Πανεπιστήμιο Πειραιώς

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μεταπτυχιακό Πρόγραμμα Σπουδών

«**Ασφάλεια Ψηφιακών Συστημάτων**»

Ιδιωτικότητα ήδη από τον Σχεδιασμό: Συγκριτική ανάλυση των 31700-1 του International Organization for Standardization και Design Process Standard ver.1 του Institute of Operational Privacy Design

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Σαραφίδη Λάζαρου

Επιβλέπων καθηγητής: Στέφανος Γκρίτζαλης

Πειραιάς, Ιανουάριος 2024

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και Ευχαριστίες

Με την ολοκλήρωση αυτής της μεταπτυχιακής διπλωματικής εργασίας, ολοκληρώνονται οι μεταπτυχιακές σπουδές μου στην «Ασφάλεια Ψηφιακών Συστημάτων» στο Πανεπιστήμιο Πειραιώς.

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες προς όλους όσους συνέβαλαν στην ολοκλήρωση αυτής της εργασίας. Ένα ειδικό ευχαριστώ απευθύνεται προς τον επιβλέποντα καθηγητή μου, κ. Στέφανο Γκρίτζαλη, για τη στήριξη, την καθοδήγηση και τις ενθαρρυντικές συμβουλές που μου παρείχε καθ' όλη τη διάρκεια της εκπόνησης αυτής της εργασίας.

Τέλος, εκφράζω τη βαθιά μου ευγνωμοσύνη προς την οικογένειά μου και τους φίλους μου, που με στήριξαν με την αγάπη και την κατανόησή τους καθ' όλη τη διάρκεια αυτής της απαιτητικής περιόδου.

του Σαραφίδη Λάζαρου

Τμήμα Ψηφιακών Συστημάτων, Μεταπτυχιακό Πρόγραμμα Σπουδών «Ασφάλεια Ψηφιακών Συστημάτων»

Πανεπιστήμιο Πειραιώς

Η σελίδα αυτή είναι σκόπιμα λευκή.

Περιεχόμενα

Λίστα Εικόνων

Ακρωνύμια

ΔΠΧ	Δεδομένα Προσωπικού Χαρακτήρα
ΣΕΥ	Συμφωνητικό Επιπέδου Υπηρεσίας (SLA)
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ΤΠ	Τεχνολογίες Πληροφορικής
ICT	Information and Communication Technologies
IOPD	Institute of Operational Privacy Design
GDPR/ΓΚΠΔ	General Data Protection Regulation/Γενικός Κανονισμός για την Προστασία Δεδομένων
API	Application Programming Interface
HR	Human Resources
NIST	National Institute of Standards and Technology
SDLC	Software Development Life Cycle

Περίληψη

Η διατριβή αυτής της μεταπτυχιακής εργασίας έχει ως στόχο τη διεξαγωγή μιας ανάλυσης και σύγκρισης δύο γνωστών προτύπων στον τομέα του Privacy by Design˙ του "*ISO 31700-1 Privacy by design for consumer goods and services*" και του "*Design Process Standard*" από το Institute of Operational Privacy Design.

Η μελέτη ξεκινάει εξετάζοντας κεντρικά στοιχεία κάθε προτύπου, συμπεριλαμβανομένων των θεμελιωδών αρχών, των μεθοδολογιών και των πεδίων εφαρμογής τους. Πρώτα αναλύεται το "*ISO 31700-1*" και στην συνέχεια το "*Design Process Standard*". Στην συνέχεια, μέσα από μια εις βάθος εξέταση αυτών των προτύπων, η έρευνα επιδιώκει να εντοπίσει ομοιότητες, διαφορές και πιθανές συνέργειες, συνεισφέροντας σημαντικές εισηγήσεις στον διάλογο για πρακτικές ιδιωτικότητας ήδη από τον σχεδιασμό.

Λέξεις κλειδιά: *Privacy by Design*, *ISO 31700-1:2023*, *Design Process Standard*

1. ISO 31700-1 [1]

Εισαγωγή

Η εμπιστοσύνη των καταναλωτών και το κατά πόσο ικανοποιούνται οι ατομικές ανάγκες της ιδιωτικότητας (privacy) αποτελούν καθοριστικές ανησυχίες για την ψηφιακή οικονομία. Αυτό περιλαμβάνει τον τρόπο με τον οποίο επεξεργάζονται (συλλέγονται, χρησιμοποιούνται, αποκτούν πρόσβαση, αποθηκεύονται και διαγράφονται) τα δεδομένα προσωπικού χαρακτήρα (ΔΠΧ) και άλλα δεδομένα των καταναλωτών – ή δεν συλλέγονται ή δεν επεξεργάζονται σκόπιμα. – από τον οργανισμό και από τα ψηφιακά αγαθά και υπηρεσίες στο πλαίσιο της εν λόγω ψηφιακής οικονομίας. Εάν τα ΔΠΧ έχουν παραβιαστεί λόγω χαλαρών, ξεπερασμένων ή ανύπαρκτων πρακτικών προστασίας της ιδιωτικότητας, οι συνέπειες για το άτομο μπορεί να είναι σοβαρές. Επιπλέον, η εμπιστοσύνη των καταναλωτών στο ψηφιακό προϊόν μπορεί να πληγεί με δυνητικές νομικές επιπτώσεις ή επιπτώσεις στη φήμη του οργανισμού που παρέχει το εν λόγω καταναλωτικό προϊόν.

Ο όρος "Απαιτήσεις Ιδιωτικότητας ήδη από τον Σχεδιασμό" (Privacy By Design) χρησιμοποιήθηκε αρχικά από τον Επίτροπο Πληροφοριών και Ιδιωτικότητας του Οντάριο του Καναδά (Information and Privacy Commissioner of Ontario, Canada), με στόχο να μην χρειάζεται το άτομο να επωμίζεται το βάρος της προσπάθειας για προστασία όταν χρησιμοποιεί ένα καταναλωτικό προϊόν.

Οι Απαιτήσεις Ιδιωτικότητας ήδη από τον Σχεδιασμό αναφέρονται σε διάφορες μεθοδολογίες για την ανάπτυξη προϊόντων, διαδικασιών, συστημάτων, λογισμικού και υπηρεσιών, π.χ. Αναφορές [2], [3], [4], [5], [6] και [7]. Αυτές οι μεθοδολογίες λαμβάνουν υπόψη την ιδιωτικότητα ενός καταναλωτή καθ' όλη τη διάρκεια του σχεδιασμού και της ανάπτυξης ενός προϊόντος, λαμβάνοντας υπόψη ολόκληρο τον κύκλο ζωής του προϊόντος – από πριν από τη διάθεσή του στην αγορά, την αγορά και τη χρήση του από τους καταναλωτές, έως τον αναμενόμενο χρόνο κατά τον οποίο το προϊόν θα σταματήσει τελικά να χρησιμοποιείται. Αυτό σημαίνει ότι ένα προϊόν διαθέτει προεπιλεγμένα αντίμετρα και ρυθμίσεις ιδιωτικότητας με γνώμονα τον καταναλωτή, τα οποία παρέχουν τα κατάλληλα επίπεδα ιδιωτικότητας, χωρίς να επιβαρύνουν υπέρμετρα τον καταναλωτή.

ΣΗΜΕΙΩΣΗ: Το παρόν έγγραφο παρέχει στη βιβλιογραφία παραπομπές σε άλλα υφιστάμενα πρότυπα και πηγές, που παρέχουν λεπτομερέστερες απαιτήσεις και οδηγίες σχετικά με την ιδιωτικότητα (π.χ. αναγνώριση των ΔΠΧ, πρόσβαση σε ΔΠΧ και αντίμετρα ιδιωτικότητας, συγκατάθεση των καταναλωτών, κοινοποίηση παραβίασης της ιδιωτικότητας, ασφαλής διάθεση των ΔΠΧ, αλληλεπιδράσεις με τρίτους εκτελών την επεξεργασία) για κοινές λειτουργίες εντός του οργανισμού (π.χ. Εταιρική διακυβέρνηση, Διακυβέρνηση Δεδομένων και

Ιδιωτικότητας, Διαχείριση Λειτουργιών και Υπηρεσιών IT, Ασφάλεια και Διοίκηση Ασφάλειας, Διαχείριση Δεδομένων και Βάσεων Δεδομένων, Μάρκετινγκ, Διαχείριση Προϊόντων, Ανάπτυξη Διαδικτυακών Εφαρμογών και Εφαρμογών Κινητού, Ανάπτυξη συστημάτων, Διαχείριση Συστημάτων, Διαχείριση Δικτύων).

Στο παρόν έγγραφο, τα οφέλη της απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό μπορούν να εξεταστούν μέσω τριών κατευθυντήριων αρχών, όπως περιγράφονται παρακάτω.

Ενδυνάμωση και διαφάνεια

Υπάρχει αυξανόμενη ζήτηση για ακριβείς ισχυρισμούς περί ιδιωτικότητας, συστηματικές μεθόδους δέουσας επιμέλειας για την ιδιωτικότητα και μεγαλύτερη διαφάνεια και ανάληψη ευθυνών στο σχεδιασμό και τη λειτουργία των καταναλωτικών προϊόντων που επεξεργάζονται ΔΠΧ. Στόχος είναι να προωθηθεί η ευρύτερη υιοθέτηση του σχεδιασμού με γνώμονα την ιδιωτικότητα, να κερδηθεί η εμπιστοσύνη των καταναλωτών και να ικανοποιηθούν οι ανάγκες των καταναλωτών για ισχυρή ιδιωτικότητα και προστασίας των δεδομένων. Επιπλέον, σκοπός είναι να δημιουργηθούν και να προωθηθούν καινοτόμες λύσεις που προστατεύουν και διαχειρίζονται την ιδιωτικότητα των καταναλωτών: α) με την ανάλυση και την εφαρμογή αντιμέτρων ιδιωτικότητας με βάση την οπτική γωνία, το πλαίσιο και τις ανάγκες του καταναλωτή και β) με τη συνοπτική τεκμηρίωση και την άμεση επικοινωνία με τους καταναλωτές του τρόπου με τον οποίο προσεγγίστηκαν τα ζητήματα της ιδιωτικότητας.

Θεσμοθέτηση και ευθύνη

Στον σημερινό ψηφιακό κόσμο των κοινών πλατφορμών, των διασυνδεδεμένων συσκευών, των εφαρμογών νέφους και της εξατομίκευσης, είναι ολοένα και πιο σημαντικό να προσδιοριστούν και να διακριθούν οι ευθύνες και οι προοπτικές του καταναλωτή των προϊόντων που επεξεργάζονται τα ΔΠΧ από εκείνες του σχεδιασμού του προϊόντος, των επιχειρήσεων και άλλων ενδιαφερομένων στα οικοσυστήματα στα οποία λειτουργεί το προϊόν.

