ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ
www.mli.uom.gr

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ
ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
& ΙΔΙΩΤΙΚΟΤΗΤΑΣ

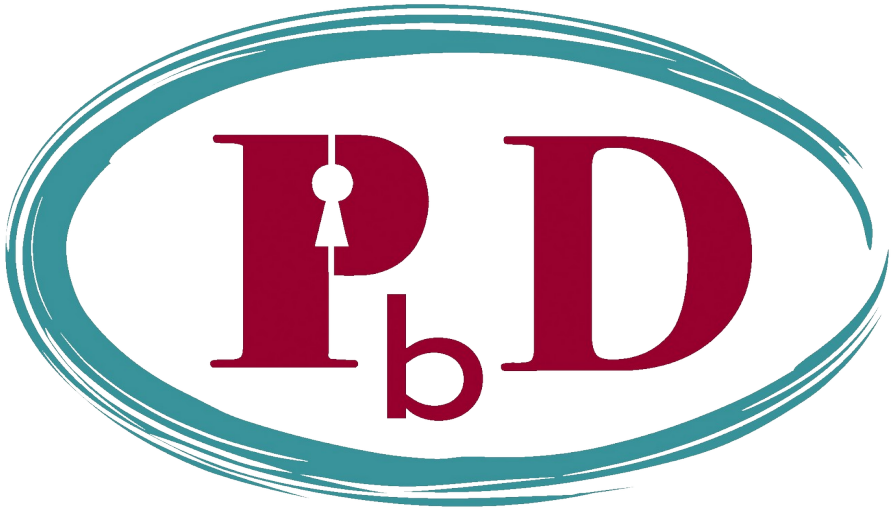
Privacy by Design: Αρχές και Εφαρμογή

© Δημήτρης Τζέλλης

version 20191205

Οι έννοιες που συνθέτουν το **Privacy by Design** (Προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό) υπήρχαν ήδη από την δεκαετία του 1970. Κομβική σημασία στην **ανάπτυξη και συστηματοποίηση** του PbD είχε η κυρία **Ann Cavoukian**, Επίτροπος Πληροφοριών και Ιδιωτικότητας του Οντάριο, στον Καναδά, για τρεις θητείες (Information and Privacy Commissioner of Ontario, Canada). Από τη δεκαετία το 1990 και έπειτα, σε συνεργασία με την Ολλανδική Αρχή Προστασίας Δεδομένων, ανέπτυξε τις αρχές του Privacy by Design σε ένα πλαίσιο που δημοσιεύθηκε το 2009 και υιοθετήθηκε το 2010 από το Διεθνές Συνέδριο Επιτρόπων Προστασίας Προσωπικών Δεδομένων και Απορρήτου ομόφωνα.

Dr. Ann Cavoukian, Εμπνεύστρια του Privacy by Design



Το **Privacy by Design** (PbD) είναι ένα σύνολο μεθόδων για την προληπτική ενσωμάτωση της προστασίας των δεδομένων στην τεχνολογία πληροφοριών, στις εταιρικές πρακτικές, στην αρχιτεκτονική των χώρων και στις δικτυακές υποδομές. Τα μέτρα του PbD είναι σχεδιασμένα ώστε να προβλέπουν και να αποτρέπουν τα παρεμβατικά γεγονότα πριν αυτά συμβούν.

Οι 7 θεμελιώδεις Αρχές του Privacy by Design

1. **Πρόληψη**, όχι Αντίδραση:
   Αποτροπή, όχι Επανόρθωση·
2. Προστασία των δεδομένων ως **Προεπιλεγμένη Ρύθμιση·**
3. Προστασία των δεδομένων **Ενσωματωμένη** στον σχεδιασμό·
4. **Πλήρης** Λειτουργικότητα:
   Θετικό Άθροισμα, όχι Μηδενικό Άθροισμα·
5. Καθολική **Ασφάλεια**:
   Προστασία **Καθ' όλη τη διάρκεια** του κύκλου ζωής·
6. Ορατότητα **και** Διαφάνεια:
   Διατήρηση **Ανοιχτής Προσέγγισης·**
7. Σεβασμός προς την Ιδιωτικότητα των Χρηστών:
   Διατήρηση του **Χρήστη στο Επίκεντρο**

1. **Πρόληψη**, όχι Αντίδραση: Αποτροπή, όχι Επανόρθωση·

Το PbD **περιλαμβάνει την πρόβλεψη γεγονότων** που επηρεάζουν την ιδιωτικότητα πριν αυτά πραγματοποιηθούν.

Κάθε σύστημα, διαδικασία ή υποδομή που χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα πρέπει, **ήδη από τη σύλληψή του και από τον αρχικό του σχεδιασμό**, να λαμβάνει υπόψη πιθανούς κινδύνους για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Οι κίνδυνοι αυτοί πρέπει να ελαχιστοποιούνται **πριν προκληθούν πραγματικές ζημίες**. Το PbD χαρακτηρίζεται από την **υιοθέτηση προληπτικών μέτρων** που προλαμβάνουν τις απειλές, εντοπίζουν αδυναμίες των συστημάτων για εξουδετέρωση ή ελαχιστοποίηση των κινδύνων, νωρίς και με τρόπο συνεπή, αντί να εφαρμόζονται διορθωτικά μέτρα για την επίλυση των συμβάντων ασφαλείας μετά την επέλευσή τους.

