από έλεγχο, που **γίνεται** στην υποδοχή του κτηρίου

4. **Πολύ σημαντική** - κλοπή εγγράφων που βρίσκονται στο χώρο αναμονής ενός γραφείου/κτηρίου.

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA (1/4)

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

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

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA (2/4)

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 (Privacy Impact Assessment/PIA).

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA (3/4)

Σκοπός του PIA 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.

Κατασκευαστής

Οφείλει να μεταφέρει τη γνώση του για το προϊόν στον υπεύθυνο επεξεργασίας. Η γνώση του περιορίζεται στο προϊόν και στις λειτουργίες του.

Δεν οφείλει να συντάσσει κείμενα ενημερώσεων, συγκαταθέσεων ή ακόμη και DPIA.

❖Δεν (οφείλει να) έχει επαρκείς γνώσεις π.χ. ως προς άλλους σκοπούς που ο υπεύθυνος επεξεργασίας μπορεί να έχει, τις πολιτικές που ο υπεύθυνος επεξεργασίας μπορεί να εφαρμόσει (π.χ. ως προς τις πληροφορίες των προσώπων που αφορούν στα δεδομένα, την περίοδο αποθήκευσης κλπ), το περιβάλλον που θα εγκαταστήσει το λογισμικό.

Εκτελούντες την επεξεργασία/Κατασκευαστές προϊόντων πληροφορικής και DPIA (4/4)

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

- Περιγρά-φεται το προϊόν
- 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.

Σημασία ορθής εκτέλεσης DPIA ή PIA

Συμμόρφωση επιχειρήσεων και οργανισμών με τον ΓΚΠΔ

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

Σας ευχαριστώ πολύ!

Γρηγόρης Λαζαράκος

grigorios@lazarakos.gr

EuroPriSe European Privacy Seal LEGAL EXPERT Product/Service Certification