Οι απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό εστιάζει στην οπτική γωνία του καταναλωτή κατά τη θεσμοθέτηση ισχυρών κανόνων ιδιωτικότητας σε όλο το οικοσύστημα, συμπεριλαμβανομένης της προστασίας της ιδιωτικότητας και των πρακτικών χειρισμού δεδομένων. Με τις απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό, η συμπεριφορική εμπλοκή του καταναλωτή με το προϊόν (τα προϊόντα) και οι ανάγκες του για ιδιωτικότητα λαμβάνονται υπόψη από νωρίς και καθ' όλη τη διαδικασία του κύκλου ζωής του προϊόντος. Με αυτόν τον τρόπο, οι αποφάσεις σχετικά με τις ανάγκες της ιδιωτικότητας των καταναλωτών θα είναι πιο συνεπείς και συστηματικές και θα αποτελέσουν λειτουργική απαίτηση παράλληλα με τα συμφέροντα του σχεδιασμού του προϊόντος, των επιχειρήσεων και άλλων ενδιαφερόμενων μερών.

Οι απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό εστιάζουν επίσης στη λογοδοσία, την ευθύνη και την ηγεσία. Αυτές οι πτυχές είναι απαραίτητες για την επιτυχή λειτουργία και θεσμοθέτηση της διαδικασίας για απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό.

Η αποδεδειγμένη δέσμευση της ηγεσίας για τις απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό είναι απαραίτητη για τη λειτουργία και τη θεσμοθέτηση της ιδιωτικότητας στη διαδικασία σχεδιασμού προϊόντων ενός οργανισμού.

Οικοσύστημα και κύκλος ζωής

Η προσέγγιση απαιτήσεων ιδιωτικότητας ήδη από τον σχεδιασμό μπορεί να εφαρμοστεί στα ευρύτερα οικοσυστήματα πληροφοριών στα οποία δραστηριοποιούνται και λειτουργούν τόσο οι τεχνολογίες όσο και οι οργανισμοί. Η προστασία της ιδιωτικότητας και του καταναλωτή ωφελείται από μια ολιστική, ολοκληρωμένη προσέγγιση που λαμβάνει υπόψη όσο το δυνατόν περισσότερους σχετικούς παράγοντες (π.χ. τον τύπο του καταναλωτή, τον στόχο και την πρόθεσή του να χρησιμοποιήσει ένα προϊόν και τα δεδομένα που θα επεξεργαστεί το προϊόν για τον εν λόγω καταναλωτή) – ακόμη και (ή ιδίως) όταν οι παράγοντες αυτοί βρίσκονται εκτός του άμεσου ελέγχου οποιουδήποτε συγκεκριμένου φορέα, οργανισμού ή στοιχείου του συστήματος. [βλέπε 5.5.3 Οδηγία α)].

Οι απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό ισχύουν για όλα τα προϊόντα που χρησιμοποιούν ΔΠΧ, είτε πρόκειται για υλικά αγαθά είτε για άυλες υπηρεσίες, όπως λογισμικό ως υπηρεσία, ή για ένα μείγμα και των δύο. Προορίζονται να είναι επεκτάσιμες στις ανάγκες όλων των τύπων οργανισμών σε διαφορετικές χώρες και διαφορετικούς τομείς, ανεξάρτητα από το μέγεθος ή την ωριμότητα του οργανισμού.

Είναι πιθανό να εντοπιστούν πρόσθετα ζητήματα ιδιωτικότητας και να προκύψει ανάγκη για σχετικά αντίμετρα σε οποιοδήποτε σημείο του κύκλου ζωής του προϊόντος, συμπεριλαμβανομένης της ανάπτυξης ή μετά την χρήση από τους καταναλωτές. Οι μεθοδολογίες για τις απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό υποστηρίζουν επαναληπτικές προσεγγίσεις στην ανάπτυξη προϊόντων, με συμπληρωματικές βελτιώσεις της ιδιωτικότητας που σχεδιάζονται και αναπτύσσονται πολύ μετά την αρχική φάση σχεδιασμού.

Κοινό για το παρόν έγγραφο

Το παρόν έγγραφο απευθύνεται κυρίως στο προσωπικό των οργανισμών και των τρίτων μερών που είναι υπεύθυνοι για την έννοια, το σχεδιασμό, την κατασκευή, τη διαχείριση, τις δοκιμές, τη λειτουργία, την εξυπηρέτηση, τη συντήρηση και την απόρριψη καταναλωτικών αγαθών και υπηρεσιών.

Προστασία του καταναλωτή – Προστασία της ιδιωτικότητας ήδη από το σχεδιασμό για καταναλωτικά αγαθά και υπηρεσίες

Μέρος 1: Απαιτήσεις υψηλού επιπέδου

1 Πεδίο εφαρμογής

Το παρόν έγγραφο καθορίζει απαιτήσεις υψηλού επιπέδου για τις απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό για την προστασία της ιδιωτικότητας καθ' όλη τη διάρκεια του κύκλου ζωής ενός καταναλωτικού προϊόντος, συμπεριλαμβανομένων των δεδομένων που επεξεργάζεται ο καταναλωτής.

Το παρόν έγγραφο δεν περιέχει συγκεκριμένες απαιτήσεις για τις διαβεβαιώσεις και τις δεσμεύσεις της ιδιωτικότητας που μπορούν να προσφέρουν οι οργανισμοί στους καταναλωτές, ούτε προσδιορίζει συγκεκριμένες μεθοδολογίες που μπορεί να υιοθετήσει ένας οργανισμός για τον σχεδιασμό και την εφαρμογή αντιμέτρων ιδιωτικότητας, ούτε την τεχνολογία που μπορεί να χρησιμοποιηθεί για τη λειτουργία των αντιμέτρων αυτών.

2 Κανονιστικές αναφορές

Δεν υπάρχουν κανονιστικές αναφορές στο παρόν έγγραφο.

3 Όροι και ορισμοί

Για τους σκοπούς του παρόντος εγγράφου, ισχύουν οι ακόλουθοι όροι και ορισμοί.

Οι οργανισμοί ISO και IEC διατηρούν βάσεις δεδομένων ορολογίας για χρήση στην τυποποίηση στις ακόλουθες διευθύνσεις:

— ISO Online browsing platform: διαθέσιμο στο https://www.iso.org/obp

— IEC Electropedia: διαθέσιμο στο https://electropedia.org/

3.1 καταναλωτής (consumer)
μεμονωμένο μέλος του ευρύτερου κοινού που αγοράζει ή χρησιμοποιεί περιουσία, προϊόντα για ιδιωτικούς σκοπούς

Σημείωση 1 στην καταχώριση: Ο όρος "καταναλωτής" (συμπεριλαμβανομένων των ηλικιωμένων, των παιδιών και των ατόμων με αναπηρία) καλύπτει τόσο τους καταναλωτές όσο και τους δυνητικούς καταναλωτές. Τα καταναλωτικά προϊόντα μπορεί να είναι εφάπαξ αγορές ή μακροπρόθεσμες συμβάσεις ή υποχρεώσεις.

Σημείωση 2 στην καταχώριση: Ο όρος αυτός ισχύει μόνο για φυσικά πρόσωπα, όχι για νομικές οντότητες.

Σημείωση 3 στην καταχώριση: Περιουσία, προϊόντα ή υπηρεσίες (3.3 παραβίαση της ιδιωτικότητας) που αγοράστηκαν ή χρησιμοποιήθηκαν από καταναλωτές μπορούν να χρησιμοποιηθούν για επαγγελματικούς σκοπούς και όχι μόνο για ιδιωτικούς (π.χ. "Φέρτε τη δική σας συσκευή").

[ΠΗΓΗ: ISO/IEC Guide 14:2018, 3.2, τροποποιημένο – "ή αλλαγμένο" έχει αφαιρεθεί από τον ορισμό, Σημείωση 1 στην καταχώριση έχει τροποποιηθεί, έχουν προστεθεί οι Σημειώσεις 2 και 3 στην καταχώριση].

3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)
πληροφορίες οι οποίες α) μπορούν να χρησιμοποιηθούν για την σύνδεση μεταξύ των πληροφοριών και του φυσικού προσώπου στο οποίο αναφέρονται οι πληροφορίες αυτές ή β) συνδέονται ή μπορούν να συνδεθούν άμεσα ή έμμεσα με φυσικό πρόσωπο

Σημείωση 1 στην καταχώριση: Για να προσδιοριστεί εάν ένα υποκείμενο των δεδομένων είναι αναγνωρίσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα που μπορούν ευλόγως να χρησιμοποιηθούν από τον ενδιαφερόμενο για την ιδιωτικότητα που κατέχει τα δεδομένα, ή από οποιοδήποτε άλλο μέρος, για να διαπιστωθεί η σχέση μεταξύ του συνόλου των ΔΠΧ και του φυσικού προσώπου.

Σημείωση 2 στην καταχώριση: Ο εκτελών επεξεργασία ΔΠΧ ενός δημόσιου νέφους (3.18 κίνδυνος παραβίασης ιδιωτικότητας (privacy risk)) δεν είναι συνήθως σε θέση να γνωρίζει ρητά εάν οι πληροφορίες που επεξεργάζεται εμπίπτουν σε κάποια συγκεκριμένη κατηγορία, εκτός εάν αυτό καθίσταται διαφανές από τον πελάτη της υπηρεσίας νέφους.

[ΠΗΓΗ: ISO/IEC 19944-1:2020, 3.3.1, τροποποιημένο – Ο παραδεκτός όρος έχει διαγραφεί, η σημείωση 1 στην καταχώριση και η σημείωση 2 στην καταχώριση έχουν συντομευτεί.]

3.3 παραβίαση της ιδιωτικότητας (privacy breach)
κατάσταση κατά την οποία τα δεδομένα προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)) υποβάλλονται σε επεξεργασία κατά παράβαση μιας ή περισσότερων σχετικών απαιτήσεων διασφάλισης της ιδιωτικότητας (3.9 απαίτηση (requirement))

[ΠΗΓΗ: ISO/IEC 29100:2011, 2.13]

3.4 υπηρεσία (service)
παραγωγή ενός οργανισμού με τουλάχιστον μία δραστηριότητα που εκτελείται αναγκαστικά μεταξύ του οργανισμού και του καταναλωτή (3.1 καταναλωτής (consumer))

Σημείωση 1 στην καταχώριση: Τα κυρίαρχα στοιχεία μιας υπηρεσίας είναι γενικά άυλα.

Σημείωση 2 στην καταχώριση: Μια υπηρεσία συχνά περιλαμβάνει δραστηριότητες κατά τη διεπαφή με τον καταναλωτή για τον καθορισμό των απαιτήσεων του καταναλωτή (3.9 απαίτηση (requirement)), καθώς και κατά την παροχή της υπηρεσίας και μπορεί να περιλαμβάνει μια συνεχή σχέση, όπως τράπεζες, λογιστήρια ή δημόσιους οργανισμούς, π.χ. σχολεία ή νοσοκομεία.

Σημείωση 3 στην καταχώριση: Η παροχή μιας υπηρεσίας μπορεί να περιλαμβάνει, για παράδειγμα, τα εξής:

— μια δραστηριότητα που εκτελείται σε ένα υλικό προϊόν που παρέχεται από τον καταναλωτή (π.χ. ένα αυτοκίνητο προς επισκευή),

— μια δραστηριότητα που εκτελείται σε ένα άυλο προϊόν που παρέχεται από τον καταναλωτή (π.χ. η κατάσταση εισοδήματος που απαιτείται για την προετοιμασία μιας φορολογικής δήλωσης),

— η παράδοση ενός άυλου προϊόντος (π.χ. η παράδοση πληροφοριών στο πλαίσιο της μετάδοσης γνώσεων),

— τη δημιουργία περιβάλλοντος για τον πελάτη (π.χ. σε ξενοδοχεία και εστιατόρια).