1. **Πρόληψη**, όχι Αντίδραση:
Αποτροπή, όχι Επανόρθωση·

Αυτό περιλαμβάνει:

Σαφή δέσμευση του οργανισμού, που πρέπει να προωθηθεί από τα υψηλότερα επίπεδα της Διοίκησης.

Ανάπτυξη νοοτροπίας δέσμευσης και συνεχούς βελτίωσης από όλους τους εργαζομένους, καθώς η πολιτική δεν σημαίνει τίποτε παρά μόνο αν μεταφραστεί σε συγκεκριμένες πρακτικές που τροφοδοτούνται από αποτελέσματα.

Καθορισμό και **ανάθεση συγκεκριμένων αρμοδιοτήτων** έτσι ώστε κάθε μέλος του οργανισμού να γνωρίζει σαφώς τα καθήκοντά του **όσον αφορά στην προστασία της ιδιωτικής ζωής**.

Ανάπτυξη συστηματικών μεθόδων, βασισμένων σε δείκτες, **ώστε να εντοπίζονται έγκαιρα οι διαδικασίες** και οι πρακτικές **που είναι ανεπαρκείς για την προστασία της ιδιωτικής ζωής**.

2. Προστασία των δεδομένων ως **Προεπιλεγμένη Ρύθμιση·**

Το PbD επιδιώκει να **παρέχει στον χρήστη το μέγιστο επίπεδο προστασίας** των προσωπικών του δεδομένων, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, και κυρίως το **να προστατεύονται τα προσωπικά δεδομένα με τρόπο αυτόματο** σε κάθε σύστημα, εφαρμογή, προϊόν ή υπηρεσία.

Η προεπιλεγμένη ρύθμιση πρέπει να καθορίζεται ήδη από τον σχεδιασμό στο επίπεδο που παρέχει τη μέγιστη προστασία των προσωπικών δεδομένων. **Δεν απαιτείται καμία ενέργεια εκ μέρους του ατόμου για την προστασία της ιδιωτικότητάς του**. Η προστασία της ιδιωτικότητάς του **είναι ενσωματωμένη στο σύστημα από προεπιλογή.**

Στην πράξη, η αρχή αυτή στηρίζεται στην ελαχιστοποίηση των δεδομένων κατά τα στάδια της επεξεργασίας, κυρίως τη συλλογή, τη χρήση, την αποθήκευση και τη διαβίβαση.

2. Προστασία των δεδομένων ως **Προεπιλεγμένη Ρύθμιση**·

Για αυτόν τον σκοπό είναι απαραίτητο:

Να προσδιοριστεί ο σκοπός της επεξεργασίας και να ενημερωθεί το άτομο (υποκείμενο των δεδομένων) για αυτόν κατά τον χρόνο της συλλογής ή πριν τη συλλογή. Οι προσδιορισμένοι σκοποί πρέπει να είναι σαφείς, περιορισμένοι και συναφείς προς τις περιστάσεις.

Να οριστούν τα κριτήρια της συλλογής δεδομένων ώστε η συλλογή να είναι περιορισμένη σε αυτό που είναι απαραίτητο για τους προσδιορισμένους σκοπούς επεξεργασίας, να είναι δίκαιη και νόμιμη. Ο σχεδιασμός των τεχνολογιών και συστημάτων εφαρμογών, πληροφοριών και επικοινωνιών πρέπει να ξεκινά με αλληλεπιδράσεις και συναλλαγές που κατ’ αρχήν δεν περιλαμβάνουν αναγνωριστικά στοιχεία.

Να περιοριστεί η χρήση των προσωπικών δεδομένων στους σκοπούς για τους οποίους αυτά συλλέχθηκαν και να επαληθευτεί ότι υπάρχει νομική βάση επεξεργασίας.

2. Προστασία των δεδομένων ως **Προεπιλεγμένη Ρύθμιση**·

Για αυτόν τον σκοπό είναι απαραίτητο:

Να περιοριστεί η πρόσβαση στα προσωπικά δεδομένα μόνο στα μέρη που συμμετέχουν στην επεξεργασία με βάση την αρχή της “ανάγκης για γνώση” και σύμφωνα με τους κανόνες που χρησιμοποιούνται για τη διαμόρφωση προφίλ πρόσβασης στα δεδομένα.

Να προσδιοριστούν αυστηρά όρια για τη διάρκεια αποθήκευσης και να καθιερωθούν λειτουργικοί μηχανισμοί που εγγυούνται τη συμμόρφωση.

Να δημιουργηθούν τεχνικά και διαδικαστικά εμπόδια στη μη εξουσιοδοτημένη σύνδεση ανεξάρτητων πηγών δεδομένων.

Όταν η ανάγκη ή ο τρόπος χρήσης προσωπικών πληροφοριών δεν είναι σαφής, πρέπει να υπάρχει τεκμήριο ιδιωτικότητας και να εφαρμόζεται η αρχή της προφύλαξης: οι προεπιλεγμένες ρυθμίσεις πρέπει να είναι οι πλέον προστατευτικές για την προστασία της ιδιωτικής ζωής.