Σημείωση 4 στην καταχώριση: Μια υπηρεσία γενικά βιώνεται από τον καταναλωτή.

[ΠΗΓΗ: ISO 9000:2015, 3.7.7, τροποποιημένο - ο όρος "πελάτης" έχει αντικατασταθεί με τον όρο "καταναλωτής".]

3.5 απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό (privacy by design)
μεθοδολογίες σχεδιασμού στις οποίες η ιδιωτικότητα λαμβάνεται υπόψη και ενσωματώνεται στο αρχικό στάδιο σχεδιασμού και καθ' όλη τη διάρκεια του κύκλου ζωής των προϊόντων, διαδικασιών ή υπηρεσιών (3.3 παραβίαση της ιδιωτικότητας (privacy breach)) που περιλαμβάνουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information) ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)), συμπεριλαμβανομένης της απόσυρσης του προϊόντος (3.15 απόσυρση (retirement)) και την πιθανή διαγραφή (3.26 διαγραφή (deletion)) κάθε δεδομένων προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information) ΔΠΧ (PII)
προσωπικά δεδομένα (personal information))

Σημείωση 1 στην καταχώριση: Ο κύκλος ζωής περιλαμβάνει επίσης αλλαγές ή ενημερώσεις.

3.6 ενδιαφερόμενο μέρος (interested party)
εμπλεκόμενος ή δικαιούχος (stakekolder)
πρόσωπο, ομάδα ατόμων ή οργανισμός που έχει συμφέρον, μπορεί να επηρεάσει, να επηρεαστεί ή να θεωρήσει ότι επηρεάζεται από μια απόφαση ή δραστηριότητα

3.7 ρύθμιση απορρήτου που μπορεί να ρυθμιστεί από τον καταναλωτή (consumer-configurable privacy setting)
ρύθμιση απορρήτου του καταναλωτή (consumer privacy setting)
συγκεκριμένες επιλογές του υποκειμένου των δεδομένων (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)) σχετικά με τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για συγκεκριμένο σκοπό

[ΠΗΓΗ: ISO/IEC 29100:2011, 2.17, τροποποιημένο – Διαγραφή προτιμώμενου όρου, προσθήκη νέων προτιμώμενων και παραδεκτών όρων.]

3.8 επεξεργασία δεδομένων προσωπικού χαρακτήρα (processing of personally identifiable information)
επεξεργασία ΔΠΧ (processing of PII)
λειτουργία ή σύνολο λειτουργιών που εκτελούνται σε δεδομένα προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information))

Σημείωση 1 στην καταχώριση: Παραδείγματα πράξεων επεξεργασίας περιλαμβάνουν, μεταξύ άλλων, τη συλλογή, αποθήκευση, τροποποίηση, ανάκτηση, διαβούλευση, κοινοποίηση, ανωνυμοποίηση, ψευδωνυμοποίηση, διάδοση ή τη διάθεση, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα.

[ΠΗΓΗ: ISO/IEC 29100:2011, 2.23]

3.9 απαίτηση (requirement)
δήλωση που μεταφράζει ή εκφράζει μια ανάγκη και τους συναφείς περιορισμούς (3.7 ρύθμιση απορρήτου που μπορεί να ρυθμιστεί από τον καταναλωτή (consumer-configurable privacy setting)
ρύθμιση απορρήτου του καταναλωτή (consumer privacy setting)) και προϋποθέσεις (3.10 συνθήκη (condition)) με σαφήνεια

Σημείωση 1 στην καταχώριση: Απαιτήσεις υπάρχουν σε διαφορετικά επίπεδα στη δομή του συστήματος.

Σημείωση 2 στην καταχώριση: Μια απαίτηση πάντα σχετίζεται με το σύστημα, το λογισμικό ή την υπηρεσία (3.4 υπηρεσία (service)), ή άλλο στοιχείο ενδιαφέροντος.

[ΠΗΓΗ: ISO/IEC/IEEE 29148:2018, 3.1.19, τροποποιημένο – στον ορισμό έχει προστεθεί η φράση "με σαφήνεια", έχει διαγραφεί η σημείωση 2 στην καταχώριση και η σημείωση 3 στην καταχώριση είναι τώρα η σημείωση 2 στην καταχώριση.]

3.10 συνθήκη (condition)
μετρήσιμο ποιοτικό ή ποσοτικό χαρακτηριστικό (3.11 χαρακτηριστικό (attribute)) που προβλέπεται για μια απαίτηση (3.9 απαίτηση (requirement)) και υποδεικνύει μια περίσταση ή ένα γεγονός κάτω από το οποίο εφαρμόζεται μια απαίτηση

[ΠΗΓΗ: ISO/IEC/IEEE 29148:2018, 3.1.6]

3.11 χαρακτηριστικό (attribute)
εγγενής ιδιότητα ή χαρακτηριστικό μιας οντότητας που μπορεί να διακριθεί ποσοτικά ή ποιοτικά με ανθρώπινα ή αυτοματοποιημένα μέσα

Σημείωση 1 στην καταχώριση: Το ISO 9000 διακρίνει δύο τύπους χαρακτηριστικών: ένα μόνιμο χαρακτηριστικό που υπάρχει εγγενώς σε κάτι – και ένα καθορισμένο χαρακτηριστικό ενός προϊόντος, μιας διαδικασίας ή ενός συστήματος (π.χ. η τιμή ενός προϊόντος, ο ιδιοκτήτης ενός προϊόντος). Το καθορισμένο χαρακτηριστικό δεν είναι εγγενές ποιοτικό χαρακτηριστικό του εν λόγω προϊόντος, της διαδικασίας ή του συστήματος.

[ΠΗΓΗ: ISO/IEC 25000:2014, 4.1, τροποποιημένο – Η σημείωση 1 στην καταχώριση έχει αφαιρεθεί – η σημείωση 2 στην καταχώριση έχει γίνει σημείωση 1 στην καταχώριση].

3.12 τρίτο μέρος (third party)
πρόσωπο ή φορέας που είναι ανεξάρτητος από τον οργανισμό (3.1 καταναλωτής (consumer))

Σημείωση 1 στην καταχώριση: Όλοι οι επιχειρηματικοί συνεργάτες είναι τρίτα μέρη, αλλά δεν είναι όλοι τα τρίτα μέρη επιχειρηματικοί συνεργάτες.

Σημείωση 2 στην καταχώριση: Ένα τρίτο μέρος μπορεί να είναι υπεύθυνος επεξεργασίας δεδομένων προσωπικού χαρακτήρα (3.19 υπεύθυνος επεξεργασίας δεδομένων προσωπικού χαρακτήρα (personally identifiable information controller)
υπεύθυνος επεξεργασίας ΔΠΧ (PII controller)) ή ο εκτελών επεξεργασίας δεδομένων προσωπικού χαρακτήρα (3.20 εκτελών την επεξεργασία δεδομένων προσωπικού χαρακτήρα (personally identifiable information processor)
εκτελών επεξεργασία ΔΠΧ (PII processor)) ή και τα δύο, ανάλογα με το πλαίσιο.

3.13 προϊόν καταναλωτή (consumer product)
αγαθό ή υπηρεσία που έχει σχεδιαστεί και παραχθεί κυρίως για προσωπική ή οικιακή χρήση, αλλά όχι μόνο, συμπεριλαμβανομένων των συστατικών του, των εξαρτημάτων, των οδηγιών και της συσκευασίας του

[ΠΗΓΗ: ISO 10377:2013, 2.2, τροποποιημένο]

3.14 κύκλος ζωής δεδομένων προσωπικού χαρακτήρα (personally identifiable information cycle)
κύκλος ζωής ΔΠΧ (PII lifecycle)
ακολουθία γεγονότων από τη δημιουργία ή την προέλευση, τη συλλογή, την αποθήκευση, τη χρήση και τη διαβίβαση έως την τελική απόρριψη (π.χ. ασφαλή καταστροφή) των δεδομένων προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)).

3.15 απόσυρση (retirement)
λήξη της ενεργού υποστήριξης λειτουργίας και συντήρησης από τον οργανισμό, μερική ή ολική αντικατάσταση από νέο σύστημα ή εγκατάσταση αναβαθμισμένου συστήματος

Σημείωση 1 στην καταχώριση: Αυτό μπορεί να περιλαμβάνει το να τεθεί ένα σύστημα εκτός λειτουργίας, την παύση της εμπορίας, της πώλησης ή της παροχής ανταλλακτικών, υπηρεσιών ή ενημερώσεων λογισμικού για το προϊόν.

[ΠΗΓΗ: ISO/IEC/IEEE 15288:2015, 4.1.39, τροποποιημένο - Προστέθηκε η σημείωση 1 στην καταχώρηση]

3.16 αντίμετρο ιδιωτικότητας (privacy control)
μέτρο που αντιμετωπίζει τους κινδύνους παραβίασης ιδιωτικότητας (3.18 κίνδυνος παραβίασης ιδιωτικότητας (privacy risk)) μειώνοντας την πιθανότητα ή τις συνέπειές τους

Σημείωση 1 στην καταχώριση: Τα αντίμετρα ιδιωτικότητας περιλαμβάνουν οργανωτικά, φυσικά και τεχνικά μέτρα, π.χ. πολιτικές, διαδικασίες, οδηγίες, νομικές συμβάσεις, πρακτικές διαχείρισης, πρωτόκολλα και τεχνικές ελαχιστοποίησης δεδομένων ή οργανωτικές δομές.

Σημείωση 2 στην καταχώριση: Αντίμετρο χρησιμοποιείται επίσης ως συνώνυμο της λέξης "διασφάλιση" και “μέτρο προστασίας”.

[ΠΗΓΗ: ISO/IEC 29100:2011, τροποποιημένο – Σημείωση 1 στην καταχώριση τροποποιήθηκε].

3.17 ασφάλεια πληροφοριών (information security)
διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών

Σημείωση 1 στην καταχώριση: Επιπλέον, μπορεί να εμπλέκονται και άλλες ιδιότητες, όπως η αυθεντικότητα, η λογοδοσία, η μη-αποποίηση και η αξιοπιστία.

[ΠΗΓΉ: ISO/IEC 27000:2018, 3.28]

3.18 κίνδυνος παραβίασης ιδιωτικότητας (privacy risk)
επίδραση της αβεβαιότητας στην ιδιωτικότητα

Σημείωση 1 στην καταχώριση: Η αβεβαιότητα είναι η κατάσταση, έστω και μερικής, ανεπάρκειας πληροφοριών που σχετίζονται με, την κατανόηση ή τη γνώση, ενός γεγονότος, της συνέπειας ή της πιθανότητάς του.

Σημείωση 2 στην καταχώριση: κίνδυνος παραβίασης ιδιωτικότητας μπορεί να είναι η κατάχρηση δεδομένων προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)) ή ο κίνδυνος οι καταναλωτές να (3.1 καταναλωτής (consumer)) βιώσουν δυσμενείς συνέπειες που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

[ΠΗΓΗ: ISO/IEC 29100:2011, 2.19, τροποποιημένο – Η σημείωση 1 στην καταχώριση έχει διαγραφεί, η σημείωση 2 στην καταχώριση έχει προστεθεί.]

3.19 υπεύθυνος επεξεργασίας δεδομένων προσωπικού χαρακτήρα (personally identifiable information controller)
υπεύθυνος επεξεργασίας ΔΠΧ (PII controller)
ενδιαφερόμενο μέρος (ή ενδιαφερόμενα μέρη) που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)) εκτός από τα φυσικά πρόσωπα που χρησιμοποιούν τα δεδομένα για προσωπικούς σκοπούς

[ΠΗΓΗ: ISO/IEC 29100:2011, 2.10, τροποποιημένη - Η σημείωση στην καταχώριση έχει αφαιρεθεί.]

3.20 εκτελών την επεξεργασία δεδομένων προσωπικού χαρακτήρα (personally identifiable information processor)
εκτελών επεξεργασία ΔΠΧ (PII processor)
Ενδιαφερόμενο μέρος που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)) για λογαριασμό και σύμφωνα με τις οδηγίες ενός υπεύθυνου επεξεργασίας ΔΠΧ (3.19 υπεύθυνος επεξεργασίας δεδομένων προσωπικού

χαρακτήρα (personally identifiable information controller)
υπεύθυνος επεξεργασίας ΔΠΧ (PII controller))

[ΠΗΓΗ: ISO/IEC 29100:2011, 2.12]

3.21 ανθρωποκεντρικός σχεδιασμός (human-centered design)
προσέγγιση του σχεδιασμού και της ανάπτυξης συστημάτων που αποσκοπεί στο να καταστήσει τα διαδραστικά συστήματα πιο εύχρηστα, εστιάζοντας στη χρήση του συστήματος από τον άνθρωπο – εφαρμογή γνώσεων και τεχνικών ανθρώπινων παραγόντων, εργονομίας και ευχρηστίας

Σημείωση 1 στην καταχώρηση: Ο όρος "ανθρωποκεντρικός σχεδιασμός" χρησιμοποιείται αντί του όρου "σχεδιασμός με τον καταναλωτή στο κέντρο" για να τονιστεί ότι ο σχεδιασμός επηρεάζει έναν αριθμό ενδιαφερομένων, όχι μόνο αυτούς που συνήθως θεωρούνται καταναλωτές (3.1 καταναλωτής (consumer)). Ωστόσο, στην πράξη, συχνά χρησιμοποιούνται συνώνυμα.

Σημείωση 2 στην καταχώριση: Τα εύχρηστα συστήματα μπορούν να προσφέρουν μια σειρά από οφέλη, όπως βελτιωμένη παραγωγικότητα, αυξημένη ευημερία των καταναλωτών, αποφυγή του άγχους, αυξημένη προσβασιμότητα και μειωμένο κίνδυνο βλάβης.

[ΠΗΓΗ: ISO/IEC 25063:2014, 3.6, τροποποιημένο – Η σημείωση 1 στην καταχώριση έχει τροποποιηθεί.]

3.22 περίπτωση χρήσης (use case)
περιγραφή μιας αλληλουχίας αλληλεπιδράσεων ενός καταναλωτή (3.1 καταναλωτής (consumer)) και ενός καταναλωτικού προϊόντος που χρησιμοποιείται για να βοηθήσει στον εντοπισμό, την αποσαφήνιση και την οργάνωση των απαιτήσεων (3.9 απαίτηση (requirement)) για την υποστήριξη ενός συγκεκριμένου επιχειρηματικού στόχου

Σημείωση 1 στην καταχώρηση: Οι καταναλωτές μπορεί να είναι χρήστες, μηχανικοί, συστήματα.

[ΠΗΓΗ: ISO/TR 14872:2019, 3.9, τροποποιημένο – Ο όρος "χρήστης" έχει αλλάξει σε "καταναλωτής", ο όρος "σύστημα" έχει αλλάξει σε "καταναλωτικό προϊόν" και έχει προστεθεί σημείωση στην καταχώριση].

3.23 ευπάθεια του καταναλωτή (consumer vulnerability)
κατάσταση κατά την οποία ένα άτομο μπορεί να βρεθεί σε μειονεκτική θέση ή να κινδυνεύσει να υποστεί ζημία κατά τη διάρκεια της αλληλεπίδρασής του με έναν πάροχο υπηρεσιών λόγω της παρουσίας προσωπικών, περιστασιακών και περιβαλλοντικών παραγόντων της αγοράς

Σημείωση 1 στην καταχώρηση: Οποιοσδήποτε μπορεί να είναι ευάλωτος οποιαδήποτε στιγμή. Η ευπάθεια μπορεί να είναι προσωρινή ή μόνιμη.

Σημείωση 2 στην καταχώρηση: Οι παράγοντες που συμβάλλουν στην ευπάθεια του καταναλωτή μπορεί να είναι προσωπικοί (π.χ. υγεία, ασθένεια, τραυματισμοί, αναπηρία, βλάβη) ή περιστασιακοί (π.χ. απώλεια εργασίας, πένθος, χαμηλό επίπεδο μόρφωσης).

Σημείωση 3 στην καταχώριση: Οι διεργασίες και οι διαδικασίες ενός οργανισμού μπορούν να μειώσουν ή να επιδεινώσουν την ευπάθεια του καταναλωτή.

Σημείωση 4 στην καταχώριση: Ένας καταναλωτής όταν είναι ευάλωτος μπορεί να:

— διατρέχει μεγαλύτερο κίνδυνο να βιώσει αρνητικά αποτελέσματα κατά την αλληλεπίδραση με τους παρόχους υπηρεσιών,

— έχει περιορισμένη ικανότητα να μεγιστοποιήσουν την ευημερία τους,

— δυσκολεύεται να λάβει ή να αφομοιώσει πληροφορίες,

— να είναι λιγότερο σε θέση να αγοράζει, να επιλέγει ή να έχει πρόσβαση σε κατάλληλες υπηρεσίες,

— να είναι πιο επιρρεπείς σε ορισμένες πρακτικές μάρκετινγκ

Σημείωση 5 στην καταχώριση: Περιβαλλοντικοί παράγοντες της αγοράς μπορεί να περιλαμβάνουν δημογραφικούς παράγοντες, περιβαλλοντικούς παράγοντες, οικονομικούς παράγοντες, κοινωνικο-πολιτισμικούς παράγοντες, πολιτικούς και νομικούς παράγοντες, διεθνές περιβάλλον, τεχνολογικούς παράγοντες.

[ΠΗΓΗ: ISO/IEC Guide 76:2020, 3.14, τροποποιημένο - Προστέθηκε η σημείωση 5 στην καταχώριση.]

3.24 φυσικό πρόσωπο που λογοδοτεί (accountable person)
ορισμένο πρόσωπο για την ορθή και εμπεριστατωμένη ολοκλήρωση ενός συγκεκριμένου παραδοτέου ή καθήκοντος, το οποίο διασφαλίζει ότι πληρούνται οι προϋποθέσεις του καθήκοντος, το οποίο αναθέτει την εργασία στο υπεύθυνο μέρος (3.25 υπεύθυνο μέρος (responsible party)) και υπογράφει (εγκρίνει) την εργασία του υπεύθυνου μέρους

3.25 υπεύθυνο μέρος (responsible party)
πρόσωπο ή πρόσωπα που ολοκληρώνουν μια ανατεθείσα εργασία ή ένα καθορισμένο παραδοτέο

Σημείωση 1 στην καταχώριση: Το υπεύθυνο μέρος μπορεί να είναι ένας ρόλος ή ένας μοιρασμένος ρόλος, αν και μπορεί να ανατεθεί σε άλλους να συνδράμουν στις απαιτούμενες εργασίες.

3.26 διαγραφή (deletion)
διαδικασία με την οποία τα δεδομένα προσωπικού χαρακτήρα (ΔΠΧ) (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)

ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)) αλλάζουν με τέτοιον τρόπο ώστε να μην είναι πλέον παρόντα, αναγνωρίσιμα ή αξιοποιήσιμα και να μπορούν να ανακατασκευαστούν μόνο με υπερβολική προσπάθεια

Σημείωση 1 στην καταχώριση: Ο όρος "διαγραφή" καλύπτει τα εξής: μηχανισμός απόσυρσης, διαγραφή, καταστροφή, καταστροφή μέσων αποθήκευσης δεδομένων.

Σημείωση 2 στην καταχώριση: Ο όρος "διαγραφή" αναφέρεται στην εξάλειψη των μοτίβων bit ή σε ανάλογες πρακτικές και όχι στην απλή σήμανση ή μετακίνηση των δεδομένων προς απόκρυψη. Κατά συνέπεια, θα απαιτηθεί υπερβολική προσπάθεια για την αναδημιουργία των ΔΠΧ, λαμβανομένων υπόψη όλων των μέσων που πιθανόν εύλογα να χρησιμοποιηθούν, π.χ. διαθέσιμο τεχνολογικό επίπεδο, ανθρώπινοι και τεχνικοί πόροι, κόστος και χρόνος.

Σημείωση 3 στην καταχώριση: Για την επιλογή των μεθόδων διαγραφής, πρέπει να λαμβάνεται υπόψη μια προσέγγιση με βάση τον κίνδυνο, συμπεριλαμβανομένης της ευαισθησίας των ΔΠΧ και της πιθανής χρήσης εγκληματολογικών εργαλείων. Τα απαιτούμενα μέτρα ενδέχεται να αλλάξουν με την πάροδο του χρόνου, ανάλογα με την κατάσταση της τεχνολογίας και άλλους παράγοντες.

Σημείωση 4 στην καταχώριση: Τα ΔΠΧ μπορεί επίσης να αλλάξουν με την εφαρμογή μη αναστρέψιμων τεχνικών από-ταυτοποίησης. Τέτοια δεδομένα συχνά είναι εκτός της νομοθεσίας για την ιδιωτικότητα.

Σημείωση 5 στην καταχώριση: Τεχνικές απο-ταυτοποίησης μπορούν να βρεθούν στο ISO/IEC 20889.

3.27 αξιολόγηση κινδύνου παραβίασης της ιδιωτικότητας (privacy risk assessment)
συνολική διαδικασία εντοπισμού, ανάλυσης, αξιολόγησης, διάθεσης, επικοινωνίας και σχεδιασμού της αντιμετώπισης και του μετριασμού της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (3.2 αναγνωριστικά στοιχεία ταυτότητας / δεδομένα προσωπικού χαρακτήρα (personally identifiable information)
ΔΠΧ (PII)
προσωπικά δεδομένα (personal information)), η οποία εντάσσεται στο ευρύτερο πλαίσιο διαχείρισης κινδύνων ενός οργανισμού

Σημείωση 1 στην καταχώριση: Η διαδικασία αυτή μπορεί να τεκμηριώνεται με διάφορους τρόπους, μεταξύ άλλων με μια εκτίμηση αντικτύπου ιδιωτικότητας.