3. Προστασία των δεδομένων **Ενσωματωμένη** στον σχεδιασμό·

Το PbD πρέπει να είναι αναπόσπαστο και εγγενές τμήμα των συστημάτων, των εφαρμογών, των προϊόντων και των υπηρεσιών, καθώς επίσης και των επιχειρηματικών πρακτικών και των διαδικασιών ενός οργανισμού. Δεν είναι ένα επιπλέον πρόσθετο σχήμα, το οποίο προσαρτάται σε μια προϋφιστάμενη οντότητα, αλλά πρέπει να ενσωματώνεται στο σύνολο των προϋποθέσεων λειτουργίας, ήδη από το στάδιο της σύλληψης και του σχεδιασμού. Η προστασία της ιδιωτικότητας είναι **ενσωματωμένη στο σύστημα, χωρίς να μειώνεται η λειτουργικότητα.**

3. Προστασία των δεδομένων **Ενσωματωμένη** στον σχεδιασμό·

Η προστασία της ιδιωτικότητας πρέπει να ενσωματωθεί στην αρχιτεκτονική των τεχνολογιών, των λειτουργιών και της πληροφορικής με τρόπο ολιστικό, ενοποιητικό και δημιουργικό.

Ολιστικό καθώς πρέπει να λαμβάνονται πάντα υπόψη και άλλες, ευρύτερες περιστάσεις.

Ενοποιητικό επειδή πρέπει να υπάρχει διαβούλευση με όλα τα ενδιαφερόμενα μέρη ώστε να εκφραστούν για τα συμφέροντα και τα δικαιώματά τους.

Δημιουργικό καθότι ορισμένες φορές η ενσωμάτωση της προστασίας της ιδιωτικότητας σημαίνει την επανεφεύρεση υφιστάμενων επιλογών, για τον λόγο ότι οι εναλλακτικές λύσεις είναι απαράδεκτες.

Θα πρέπει να υιοθετηθεί μια συστημική, συνεπής στις αρχές προσέγγιση που θα βασίζεται σε αποδεκτά πρότυπα και πλαίσια, τα οποία υπόκεινται σε εξωτερικές αναθεωρήσεις και ελέγχους.

3. Προστασία των δεδομένων **Ενσωματωμένη** στον σχεδιασμό·

Για να εγγυηθούμε ότι η προστασία της ιδιωτικότητας είναι μέρος του αρχικού σταδίου του σχεδιασμού **θα πρέπει:**

Να θεωρείται η προστασία της ιδιωτικότητας ως ουσιώδης απαίτηση εντός του πλαισίου του κύκλου ζωής των συστημάτων και των υπηρεσιών, καθώς και στον σχεδιασμό των οργανωτικών διαδικασιών.

Να διεξάγονται και να δημοσιεύονται **λεπτομερείς αξιολογήσεις των επιπτώσεων και των κινδύνων** για την ιδιωτική ζωή, με σαφή τεκμηρίωση των κινδύνων για την προστασία της ιδιωτικής ζωής και όλων των μέτρων που ελήφθησαν για τον περιορισμό αυτών των κινδύνων, συμπεριλαμβανομένης της ανάλυσης εναλλακτικών λύσεων και της επιλογής μετρήσεων. Κατά περίπτωση, να διεξάγεται **Εκτίμηση Αντικτύπου**, ως αναπόσπαστο μέρος κάθε νέας πρωτοβουλίας επεξεργασίας.

3. Προστασία των δεδομένων **Ενσωματωμένη** στον σχεδιασμό·

Για να εγγυηθούμε ότι η προστασία της ιδιωτικότητας είναι μέρος του αρχικού σταδίου του σχεδιασμού θα πρέπει:

Να τεκμηριώνονται όλες οι αποφάσεις που υιοθετεί ο οργανισμός από την προοπτική του “σχεδιασμού της προστασίας της ιδιωτικότητας”.

4. **Πλήρης** Λειτουργικότητα: Θετικό Άθροισμα, όχι Μηδενικό Άθροισμα·

Το 1755 ο Βενιαμίν Φραγκλίνος φέρεται να έχει γράψει τη φράση “Εκείνοι που θα παραιτηθούν από κάποια απαραίτητη Ελευθερία, για να αγοράσουν μια μικρή πρόσκαιρη Ασφάλεια, δεν δικαιούνται ούτε Ελευθερία ούτε Ασφάλεια”.

Παραδοσιακά έχει θεωρηθεί ότι η προστασία της ιδιωτικότητας αποκτάται σε βάρος άλλων δυνατοτήτων, δημιουργώντας διχοτομίες όπως ιδιωτικότητα σε αντιδιαστολή προς την ευχρηστία, τη λειτουργικότητα, το επιχειρηματικό κέρδος, ακόμα και ιδιωτικότητα εναντίον ασφάλειας.

Αυτή είναι μια **μεθοδευμένη προσέγγιση**, και το PbD επιδιώκει να ικανοποιήσει όλα τα νόμιμα συμφέροντα και στόχους με τρόπο που δημιουργεί θετικά αποτελέσματα για όλα τα μέρη, χωρίς την παρωχημένη προσέγγιση μηδενικού αθροίσματος, όπου γίνονται **άσκοπες αντισταθμίσεις**.

4. **Πλήρης** Λειτουργικότητα: Θετικό Άθροισμα, όχι Μηδενικό Άθροισμα·

Το PbD δεν συνεπάγεται απλώς τη διατύπωση δηλώσεων και δεσμεύσεων - αφορά στην **ικανοποίηση όλων των θεμιτών στόχων** - όχι μόνο τους στόχους προστασίας της ιδιωτικής ζωής. Το PbD έχει διπλό χαρακτήρα, επιτρέπει την **πλήρη λειτουργικότητα** - πραγματικά, πρακτικά αποτελέσματα και ευεργετικά αποτελέσματα που πρέπει να επιτευχθούν για πολλά μέρη.