[ΠΗΓΗ: ISO/IEC 29100:2011/Amd.1:2018, 2.20, τροποποιημένο – Ο παραδεκτός όρος "εκτίμηση αντικτύπου ιδιωτικότητας " έχει αφαιρεθεί και έχει προστεθεί η σημείωση 1 στην καταχώριση].

3.28 τεκμηριωμένες πληροφορίες (documented information)
πληροφορίες που πρέπει να ελέγχονται και να διατηρούνται από έναν οργανισμό και το μέσο στο οποίο περιέχονται

Σημείωση 1 στην καταχώριση: Η τεκμηριωμένη πληροφορία μπορεί να έχει οποιαδήποτε μορφή και μέσο και να προέρχεται από οποιαδήποτε πηγή.

Σημείωση 2 στην καταχώριση: Οι τεκμηριωμένες πληροφορίες μπορούν να αναφέρονται:

— στο σύστημα διαχείρισης, συμπεριλαμβανομένων των σχετικών διαδικασιών,

— πληροφορίες που δημιουργούνται προκειμένου να λειτουργήσει ο οργανισμός (εγχειρίδια),

— αποδεικτικά στοιχεία για τα αποτελέσματα που επιτεύχθηκαν (αρχεία ιστορικού).

[ΠΗΓΗ: ISO/IEC 27000:2018, 3.19]

3.29 διοίκηση της ασφάλειας των πληροφοριών (information security management)
διαχείριση της διατήρησης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών

[ΠΗΓΗ: ISO/IEC TR 27016:2014, 3.12]

3.30 ευπαθής καταναλωτής (vulnerable consumer)
καταναλωτής (3.1 καταναλωτής (consumer)) ο οποίος θα μπορούσε να διατρέχει μεγαλύτερο κίνδυνο βλάβης από τα προϊόντα λόγω, για παράδειγμα, της ηλικίας του, του επιπέδου εκπαίδευσής του (συμπεριλαμβανομένου του τεχνολογικού αλφαβητισμού), της φυσικής του κατάστασης ή των περιορισμών του ή της αδυναμίας πρόσβασης σε πληροφορίες για την ασφάλεια των προϊόντων και ο οποίος θα μπορούσε να είναι μόνιμα ή προσωρινά ανίκανος να εκπροσωπήσει τα συμφέροντά του, για παράδειγμα, λόγω νοητικής, συναισθηματικής, κοινωνικής ή φυσικής αιτίας που μπορεί να περιορίσει την ικανότητά του να λαμβάνει εκούσιες και τεκμηριωμένες αποφάσεις

3.31 διαχείριση αλλαγών (change management)
συνετή χρήση μέσων για την πραγματοποίηση μιας αλλαγής ή μιας προτεινόμενης αλλαγής σε ένα προϊόν ή μια υπηρεσία

[ΠΗΓΗ: ISO/IEC/IEEE 24765:2017]

3.32 υποκείμενο των δεδομένων (personally identifiable principal)
φυσικό πρόσωπο στο οποίο συσχετίζονται τα δεδομένα προσωπικού χαρακτήρα

[ΠΗΓΗ: ISO/IEC 29100:2011, τροποποιημένο – Σημείωση στην καταχώριση διαγράφηκε.]

3.33 τέλος χρήσης (end of use)
κατάσταση ενός προϊόντος που δεν χρησιμοποιείται πλέον από έναν καταναλωτή

Σημείωση 1 στην καταχώριση: Το τέλος της χρήσης μπορεί να συμβεί για πολλούς λόγους, όπως ενδεικτικά: το προϊόν έχει χαλάσει, δεν λειτουργεί πλέον σωστά, δεν ικανοποιεί πλέον την απαίτηση (3.9 απαίτηση (requirement)) του καταναλωτή (3.1 καταναλωτής (consumer)), ο καταναλωτής έχει αποβιώσει ή είναι ανίκανος, το προϊόν έχει ανακυκλωθεί ή καταστραφεί ή ο καταναλωτής έχει μεταβιβάσει το προϊόν σε άλλους καταναλωτές μέσω δώρων ή αγορών μεταχειρισμένων προϊόντων.

3.34 κυβερνοασφάλεια (cybersecurity)
προστασία ενός συστήματος IT από επιθέσεις ή ζημίες στο υλικό, το λογισμικό ή τις πληροφορίες του, καθώς και από τη διακοπή ή την παρεμπόδιση των υπηρεσιών (3.3 παραβίαση της ιδιωτικότητας (privacy breach)) που παρέχει

[ΠΗΓΗ: ISO/TR 22100-4:2018, 3.10, τροποποιημένο – Ο προτιμώμενος όρος "Ασφάλεια Τεχνολογίας Πληροφοριών" έχει διαγραφεί].

3.35 κίνδυνος (risk)
επίδραση της αβεβαιότητας στους στόχους

[ΠΗΓΗ: ISO/IEC Guide 73:2009, 1.1, τροποποιημένο – Διαγράφηκαν οι σημειώσεις στην καταχώριση].

4 Γενικά

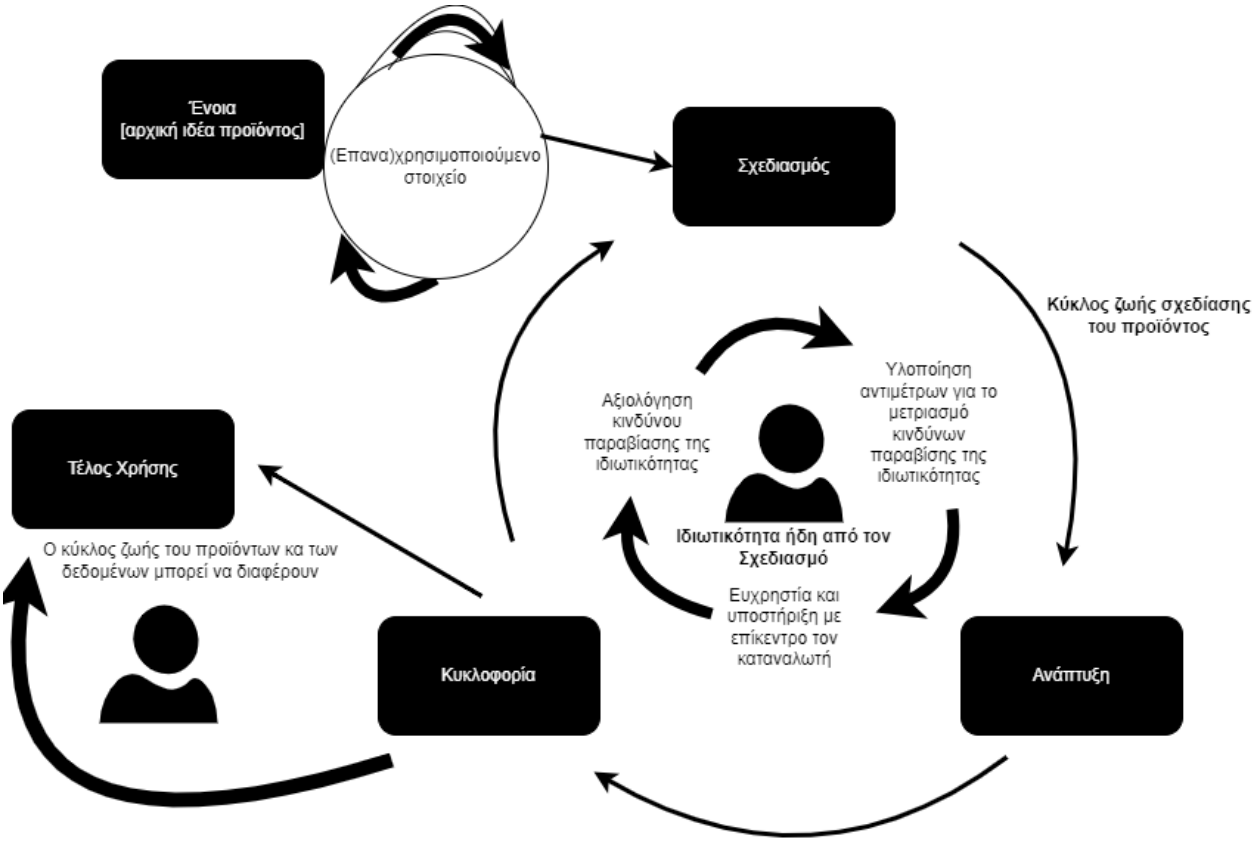
4.1 Επισκόπηση
Προκειμένου να εφαρμοστεί και να τηρηθεί η αρχή απαιτήσεων ιδιωτικότητας ήδη από τον σχεδιασμό για καταναλωτικά προϊόντα, υπάρχουν απαιτήσεις που πρέπει να πληρούν όσοι εμπλέκονται ή συμβάλλουν στο σχεδιασμό, την πώληση ή τη διαχείριση καταναλωτικών προϊόντων που επεξεργάζονται τα ΔΠΧ καθ' όλη τη διάρκεια του κύκλου ζωής τους. Τα δικαιώματα και οι προτιμήσεις των καταναλωτών όσον αφορά την ιδιωτικότητα μπορούν να διαδραματίσουν σημαντικό και ενημερωτικό ρόλο κατά τον καθορισμό των απαιτήσεων της ιδιωτικότητας για το καταναλωτικό προϊόν.

Τα ΔΠΧ έχουν κύκλο ζωής, από τη δημιουργία ή την προέλευση, τη συλλογή, την αποθήκευση, τη χρήση και τη μεταφορά μέχρι την τελική τους διάθεση (π.χ. ασφαλή καταστροφή). Η αξία των ΔΠΧ και οι σχετικοί κίνδυνοι για τον καταναλωτή μπορεί να ποικίλλουν κατά τη διάρκεια του κύκλου ζωής των ΔΠΧ, αλλά η προστασία του καταναλωτή παραμένει σημαντική σε όλα τα στάδια και σε όλα τα πλαίσια του κύκλου ζωής τους.

Τα πληροφοριακά συστήματα (information systems) έχουν επίσης κύκλους ζωής εντός των οποίων σχεδιάζονται, προδιαγράφονται, σχεδιάζονται, αναπτύσσονται, δοκιμάζονται, υλοποιούνται, χρησιμοποιούνται, συντηρούνται και τελικά αποσύρονται από την υπηρεσία και απορρίπτονται. Η προστασία των ΔΠΧ μπορεί επίσης να ληφθεί υπόψη σε καθένα από αυτά τα στάδια. Οι εξελίξεις νέων συστημάτων και οι αλλαγές σε υφιστάμενα συστήματα παρέχουν

ευκαιρίες στους οργανισμούς να ανανεώσουν και να βελτιώσουν την ιδιωτικότητα και τα σχετικά αντίμετρα ασφαλείας. Αυτό μπορεί να επιτευχθεί λαμβάνοντας υπόψη τους τρέχοντες και προβλεπόμενους κινδύνους για την ιδιωτικότητα και την ασφάλεια των πληροφοριών και τα πραγματικά περιστατικά σε περίπτωση που προκύψουν [8].

Όπως απεικονίζεται στο Εικόνα 1, ο κύκλος ζωής των ΔΠΧ και ο κύκλος ζωής του προϊόντος δεν είναι ακριβώς το ίδιο. Ο κύκλος ζωής του προϊόντος αρχίζει με την έναρξη ή την ιδέα ενός προϊόντος και τελειώνει με την καταστροφή ή την απόρριψη του προϊόντος. Αυτό μπορεί να συμβεί ακόμη και μετά τη λήξη της υποστήριξης του προϊόντος και αφού ο καταναλωτής έχει αποσύρει το προϊόν. Το "τόξο" του κύκλου ζωής των ΔΠΧ εκτείνεται από τη δημιουργία ή τη συλλογή των ΔΠΧ από ένα προϊόν έως την καταστροφή ή τη απόρριψή του. Μερικές φορές ο κύκλος ζωής των ΔΠΧ εκτείνεται πέρα από τον κύκλο ζωής του προϊόντος. Για να σχεδιαστεί ένα προϊόν με γνώμονα την ιδιωτικότητα, οι σχεδιαστές του πρέπει να κατανοήσουν και τους δύο κύκλους ζωής για το υπό σχεδιασμό προϊόν και τις απαιτήσεις και για αυτούς που προστατεύουν την ιδιωτικότητα και τα ΔΠΧ των καταναλωτών του προϊόντος και όσων αλληλεπιδρούν με αυτό καθ' όλη τη διάρκεια και των δύο κύκλων ζωής.



Εικόνα 1 - Κύκλος ζωής δεδομένων προσωπικού χαρακτήρα και προϊόντος

4.2 Σχεδιασμός δυνατοτήτων που θα επιτρέπουν στους καταναλωτές να επιβάλλουν τα δικαιώματά τους στην ιδιωτικότητα

4.2.1 Απαίτηση

Ο οργανισμός θα πρέπει να εφαρμόζει τα μέσα με τα οποία ο καταναλωτής μπορεί να ασκήσει τα δικαιώματα και τα προνόμιά του για την ιδιωτικότητα.

ΣΗΜΕΙΩΣΗ 1 Τα μέσα μπορούν να περιλαμβάνουν, αλλά δεν περιορίζονται: στο σχεδιασμό, τα χαρακτηριστικά, τη λειτουργία των αντιμέτρων, την αποδεδειγμένη αποτελεσματικότητα του προϊόντος .

ΣΗΜΕΙΩΣΗ 2 Προϋποτίθεται ότι αυτό γίνεται σύμφωνα με τους σχετικούς κανονισμούς και απαιτήσεις όπου πωλείται ή διανέμεται το καταναλωτικό προϊόν.

4.2.2 Επεξήγηση

Πολλές αποφάσεις σχετικά με τα ΔΠΧ των καταναλωτών δεν ανήκουν αποκλειστικά στον οργανισμό. Οι αποφάσεις σχετικά με τα ΔΠΧ διέπονται από νόμους ή κανονισμούς, από πολιτιστικά πρότυπα, από μονομερή πολιτική, από συμβάσεις, από οικονομικά κριτήρια ή από τεχνικούς ελέγχους που εφαρμόζουν την ατομική συγκατάθεση και τις προσωπικές προτιμήσεις (βλ. 4.3.1 Απαίτηση) [9] [10] [11] [12] [13] [14] [15]

Η χρήση του προϊόντος από τους καταναλωτές συνεπάγεται επίσης υποχρεώσεις για τον οργανισμό όσον αφορά τον σεβασμό των δικαιωμάτων του καταναλωτή στην ιδιωτικότητα. Τα δικαιώματα της ιδιωτικότητας περιλαμβάνουν, για παράδειγμα, τον ατομικό έλεγχο των ΔΠΧ, την παροχή ή ανάκληση συγκατάθεσης, τη λήψη πληροφοριών μέσω ειδοποιήσεων για την ιδιωτικότητα, επεξηγηματικών κειμένων ή άλλης τεκμηρίωσης, πρόσβαση στα ΔΠΧ, φορητότητα, δικαιώματα διαγραφής και διόρθωσης των δεδομένων. Οι υποχρεώσεις αυτές μπορεί να είναι επαχθείς για τον οργανισμό ή μπορεί να σχεδιαστούν χωρίς ιδιαίτερο κόπο. Εάν ο οργανισμός δεν κατανοήσει το ρόλο του καταναλωτή στην εκπλήρωση των υποχρεώσεων αυτών, μπορεί να σπαταλήσει σημαντικούς πόρους, ενώ παράλληλα δεν θα έχει εκπληρώσει τις υποχρεώσεις του.

Λόγω της επίδρασής τους ή της δυνητικής επίδρασής τους στην ικανότητα του οργανισμού να παρέχει με συνέπεια προϊόντα που ανταποκρίνονται στις απαιτήσεις των καταναλωτών και στις ισχύουσες νομοθετικές και κανονιστικές απαιτήσεις, είναι σημαντικό να συμπεριληφθούν οι ανάγκες της ιδιωτικότητας των καταναλωτών στη διαδικασία εξέτασης των αναγκών των ενδιαφερόμενων μερών από τον οργανισμό. Η ενδυνάμωση των καταναλωτών περιλαμβάνει την ικανότητα να διαδραματίζουν συμμετοχικό ρόλο και να ασκούν αποτελεσματικά δικαιώματα σχετικά με την ιδιωτικότητα καθ' όλη τη διάρκεια του κύκλου ζωής των δικών τους ΔΠΧ που υποβάλλονται σε επεξεργασία από το προϊόν.

4.2.3 Οδηγία

α) Ο οργανισμός θα πρέπει να ακολουθεί ένα σύστημα διοίκησης πληροφοριών για την ιδιωτικότητα (privacy information management system).

ΣΗΜΕΙΩΣΗ Το ISO/IEC 27701 και το NIST Privacy Framework παρέχουν περισσότερες εξηγήσεις για την διοίκηση της ιδιωτικότητας [16] [17].

β) Ο οργανισμός θα πρέπει να προσδιορίσει τους παράγοντες που επηρεάζουν τα προϊόντα του σε σχέση με τα δικαιώματα των καταναλωτών στην ιδιωτικότητα. Οι παράγοντες αυτοί μπορεί να περιλαμβάνουν νομικές απαιτήσεις, πολιτισμικά πρότυπα, μονομερή πολιτική, συμβάσεις, οικονομικά και διαθέσιμη τεχνολογία. Κατά τον τρόπο αυτό, ο οργανισμός θα πρέπει να εμπλέξει εμπειρογνώμονες.

γ) Ο οργανισμός θα πρέπει να προσδιορίσει εάν εμπίπτει σε κάποιον κωδικοποιημένο ρόλο (π.χ. υπεύθυνος επεξεργασίας ΔΠΧ ή εκτελών την επεξεργασία ΔΠΧ), διότι οι ρόλοι αυτοί μπορεί να επιβάλλουν συγκεκριμένες νομικές υποχρεώσεις έναντι του καταναλωτή.

δ) Ο οργανισμός θα πρέπει να εφαρμόζει βέλτιστες πρακτικές και μέτρα προστασίας της ιδιωτικότητας και ασφάλειας στην αλυσίδα εφοδιασμού (supply chain), ώστε να επιτρέπει στους καταναλωτές να ασκούν τα δικαιώματα και τα προνόμιά τους.

ε) Η πρόσβαση σε ΔΠΧ, συμπεριλαμβανομένης της συλλογής και της επεξεργασίας, θα πρέπει να χορηγείται μόνο σε εξουσιοδοτημένο προσωπικό που έχει ανάγκη στο πλαίσιο του οργανισμού για τα δεδομένα, όπως καθορίζεται από τις πολιτικές ιδιωτικότητας.

ζ) Ο οργανισμός θα πρέπει να λαμβάνει υπόψη τη χρηστικότητα και τη συνολική εμπειρία του καταναλωτή όταν καθορίζει τόσο τα χαρακτηριστικά του προϊόντος όσο και τις απαιτήσεις της ιδιωτικότητας ήδη από τον σχεδιασμό.

η) Ο οργανισμός θα πρέπει να παρέχει μια πραγματικά κατατοπιστική δήλωση ιδιωτικότητας (privacy statement), η οποία να εξηγεί με σαφείς και απλούς όρους, μεταξύ άλλων, πώς ο καταναλωτής μπορεί να ασκήσει τα δικαιώματα για την ιδιωτικότητά του πριν το εφαρμοστέο προϊόν συλλέξει τα προσωπικά δεδομένα του καταναλωτή, βλ. ISO/IEC 29184 [18].

θ) Ένα καταναλωτικό προϊόν θα πρέπει να αποκτά πρόσβαση, να συλλέγει, να χρησιμοποιεί, να αποκαλύπτει, να μεταβιβάζει ή να αποθηκεύει μόνο τις ελάχιστες πληροφορίες που απαιτούνται για την παροχή, τη λειτουργία ή τη συντήρηση του προϊόντος, για την εκπλήρωση των προσδιορισμένων σκοπών του οργανισμού.

ι) Οι δεσμεύσεις της εταιρείας (π.χ. πολιτική απορρήτου [privacy policy] ή δημόσιες δηλώσεις [public statement]) θα πρέπει να επανεξετάζονται κατά τη διαμόρφωση των ρυθμίσεων απορρήτου των καταναλωτών σε νέα ή τροποποιημένα προϊόντα και να επικαιροποιούνται. Προϋποτίθεται ότι αυτή η επανεξέταση γίνεται για να εξασφαλιστεί ότι δεν υπάρχουν παραβιάσεις των υποχρεώσεων του οργανισμού προς τον καταναλωτή.

κ) Όταν ο καταναλωτής υποβάλλει ένα αίτημα, ο οργανισμός θα πρέπει να είναι σε θέση να εντοπίζει όλα τα σχετικά ΔΠΧ ενός καταναλωτή και να εκτελεί τις απαραίτητες ενέργειες (π.χ. πλήρη διαγραφή, εξαγωγή, περιορισμό, διόρθωση) με κλιμακούμενο, έγκαιρο και ασφαλή τρόπο.

λ) Μετά την απόσυρση του προϊόντος, ο οργανισμός θα πρέπει να επεξεργάζεται μόνο τα ελάχιστα ΔΠΧ που απαιτούνται για την επίτευξη των προσδιορισμένων σκοπών του οργανισμού και θα πρέπει να διαγράφει αμέσως και με ασφάλεια όλα τα ΔΠΧ που δεν χρειάζονται για την τήρηση των εν λόγω απαιτήσεων [19]. Προϋποτίθεται ότι οι εν λόγω σκοποί συνάδουν με τις ισχύουσες νομικές ή συμβατικές απαιτήσεις.

4.3 Ανάπτυξη δυνατότητας καθορισμού των προτιμήσεων του καταναλωτή για την ιδιωτικότητα (consumer privacy preferences)

4.3.1 Απαίτηση

Ο οργανισμός θα πρέπει να προσδιορίζει τις ανάγκες των καταναλωτών σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα από προϊόντα που έχουν σχεδιαστεί και αναπτυχθεί για τους καταναλωτές.