Η ενσωμάτωση της προστασίας της ιδιωτικής ζωής σε μια συγκεκριμένη τεχνολογία, διαδικασία ή σύστημα θα πρέπει να γίνεται με αντίληψη ανοιχτή, που αποδέχεται νέες λύσεις για πλήρη λειτουργικότητα, αποδοτικές και αποτελεσματικές **τόσο στο επίπεδο της επιχείρησης όσο και στο επίπεδο της προστασίας της ιδιωτικότητας**.

4. **Πλήρης** Λειτουργικότητα:
Θετικό Άθροισμα, όχι Μηδενικό Άθροισμα·

Για να το πετύχει αυτό, ο οργανισμός θα πρέπει:

Να αποδεχθεί ότι **μπορούν να συνυπάρξουν διάφορα νόμιμα συμφέροντα: αυτά του οργανισμού και αυτά των χρηστών** στους οποίους παρέχει υπηρεσίες και ότι αυτά είναι απαραίτητο να προσδιοριστούν, να εκτιμηθούν και να εξισορροπηθούν ανάλογα.

Να καθιερώσει **διαύλους επικοινωνίας** για συνεργασία και διαβούλευση με τους συμμετέχοντες, προκειμένου να κατανοηθούν και να προσεγγιστούν πολλαπλά συμφέροντα που, εκ πρώτης όψης, φαίνεται να αποκλίνουν.

Εάν οι προτεινόμενες λύσεις απειλούν την προστασία της ιδιωτικής ζωής, να αναζητήσει **νέες και εναλλακτικές λύσεις** για την επίτευξη της επιδιωκόμενης λειτουργικότητας και σκοπών, χωρίς όμως ποτέ ο οργανισμός να παραβλέψει το ότι πρέπει να διαχειριστεί επαρκώς τους κινδύνους για την ιδιωτικότητα του χρήστη.

5. Καθολική **Ασφάλεια**:
Προστασία **Καθ’ όλη τη διάρκεια** του κύκλου ζωής·

Το PbD, έχοντας ενσωματωθεί στο σύστημα πριν ακόμα συλλεχθεί το πρώτο στοιχείο πληροφοριών, επεκτείνεται σε όλη τη διάρκεια του κύκλου ζωής των εμπλεκόμενων δεδομένων. Η ύπαρξη ισχυρών μέτρων ασφαλείας είναι απαραίτητη για την χρονικά καθολική προστασία της ιδιωτικής ζωής. Κατοχυρώνεται ότι **κατά την επεξεργασία τα δεδομένα διατηρούνται με ασφαλή τρόπο** και ότι **στο τέλος της επεξεργασίας καταστρέφονται εγκαίρως με ασφαλή τρόπο**. Έτσι, το PbD εξασφαλίζει την ασφαλή διαχείριση των πληροφοριών **από την αρχή μέχρι το τέλος της επεξεργασίας**.

Δεν πρέπει να υπάρχουν κενά ούτε στην προστασία ούτε στη λογοδοσία. Στην ουσία, **χωρίς ισχυρή ασφάλεια, δεν μπορεί να υπάρξει ιδιωτικότητα**.

5. Καθολική **Ασφάλεια**: Προστασία **Καθ’ όλη τη διάρκεια** του κύκλου ζωής·

Οι οργανισμοί πρέπει να αναλάβουν την ευθύνη για την προστασία των προσωπικών δεδομένων καθ’ όλη τη διάρκεια του κύκλου ζωής τους, σύμφωνα με πρότυπα που έχουν αναπτυχθεί από αναγνωρισμένους φορείς ανάπτυξης προτύπων.

Τα εφαρμοσμένα πρότυπα ασφάλειας πρέπει να διασφαλίζουν την **εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα** των προσωπικών δεδομένων καθ’ όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένων, μεταξύ άλλων, μεθόδων ασφαλούς καταστροφής, κατάλληλης κρυπτογράφησης και ισχυρών μεθόδων ελέγχου και καταγραφής πρόσβασης. Περιλαμβάνεται, εδώ, η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η ανθεκτικότητα των συστημάτων. Η προστασία της ιδιωτικής ζωής εγγυάται επίσης την αδυναμία διασύνδεσης (unlinkability), τη διαφάνεια και την ικανότητα παρέμβασης και ελέγχου του υποκειμένου των δεδομένων στην επεξεργασία (παρεμβατικότητα).

5. Καθολική **Ασφάλεια**: Προστασία **Καθ' όλη τη διάρκεια** του κύκλου ζωής·

Για την ενσωμάτωση της προστασίας της ιδιωτικότητας σε όλα τα στάδια της επεξεργασίας δεδομένων, πρέπει να αναλυθούν διεξοδικά οι διαφορετικές ενέργειες επεξεργασίας (συλλογή, καταγραφή, ταξινόμηση, διατήρηση, διαβούλευση, διανομή, περιορισμός, διαγραφή, κλπ.) και πρέπει να εφαρμοστούν τα πλέον κατάλληλα, κατά περίπτωση, μέτρα για την προστασία των πληροφοριών, όπως:

Τεχνικές **ψευδωνυμοποίησης ή ανωνυμοποίησης** όπως k-ανωνυμία, από τα πρώτα στάδια.

Ταξινόμηση και οργάνωση των δεδομένων και των επεξεργασιών βάσει των προφίλ πρόσβασης.

Προεπιλογή της κρυπτογράφησης έτσι ώστε, όταν κλαπούν τα υλικά μέσα αποτύπωσης των προσωπικών δεδομένων ή όταν υποκλαπούν τα προσωπικά δεδομένα, η "φυσική" κατάσταση των δεδομένων να είναι "δυσανάγνωστη".

Ασφαλής και **εγγυημένη καταστροφή** των πληροφοριών στο τέλος του κύκλου ζωής τους.

6. Ορατότητα **και** Διαφάνεια: Διατήρηση **Ανοιχτής Προσέγγισης·**

Ένα από τα κλειδιά για την εγγύηση της προστασίας της ιδιωτικής ζωής είναι το ότι **ο οργανισμός είναι σε θέση να αποδείξει τη συμμόρφωση με τις υποχρεώσεις του**, επαληθεύοντας ότι η επεξεργασία είναι σύμφωνη με τις περιστάσεις. **Αντίστοιχα, τα υποκείμενα των δεδομένων θα πρέπει να μπορούν να επαληθεύσουν την εμπιστοσύνη που επέδειξαν**. Trust, but verify.

6. Ορατότητα **και** Διαφάνεια: Διατήρηση **Ανοιχτής Προσέγγισης·**

Οι οργανισμοί θα πρέπει να δώσουν έμφαση κυρίως στη:

Λογοδοσία: Η συλλογή προσωπικών δεδομένων συνεπάγεται καθήκον φροντίδας για την προστασία τους.

Η ευθύνη για όλες τις πολιτικές και διαδικασίες που σχετίζονται με την προστασία της ιδιωτικής ζωής πρέπει να τεκμηριώνεται, να κοινοποιείται κατά περίπτωση, και να ανατίθεται σε συγκεκριμένο άτομο. Κατά τη διαβίβαση προσωπικών πληροφοριών σε τρίτους, εξασφαλίζεται ισοδύναμη προστασία της ιδιωτικής ζωής μέσω συμβάσεων ή με άλλα μέσα.

Διαφάνεια: **Η ανοιχτή νοοτροπία και η διαφάνεια είναι το κλειδί της λογοδοσίας**. Τα άτομα πρέπει να έχουν στη διάθεσή τους τις πληροφορίες που αφορούν στις πολιτικές και στις πρακτικές οι οποίες αποβλέπουν στη διαχείριση των προσωπικών πληροφοριών.

6. Ορατότητα **και** Διαφάνεια: Διατήρηση **Ανοιχτής Προσέγγισης·**

Οι οργανισμοί θα πρέπει να δώσουν έμφαση κυρίως στη:

Συμμόρφωση: Θα πρέπει να θεσπιστούν μηχανισμοί καταγγελίας και έννομης προστασίας, και να γνωστοποιηθούν αυτοί στα υποκείμενα, συμπεριλαμβανομένου του τρόπου πρόσβασης στο επόμενο προβλεπόμενο επίπεδο προσφυγής. Θα πρέπει να ληφθούν τα αναγκαία μέτρα για την παρακολούθηση, την αξιολόγηση και την επαλήθευση της συμμόρφωσης με τις πολιτικές και τις διαδικασίες προστασίας της ιδιωτικότητας.

6. Ορατότητα **και** Διαφάνεια: Διατήρηση **Ανοιχτής Προσέγγισης·**

Η προώθηση της διαφάνειας και της ορατότητας απαιτεί την υιοθέτησης μιας σειράς μέτρων, όπως:

Δημοσιοποίηση των πολιτικών προστασίας της ιδιωτικής ζωής που διέπουν τη λειτουργία του οργανισμού.

Ανάπτυξη και δημοσίευση σύντομων, σαφών και κατανοητών ρητρών πληροφόρησης που είναι εύκολα προσβάσιμες και επιτρέπουν στα υποκείμενα των δεδομένων να κατανοούν το εύρος της επεξεργασίας των δεδομένων τους, τους κινδύνους στους οποίους ενδέχεται να εκτεθούν, καθώς και τον τρόπο άσκησης των δικαιωμάτων τους όσον αφορά στην προστασία δεδομένων.

Αν και δεν είναι υποχρεωτική για όλους τους υπεύθυνους επεξεργασίας, η δημοσιοποίηση ή τουλάχιστον η εύκολη πρόσβαση των υποκειμένων των δεδομένων στον κατάλογο όλων των επεξεργασιών που διεξάγονται στον οργανισμό.

6. Ορατότητα **και** Διαφάνεια: Διατήρηση **Ανοιχτής Προσέγγισης·**

Η προώθηση της διαφάνειας και της ορατότητας απαιτεί την υιοθέτησης μιας σειράς μέτρων, όπως:

Δημοσιοποίηση των στοιχείων επικοινωνίας του προσώπου που είναι υπεύθυνο για την οργάνωση των μέτρων προστασίας της ιδιωτικότητας εντός του οργανισμού.

Δημιουργία προσιτών, απλών και αποτελεσματικών μηχανισμών επικοινωνίας, καταγγελιών, και αποζημίωσης για τα υποκείμενα των δεδομένων.

7. Σεβασμός προς την Ιδιωτικότητα των Χρηστών: Διατήρηση του **Χρήστη στο Επίκεντρο**

Χωρίς να λησμονούμε τα έννομα συμφέροντα του οργανισμού όσον αφορά στην επεξεργασία δεδομένων, ο τελικός στόχος πρέπει να είναι η διασφάλιση των δικαιωμάτων και των ελευθεριών των χρηστών, των οποίων τα δεδομένα αποτελούν αντικείμενο επεξεργασίας και ως εκ τούτου, **κάθε μέτρο που πρέπει να ληφθεί πρέπει να επικεντρώνεται στην εξασφάλιση της ιδιωτικής τους ζωής**. Αυτό συνεπάγεται τον σχεδιασμό διαδικασιών, εφαρμογών, προϊόντων και υπηρεσιών «προσανατολισμένων στον χρήστη», που να προβλέπουν τις ανάγκες του.