4.3.2 Επεξήγηση

Η επεξεργασία ΔΠΧ επιτρέπει τη λειτουργία του προϊόντος και την υποστήριξη του καταναλωτή από τον οργανισμό κατά τη διάρκεια του κύκλου ζωής του προϊόντος. Εάν ο οργανισμός δεν έχει σαφή άποψη για τις προτιμήσεις των καταναλωτών όσον αφορά την ιδιωτικότητα, θα είναι δύσκολο να σχεδιάσει το προϊόν ώστε να ανταποκρίνεται στις προτιμήσεις αυτές με τρόπο που να προστατεύει την ιδιωτικότητα του καταναλωτή και να επιτρέπει στον οργανισμό να εκπληρώνει τις άλλες υποχρεώσεις του. Επιπλέον, οι διευθύνσεις IP, οι διευθύνσεις MAC και άλλοι τύποι πληροφοριών που κάποτε θεωρούνταν δεδομένα μηχανής ή τηλεμετρίας θεωρούνται πλέον ΔΠΧ σε πολλές δικαιοδοσίες, εάν οι πληροφορίες αυτές μπορούν εύκολα να συνδεθούν με τη συσκευή ενός καταναλωτή. Οι καταναλωτές μπορεί να έχουν πολύ διαφορετικά επίπεδα κατανόησης της υφιστάμενης και αναδυόμενης διασύνδεσης των "δικτύων" (επικοινωνιακών, κοινωνικών, προσωπικών κ.λπ.), των τεχνολογιών επικοινωνίας πληροφοριών (ΤΠΕ) (information communication technologies ICTs) και άλλων ψηφιακών στοιχείων των προϊόντων με τα οποία αλληλεπιδρά ο καταναλωτής. Οι εξελίξεις στην πληροφορική επηρεάζουν επομένως τις προσδοκίες των καταναλωτών για την ιδιωτικότητα: για παράδειγμα, ένα σύνολο πληροφοριών που φαίνεται να μην ταυτοποιεί τον καταναλωτή, όταν συνδέεται με άλλα σύνολα πληροφοριών, θα μπορούσε να επιτρέψει την ταυτοποίηση του καταναλωτή, να αποκαλύψει προσωπικές πληροφορίες για τον καταναλωτή (για παράδειγμα, τη συμπεριφορά του, το προσωπικό του ιστορικό, τις σχέσεις του ή την τοποθεσία του) ή θα μπορούσε να διαστρεβλώσει προσωπικές του πληροφορίες μέσω της προσθήκης ψευδών στοιχείων. Οι καταναλωτές έχουν ένα εύρος δυνατοτήτων και ευπαθειών [20] [21] [22] [23] που θα επηρεάσουν τον τρόπο με τον οποίο αλληλεπιδρούν με το προϊόν και τα αντίμετρα ιδιωτικότητας. Αν ο οργανισμός δεν κατανοεί καλά τους καταναλωτές του, δεν μπορεί να είναι

βέβαιος ότι ο σχεδιασμός των αντιμέτρων της ιδιωτικότητας που απαιτούν δράση ή αδράνεια του καταναλωτή, θα λειτουργήσει όπως έχει σχεδιαστεί.

ΣΗΜΕΙΩΣΗ Για περισσότερες πληροφορίες σχετικά με την ευπάθεια των καταναλωτών και την ευάλωτη κατάσταση ανατρέξτε στο ISO 22458 [20] και στο ISO/IEC Guide 76 [21]

4.3.3 Οδηγία

α) Οι προτιμήσεις και οι ανάγκες των καταναλωτών για την ιδιωτικότητα θα πρέπει να έχουν σημαντικό και κατατοπιστικό ρόλο κατά τον καθορισμό των απαιτήσεων της ιδιωτικότητας για το καταναλωτικό προϊόν (βλ. 4.4.1 Απαίτηση).

β) Οι απόψεις και οι προτιμήσεις των καταναλωτών θα πρέπει να αναζητούνται στο πλαίσιο της διαδικασίας σχεδιασμού του προϊόντος, ώστε να διασφαλίζεται ότι τα αντίμετρα ιδιωτικότητας του προϊόντος θα λειτουργούν όπως έχουν σχεδιαστεί, με τρόπο που να παρέχει μια ωφέλιμη εμπειρία χρήσης για τους καταναλωτές, η οποία θα σέβεται την ευαισθησία των δεδομένων τους και τα δικαιώματα και τις ανάγκες τους όσον αφορά την ιδιωτικότητα [23].

γ) Ο οργανισμός θα πρέπει να κατανοεί τον τρόπο με τον οποίο ο καταναλωτής χρησιμοποιεί τα αντίμετρα ιδιωτικότητας, ώστε τα αντίμετρα ιδιωτικότητας του προϊόντος να μπορούν να παραμείνουν αποτελεσματικά παρά τις ενέργειες ή την αδράνεια των καταναλωτών.

δ) Ο οργανισμός θα πρέπει να θεωρεί τους υφιστάμενους και μελλοντικούς καταναλωτές του ως βασικό πόρο στον κύκλο ζωής του προϊόντος. Αυτό μπορεί να λάβει τη μορφή μιας επίσημης προσέγγισης για συνεργασία με τους καταναλωτές, για παράδειγμα, από την απλή παροχή προσεκτικής ανάλυσης των εισροών από εύχρηστους μηχανισμούς ανατροφοδότησης έως την πιο ενδελεχή (και δαπανηρή) έρευνα χρηστών από επαγγελματίες ερευνητές χρηστών με γνώση της ιδιωτικότητας που χρησιμοποιούν αυστηρές μεθοδολογίες έρευνάς της.

ε) Εάν το προϊόν διαθέτει αντίμετρα ιδιωτικότητας που μπορεί να χειριστεί ο καταναλωτής, ο καταναλωτής θα πρέπει να ενημερωθεί για τον τρόπο χειρισμού τους, ώστε να αποφευχθούν λάθη, είτε εν γνώσει είτε εν αγνοία του. Τα σφάλματα αυτά μπορεί να περιλαμβάνουν, μεταξύ άλλων, την επεξεργασία δεδομένων που είναι αντίθετη με τις επιθυμίες του καταναλωτή, εάν ο καταναλωτής: έκανε εν αγνοία του κλικ σε λάθος επιλογή, δεν κατανόησε το αποτέλεσμα ή την επίπτωση της ενεργοποίησης ή απενεργοποίησης μιας συγκεκριμένης ρύθμισης ή ενός ελέγχου στον περαιτέρω χειρισμό των προσωπικών του δεδομένων, ή αν η τοποθεσία του παρακολουθείται εν αγνοία του από το προϊόν εξ' ορισμού.

ζ) Ο οργανισμός θα πρέπει να έχει σαφή άποψη σχετικά με τις προτιμήσεις των καταναλωτών για την ιδιωτικότητα. Εάν δεν έχει, θα είναι δύσκολο να σχεδιάσει το προϊόν για να αντιμετωπίσει αυτές τις προτιμήσεις με τρόπο που να προστατεύει την ιδιωτικότητα των καταναλωτών και να επιτρέπει στον οργανισμό να εκπληρώσει άλλες υποχρεώσεις του.

4.4 Σχεδιασμός διεπαφής ανθρώπου-υπολογιστή (human computer interface HCI) για την ιδιωτικότητα

4.4.1 Απαίτηση

Ο οργανισμός θα πρέπει να σχεδιάζει τις ρυθμίσεις ιδιωτικότητας που μπορούν να ρυθμιστούν από τον καταναλωτή και μέτρα διαχείρισης απορρήτου που μπορούν να διαμορφωθούν από τον καταναλωτή, λαμβάνοντας υπόψη τις δυνατότητες των καταναλωτών και τις πιθανές ειδικές ανάγκες αυτών.

4.4.2 Επεξήγηση

Η χρήση ανθρωποκεντρικού σχεδιασμού δεν ωφελεί μόνο τον καταναλωτή, αλλά έχει σημαντική οικονομική αξία για τους οργανισμούς. Τα συστήματα, οι υπηρεσίες και τα αγαθά με υψηλή χρηστικότητα τείνουν να είναι πιο επιτυχημένα τόσο τεχνικά όσο και εμπορικά.

Η παροχή στους καταναλωτές της δυνατότητας να διαχειρίζονται οι ίδιοι τα δεδομένα τους, καθώς και τα αντίμετρα και τις προτιμήσεις ιδιωτικότητας, αποτελεί κρίσιμο μέτρο ελέγχου κατά των καταχρήσεων και των εσφαλμένων χρήσεων των ΔΠΧ. Η κατανόηση από τους καταναλωτές του τρόπου και του πλαισίου επεξεργασίας των ΔΠΧ από το προϊόν – και η παροχή σε αυτούς κάποιου επιπέδου ελέγχου – αποτελεί θεμέλιο για τη διαφάνεια και την εμπιστοσύνη.

Σε περίπτωση που ο καταναλωτής χειρίζεται αντίμετρα ιδιωτικότητας στο προϊόν, αυτά πρέπει να ορίζονται, να τεκμηριώνονται στις περιπτώσεις χρήσης [24] [25] και να σχεδιάζονται ώστε να λαμβάνουν υπόψη την εμπειρία του καταναλωτή, τους ανθρώπινους παράγοντες και το ευρύ φάσμα των δυνατοτήτων, των εμπειριών και των ειδικών αναγκών των δυνητικών καταναλωτών σε σχέση με τις δυνατότητες του προϊόντος.

Οι χρήσεις περιπτώσεων [26] περιγράφουν τη χρήση του προϊόντος από τον καταναλωτή και επηρεάζουν την ανάλυση των κινδύνων παραβίασης ιδιωτικότητας των καταναλωτών. Ο καθορισμός των κεντρικών περιπτώσεων χρήσης επιτρέπει στους σχεδιαστές του προϊόντος να διερευνήσουν τις περιφερειακές περιπτώσεις χρήσης και εκείνες που αντιπροσωπεύουν περιπτώσεις κατάχρησης και κακής χρήσης. Οι περιπτώσεις χρήσης μπορούν να χρησιμοποιηθούν για τον εντοπισμό των αναγκών προστασίας της ιδιωτικότητας των καταναλωτών που προκύπτουν από τις αλληλεπιδράσεις των καταναλωτών και τα γνωστά τεχνικά και καταναλωτικά ευάλωτα σημεία.

4.4.3 Οδηγία

α) Ο έλεγχος και η επιλογή του καταναλωτή θα πρέπει να είναι σαφείς και εμφανείς στο σχεδιασμό των ρυθμίσεων απορρήτου του καταναλωτή.

β) Ο σχεδιασμός ρυθμίσεων απορρήτου που μπορεί να διαμορφωθεί από τον καταναλωτή θα πρέπει να υιοθετεί τεχνικές μηχανικής της ιδιωτικότητας [23].