Ο χρήστης πρέπει να διαδραματίσει ενεργό ρόλο στη διαχείριση των δεδομένων του και στον έλεγχο του τι κάνουν οι άλλοι με αυτά. Η αδράνειά του δεν πρέπει να συνεπάγεται μείωση της προστασίας της ιδιωτικής ζωής, βάσει και της προαναφερθείσας αρχής που υποστηρίζει την ιδιωτικότητα ως προεπιλεγμένη ρύθμιση, προσφέροντας το υψηλότερο δυνατό επίπεδο προστασίας.

7. Σεβασμός προς την Ιδιωτικότητα των Χρηστών: Διατήρηση του **Χρήστη στο Επίκεντρο**

Ο σχεδιασμός διαδικασιών, εφαρμογών, προϊόντων και υπηρεσιών που επικεντρώνεται στην εξασφάλιση της ιδιωτικής ζωής των υποκειμένων των δεδομένων **περιλαμβάνει:**

Εφαρμογή ρυθμίσεων απορρήτου που είναι “στιβαρές” από προεπιλογή, και όπου **οι χρήστες ενημερώνονται** για τις συνέπειες που θα επιφέρει στην ιδιωτικότητά τους η τροποποίηση των παραμέτρων.

Παροχή πλήρων και κατάλληλων πληροφοριών που οδηγούν σε μια ενημερωμένη, ελεύθερη, συγκεκριμένη και σαφή συγκατάθεση, η οποία πρέπει να είναι ρητή σε όλες τις περιπτώσεις που το απαιτούν. Η συγκατάθεση μπορεί αργότερα να ανακληθεί.

7. Σεβασμός προς την Ιδιωτικότητα των Χρηστών: Διατήρηση του **Χρήστη στο Επίκεντρο**

Ο σχεδιασμός διαδικασιών, εφαρμογών, προϊόντων και υπηρεσιών που επικεντρώνεται στην εξασφάλιση της ιδιωτικής ζωής των υποκειμένων των δεδομένων περιλαμβάνει:

Παροχή στα υποκείμενα των δεδομένων πρόσβασης στα δεδομένα τους και σε λεπτομερείς πληροφορίες σχετικά με τους σκοπούς επεξεργασίας και τις διαβιβάσεις που πραγματοποιούνται. Τα υποκείμενα πρέπει να μπορούν να αμφισβητήσουν την ακρίβεια και την πληρότητα των δεδομένων και να τα διορθώσουν.

Εφαρμογή αποδοτικών και αποτελεσματικών **μηχανισμών που επιτρέπουν** στα υποκείμενα των δεδομένων **να ασκούν τα δικαιώματά τους** για την προστασία των δεδομένων.

Στις 25-05-2018 τέθηκε σε εφαρμογή ο Κανονισμός (ΕΕ) 2016/679, γνωστός ως **Γενικός Κανονισμός για την Προστασία Δεδομένων** (ΓΚΠΔ) ή General Data Protection Regulation (GDPR), με τον οποίο η ιδέα του PbD μετουσιώθηκε σε δεσμευτική νομική υποχρέωση, η παραβίαση της οποίας δύναται να επισύρει κυρώσεις.

Με τον ΓΚΠΔ **μεταβαίνουμε από** το **Privacy by Design** (PbD) στο **Data Protection by Design and by Default** (DPbDD ή $DPbD^2$), όπως τιτλοφορείται το άρθρο 25.

Ο ΓΚΠΔ εισάγει την **αρχή της Λογοδοσίας**, κατά την οποία ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία οφείλει να μπορεί να αποδείξει τη συμμόρφωση με τις υποχρεώσεις του.

Κανονισμός (ΕΕ) 2016/679

Γενικός Κανονισμός για την Προστασία Δεδομένων

ΚΕΦΑΛΑΙΟ IV

Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία

Τμήμα 1

Γενικές υποχρεώσεις

Άρθρο 25

Προστασία των δεδομένων ήδη από το σχεδιασμό

"εφαρμογή αρχών προστασίας των δεδομένων"

"τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας"

Προστασία των δεδομένων εξ ορισμού

Ισχύουν αυτόματα οι αυστηρότερες ρυθμίσεις προστασίας δεδομένων.

Κανονισμός (ΕΕ) 2016/679

Γενικός Κανονισμός για την Προστασία Δεδομένων

Αιτιολογική σκέψη 78

“Προκειμένου να μπορεί να αποδείξει συμμόρφωση προς τον παρόντα κανονισμό, ο υπεύθυνος επεξεργασίας θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τα οποία ανταποκρίνονται ειδικότερα στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού”.

“Οι αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού θα πρέπει επίσης να λαμβάνονται υπόψη στο πλαίσιο των δημόσιων διαγωνισμών”.

Αιτιολογική σκέψη 108

“Ελλείψει απόφασης επάρκειας … λαμβάνουν μέτρα … τήρηση των γενικών αρχών που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και των αρχών περί προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού”.

Κανονισμός (ΕΕ) 2016/679

Γενικός Κανονισμός για την Προστασία Δεδομένων

Άρθρο 47 (Δεσμευτικοί εταιρικοί κανόνες)

"… διευκρινίζουν τουλάχιστον … την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού".

Άρθρο 83 (Γενικοί όροι επιβολής διοικητικών προστίμων)

" … ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν δυνάμει των άρθρων 25 και 32".

Ο υπεύθυνος επεξεργασίας οφείλει 1) να εφαρμόσει κατάλληλα Τεχνικά και Οργανωτικά Μέτρα που είναι σχεδιασμένα να εξασφαλίσουν τη συμμόρφωση με τις αρχές της επεξεργασίας, που αναφέρονται στο άρθρο 5 του ΓΚΠΔ **και 2) να** ενσωματώσει στην επεξεργασία τις απαραίτητες δικλείδες ασφαλείας ώστε να **συμμορφωθεί με τις υποχρεώσεις του ΓΚΠΔ** και **να προστατέψει τα δικαιώματα των υποκειμένων των δεδομένων**, όπως αναφέρονται στα άρθρα 12 έως 22 του ΓΚΠΔ, **και τις ελευθερίες τους**, όπως αναφέρονται στην αιτιολογική σκέψη 4 του ΓΚΠΔ και στον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

Προς τούτο λαμβάνει υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, και τους κινδύνους - διαφορετικής πιθανότητας επέλευσης και σοβαρότητας - για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία.

Επίσης, τις αρχές της διαφάνειας, της νομιμότητας, της αντικειμενικότητας, της ελαχιστοποίησης του σκοπού, της ελαχιστοποίησης των δεδομένων, της ακρίβειας, του περιορισμού της διάρκειας, και της ακεραιότητας και εμπιστευτικότητας.

Στόχος προστασίας ιδιωτικότητας	**Στρατηγικές** προστασίας της ιδιωτικότητας που **εφαρμόζονται** στα **δεδομένα**	Στρατηγικές προστασίας της ιδιωτικότητας που εφαρμόζονται σε **διαδικασίες**
Μη διασυνδεσιμότητα	Ελαχιστοποίηση Απόκρυψη Διαχωρισμός Αφαιρετικότητα	
Διαφάνεια		Ενημέρωση
Έλεγχος		Έλεγχος Επιβολή Επίδειξη

Πηγές:

Κατευθυντήριες Γραμμές 4/2019 για το Άρθρο 25 Προστασία των δεδομένων από το Σχεδιασμό και εξ Ορισμού του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ).

Οδηγός για το Privacy by Design της Ισπανικής Αρχής Προστασίας Δεδομένων.

Ιστότοποι της ENISA, του Κέντρου Αριστείας για το Privacy by Design του Πανεπιστημίου του Ryerson, του Internet Privacy Engineering Network (IPEN).

Διοικητικά πρόστιμα:

Το πρώτο πρόστιμο σχετικά με παραβίαση του άρθρου 25 του ΓΚΠΔ επιβλήθηκε στις 27-06-2019 από την Αρχή Προστασίας Δεδομένων της Ρουμανίας.

Η Αρχή διέγνωσε ότι η υπεύθυνος επεξεργασίας UNICREDIT BANK S.A. **παραβίασε την αρχή της ελαχιστοποίησης των δεδομένων** και τις νόμιμες υποχρεώσεις της για **προστασία των δεδομένων ήδη από τον σχεδιασμό**, λόγω σφάλματος στο σύστημα της Τράπεζας. Συγκεκριμένα, καθένας που λάμβανε χρηματικό ποσό μέσω κατάθεσης στον λογαριασμό του στην Τράπεζα μπορούσε να δει τον αριθμό ταυτότητας και τη διεύθυνση του αποστολέα.

Αριθμός υποκειμένων δεδομένων που προσβλήθηκαν: 337.042

Χρονική περίοδος: 25-05-2018 μέχρι 10-12-2018

Πρόστιμο: 130.000 ευρώ.

Στην Ελλάδα, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) έγινε πρόσφατα αποδέκτης καταγγελιών σε δυο διαφορετικές περιπτώσεις.

Υπενθυμίζεται ότι, σύμφωνα με το άρθρο 11 του ν. 3471/2006 οι πάροχοι υπηρεσιών ηλεκτρονικής επικοινωνίας τηρούν **μητρώο αντιρρήσεων** («opt-out»), στο οποίο περιλαμβάνονται οι συνδρομητές του παρόχου που έχουν ζητήσει να μην δέχονται κλήσεις για απ' ευθείας εμπορική προώθηση και για κάθε είδους διαφημιστικούς σκοπούς.

Απόφαση υπ’ αριθ. **31/2019 της ΑΠΔΠΧ**:

Συνδρομητές του ΟΤΕ, παρότι είχαν εγγραφεί στο μητρώο αντιρρήσεων, λάμβαναν τηλεφωνικές κλήσεις από τρίτες εταιρείες για σκοπούς προώθησης προϊόντων και υπηρεσιών.

Η ΑΠΔΠΧ διαπίστωσε ότι συνδρομητές του ΟΤΕ που είχαν υποβάλει αίτημα φορητότητας και στην συνέχεια είχαν ακυρώσει το αίτημα αυτό, εμφανίζονταν μεν ως εγγεγραμμένοι στο μητρώο opt-out στην εσωτερική εφαρμογή πελατειακών σχέσεων, αλλά οι τηλεφωνικοί τους αριθμοί δεν περιλαμβάνονταν στο μητρώο που έστελνε ο ΟΤΕ στις διαφημιζόμενες εταιρείες, καθώς τα δύο συστήματα, λόγω σφάλματος στη διασύνδεσή τους, δεν είχαν το ίδιο περιεχόμενο.

Σύμφωνα με την Αρχή, το περιστατικό επηρέασε μεγάλο αριθμό φυσικών προσώπων συνδρομητών και **παραβιάστηκε το άρθρο 25** (προστασία των δεδομένων ήδη από τον σχεδιασμό) **και το άρθρο 5** παρ. 1 γ΄ (αρχή της ακρίβειας) **του ΓΚΠΔ**.

Διοικητικό πρόστιμο: 200.000 ευρώ.

Απόφαση υπ’ αριθ. **34/2019 της ΑΠΔΠΧ**:

Από το 2013 και μετά, λόγω τεχνικού σφάλματος στο σύστημα του ΟΤΕ, όσοι χρησιμοποιούσαν τον σύνδεσμο "unsubscribe" για να διαγραφούν από τη λίστα αποδεκτών μηνυμάτων διαφημιστικού περιεχομένου εγγράφονταν μεν στη λίστα προς διαγραφή, αλλά το σύστημα του ΟΤΕ δεν εκτελούσε τη διαγραφή τους από τη λίστα αποδεκτών μηνυμάτων. Ο ΟΤΕ δεν διέθετε καθορισμένη διαδικασία μέσω της οποίας να εντοπίζει ότι το δικαίωμα εναντίωσης του υποκειμένου δεν μπορούσε να ικανοποιηθεί, δεν διέθετε δηλαδή κατάλληλο οργανωτικό μέτρο.

Μόλις το σφάλμα έγινε αντιληπτό μετά την επέμβαση της Αρχής, ο ΟΤΕ διόρθωσε το σφάλμα και προέβηκε στη διαγραφή περίπου 8.000 ονομάτων από τις λίστες αποδεκτών μηνυμάτων.

Σύμφωνα με την απόφαση της Αρχής **παραβιάστηκε το άρθρο 25** (προστασία των δεδομένων ήδη από τον σχεδιασμό) **και το άρθρο 21** παρ. 3 (δικαίωμα εναντίωσης του υποκειμένου στην επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης) **του ΓΚΠΔ**.

Διοικητικό πρόστιμο: 200.000 ευρώ.

Στις 30-10-2019 η Επίτροπος Προστασίας Προσωπικών Δεδομένων και Ελευθερίας των Πληροφοριών του Βερολίνου (Berliner Beauftragte für Datenschutz und Informationsfreiheit – Berlin DPA) επέβαλε πρόστιμο ύψους 14,5 εκατομμυρίων ευρώ σε γερμανική εταιρεία ακινήτων, τη Deutsche Wohnen SE.

Η Επίτροπος διαπίστωσε ότι προσωπικά δεδομένα διατηρούνταν για χρονικό διάστημα σημαντικά μεγαλύτερο από το απαραίτητο, και δεν διαγράφονταν, και διέγνωσε παραβίαση του ΓΚΠΔ κατά τρεις τρόπους:

i) ο υπεύθυνος επεξεργασίας **δεν είχε νομική βάση για τη διατήρηση** των προσωπικών δεδομένων,

ii) **παραβιάστηκε** η υποχρέωση για προστασία των δεδομένων ήδη από τον σχεδιασμό, σύμφωνα με **το άρθρο 25 παρ. 1 του ΓΚΠΔ**, και

iii) παραβιάστηκαν οι γενικές αρχές επεξεργασίας που ορίζονται στο **άρθρο 5 του ΓΚΠΔ**.

Ολοκληρώνοντας, η πλέον αποτελεσματική προστασία της ιδιωτικότητας και των προσωπικών δεδομένων επιτυγχάνεται με την **προληπτική ενσωμάτωση** των αρχών του Privacy by Design, προλαμβάνοντας την επέλευση της ζημίας και αποτρέποντας την παραβίαση των προσωπικών δεδομένων.

Η πρόληψη είναι πάντοτε πιο εύκολη και πολύ πιο αποδοτική όταν η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων έχει εισαχθεί στο σύστημα εξ αρχής, παρά εκ των υστέρων.

Οι οργανισμοί οφείλουν να εγκαταλείψουν τη λογική του στενά θεωρημένου μονόπλευρου κέρδους και να υιοθετήσουν στρατηγικές που αποκομίζουν κέρδη προς όλες τις κατευθύνσεις, να πουν όχι στο ψευδοεπιχείρημα Προστασία δεδομένων **ή** ασφάλεια, αλλά να αναγνωρίσουν ότι μπορεί να συνυπάρξει Προστασία **και** ασφάλεια.

Η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων δεν αποβλέπει στη μυστικότητα ή στην απόκρυψη γεγονότων. Χωρίς την προστασία των δύο παραπάνω στοιχείων, η ανθρώπινη δημιουργικότητα, καινοτομία, και ευημερία χάνουν την ουσία τους.

Καρδία της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων είναι η ελευθερία. **Η ελευθερία** είναι που εξασφαλίζει στο υποκείμενο των δεδομένων την αυτοδιάθεσή του ώστε να προβεί στις επιλογές που επιθυμεί, και είναι η ελευθερία που επιτρέπει σε κάθε έναν από εμάς την έκφραση της προσωπικότητάς του, ως ενεργού πολίτη.

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ
www.mli.uom.gr

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ
ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
& ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Ευχαριστώ για την προσοχή σας!

version 20191205