γ) Ο σχεδιασμός του προϊόντος μπορεί να μεταφέρει το πλαίσιο για την επεξεργασία των ΔΠΧ. Οι ομάδες ανάπτυξης προϊόντων θα πρέπει να αποφεύγουν πρακτικές σχεδιασμού που ενδέχεται να παρεμποδίζουν τη διαφάνεια, να είναι ασαφείς και να δημιουργούν αρνητική εμπειρία στον καταναλωτή όσον αφορά τη χρήση των ΔΠΧ. Αυτό απαιτεί προσεκτική εξέταση των αντιμέτρων ιδιωτικότητας σε όλα τα στάδια ανάπτυξης του προϊόντος, συμπεριλαμβανομένης της εμπειρίας του καταναλωτή και του σχεδιασμού των συστημάτων, ώστε να διασφαλίζεται ότι οι καταναλωτές δεν μοιράζονται άθελά τους τα ΔΠΧ, δεν εμποδίζονται να διαχειριστούν τον τρόπο με τον οποίο μπορεί να υποστούν επεξεργασία τα ΔΠΧ ή δεν οδηγούνται σε απροσδόκητες χρήσεις των ΔΠΧ.

4.5 Ανάθεση σχετικών ρόλων και αρμοδιοτήτων

4.5.1 Απαίτηση

Ο οργανισμός θα πρέπει να ορίζει και διατηρεί ρόλους και αρμοδιότητες, συμπεριλαμβανομένου τουλάχιστον ενός υπεύθυνου για την επισκόπηση ολόκληρου του κύκλου ζωής των ΔΠΧ και των προϊόντων, με ευθύνη για τη διασφάλιση της διαχείρισης των κινδύνων παραβίασης της ιδιωτικότητας και των αντιμέτρων για τα ΔΠΧ καθ' όλη τη διάρκεια του κύκλου ζωής των ΔΠΧ.

4.5.2 Επεξήγηση

Οι ρόλοι και οι εξουσίες για τον κύκλο ζωής ενός καταναλωτικού προϊόντος και τον κύκλο ζωής των ΔΠΧ, ενημερώνουν για τη διαχείριση του κινδύνου και παρέχουν λογοδοσία για τα αντίμετρα ιδιωτικότητας που σχετίζονται με το προϊόν.

4.5.3 Οδηγία

α) Ο ρόλος του φυσικού προσώπου που λογοδοτεί θα πρέπει να περιλαμβάνει την κατάσταση της ιδιωτικότητας, η οποία μπορεί να περιλαμβάνει, μεταξύ άλλων, την τρέχουσα κατάσταση της επεξεργασίας ή της χρήσης των δεδομένων, την κατάσταση αναγνωρισιμότητας των δεδομένων (ακατέργαστα, ψευδωνυμοποιημένα/αποταυτοποιημένα, ανώνυμα), την προβλεπόμενη ημερομηνία διαγραφής των ΔΠΧ που σχετίζονται με ένα προϊόν. Ο ρόλος αυτός μπορεί να συμβάλει στον κύκλο ζωής ενός προϊόντος και στον κύκλο ζωής των ΔΠΧ που επεξεργάζεται, ώστε να διασφαλίζεται η αποτελεσματικότητα όλων των αντιμέτρων ιδιωτικότητας του προϊόντος. Ένα φυσικό πρόσωπο που λογοδοτεί μπορεί να περιλαμβάνει μεταξύ άλλων: συντονιστές αντιμετώπισης περιστατικών, υπεύθυνο παραγωγής και επικοινωνία με τους καταναλωτές.

b) Η υπευθυνότητα και οι αρμοδιότητες θα πρέπει να ορίζονται σαφώς, να διαθέτουν επαρκείς πόρους και να επανεξετάζονται περιοδικά ως προς την αποτελεσματικότητά τους.

4.6 Καθορισμός πολυλειτουργικών αρμοδιοτήτων

4.6.1 Απαίτηση

Ο οργανισμός θα πρέπει να ορίζει ένα φυσικό πρόσωπο που λογοδοτεί για κάθε λειτουργία ή οργανισμό που συμβάλλει στο σχεδιασμό ή τη λειτουργία των αντιμέτρων της ιδιωτικότητας ή διαχειρίζεται την επεξεργασία των ΔΠΧ από το προϊόν.

4.6.2 Επεξήγηση

Ενώ το φυσικό πρόσωπο που λογοδοτεί είναι υπεύθυνο για τη συνολική αποτελεσματικότητα των αντιμέτρων ιδιωτικότητας του προϊόντος, ο σχεδιασμός και η λειτουργία συχνά απαιτούν τη συμβολή εμπειρογνωμοσύνης από πολλαπλές λειτουργίες και από πολλούς οργανισμούς. Ορισμένες φορές οι ομάδες σχηματίζονται συνδυάζοντας πολλαπλές λειτουργικές ομάδες σε μία. Αυτές οι πολυλειτουργικές ομάδες αποτελούνται από εμπειρογνώμονες από διάφορους λειτουργικούς τομείς και εργάζονται συνεργατικά για την επίτευξη κάποιου οργανωτικού στόχου.

Η διασφάλιση ότι η ιδιωτικότητα αποτελεί αναπόσπαστο μέρος της διαδικασίας σχεδιασμού απαιτεί τεχνογνωσία πολλαπλών λειτουργιών. Οι ολοκληρωμένες ομάδες σχεδιασμού εκθέτουν τους μηχανικούς σε άλλες μη τεχνικές προοπτικές (π.χ. νομικές, καταναλωτικές) και το αντίστροφο, βοηθώντας έτσι στην ενσωμάτωση ισχυρών κανόνων ιδιωτικότητας μεταξύ των τεχνικών ειδικών, των οποίων η εστίαση είναι γενικά στην ασφάλεια.

Οι πολυλειτουργικές ομάδες ανάπτυξης μπορούν να περιλαμβάνουν εμπειρογνώμονες τόσο σε θέματα ασφάλειας όσο και σε θέματα ιδιωτικότητας όταν σχεδιάζουν την ιδιωτικότητα σε καταναλωτικά προϊόντα, δεδομένου ότι οι κίνδυνοι για την παραβίαση της ιδιωτικότητας δεν προκύπτει μόνο από περιστατικά που σχετίζονται με την κυβερνοασφάλεια, αλλά και από την εξουσιοδοτημένη επεξεργασία ΔΠΧ.

Παρ' όλα αυτά, η ιδιωτικότητα και η ασφάλεια των πληροφοριών είναι και οι δύο αναπόσπαστες συνιστώσες ενός συνεκτικού μηχανισμού ελέγχου. Οι αρχές της ιδιωτικότητας περιλαμβάνουν την ασφάλεια των πληροφοριών και τις απαιτήσεις για εύλογες εγγυήσεις για τα ΔΠΧ, οι οποίες περιλαμβάνουν, μεταξύ άλλων: ελέγχους, μηχανισμούς και τεχνικές προστασίες. Η ιδιωτικότητα συμβάλλει στη διασφάλιση σημαντικών αξιών, όπως η ανθρώπινη αυτονομία και αξιοπρέπεια. Οι κατευθυντήριες αποφάσεις μπορούν να προκύψουν από ισχυρούς ηθικούς κανόνες, αρχές, πρακτικές και οργανωτικές πολιτικές. Οι μηχανισμοί διακυβέρνησης (governance) μπορούν να υποστηρίξουν, να διατηρήσουν και να εξελίξουν αυτούς τους κανόνες, τις αρχές και τις πρακτικές. Η ασφάλεια των πληροφοριών επιδιώκει να επιτρέψει και να προστατεύσει τις δραστηριότητες και τα περιουσιακά στοιχεία τόσο των ανθρώπων όσο και των επιχειρήσεων από την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας [25][26].

4.6.3 Οδηγία

α) Θα πρέπει να οριστούν ανώτεροι ρόλοι σε κάθε λειτουργία και οργανισμό που συμβάλλουν με εμπειρογνωμοσύνη στο σχεδιασμό ή τη λειτουργία των αντιμέτρων ιδιωτικότητας, ώστε να εκπροσωπούν και να αναλαμβάνουν την ευθύνη για τις εν λόγω συνεισφορές.

β) Οι ρόλοι θα πρέπει να είναι επαρκώς ανώτεροι ώστε να διασφαλίζεται ότι η σημασία της ιδιωτικότητας μπορεί να συμπεριληφθεί κατάλληλα παράλληλα με άλλες επιχειρησιακές προτεραιότητες.

4.7 Ανάπτυξη γνώσεων, δεξιοτήτων και ικανοτήτων σχετικά με την ιδιωτικότητα

4.7.1 Απαίτηση

Τα πρόσωπα που είναι υπεύθυνα για το σχεδιασμό και τη λειτουργία των αντιμέτρων της ιδιωτικότητας θα πρέπει να εξασφαλίζουν ότι υπάρχει η απαραίτητη κατάρτιση, ώστε να διασφαλίζεται ότι οι ομάδες διαθέτουν τις γνώσεις, τις δεξιότητες και τις ικανότητες για να εκτελούν αποτελεσματικά τους ρόλους τους.

4.7.2 Επεξήγηση

Η γνώση των απαιτήσεων ιδιωτικότητας ήδη από τον σχεδιασμό και η ικανότητα εφαρμογής τους σε συστήματα, στοιχεία, προϊόντα και υπηρεσίες αποτελούν σημαντικές δεξιότητες για το προσωπικό που ασχολείται με την ιδιωτικότητα, συμπεριλαμβανομένου του φυσικού προσώπου που λογοδοτεί και του υπεύθυνου μέρους [27] [28].

4.7.3 Οδηγία

α) Ο οργανισμός θα πρέπει να προσαρμόσει την προσέγγιση για την εκπαίδευση του του φυσικού προσώπου που λογοδοτεί και του υπεύθυνου μέρους στις απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό, σύμφωνα με τους στόχους της εκπαίδευσης.

β) Ο οργανισμός θα πρέπει να παρακολουθεί τον αντίκτυπο της εκπαίδευσης για να διαπιστώσει τη μακροπρόθεσμη αποτελεσματικότητά της, και να επανεξετάζει και να αναθεωρεί για να τη διατηρεί επίκαιρη.

γ) Η εκπαίδευση θα πρέπει να καλύπτει όλες τις πτυχές του κύκλου ζωής των ΔΠΧ και, για παράδειγμα, το πεδίο εφαρμογής των ΔΠΧ, τους τύπους και την ταξινόμηση των δεδομένων που υποβάλλονται σε επεξεργασία, τις περιπτώσεις χρήσης, τις πολιτικές σχετικά με τα δεδομένα στις συσκευές των εργαζομένων, τα εργαλεία για την κοινή χρήση δεδομένων, τα δεδομένα στα εργαλεία που παρέχονται από την εταιρεία (π.χ. ηλεκτρονικό ταχυδρομείο, συνομιλία) και τον τρόπο επικοινωνίας με την ομάδα της ιδιωτικότητας για περαιτέρω ερωτήσεις.

δ) Το προσωπικό που ασχολείται με την επεξεργασία δεδομένων θα πρέπει να λαμβάνει εκπαίδευση και κατάρτιση σε θέματα ευαισθητοποίησης σε θέματα προστασίας της ιδιωτικότητας, ώστε να εκτελεί τα καθήκοντα και τις ευθύνες που σχετίζονται με την με τις πολιτικές, τις διαδικασίες, τις διαδικασίες και τις αξίες ιδιωτικότητας του οργανισμού.

ε) Το προσωπικό που χειρίζεται τις διαδικασίες για την εκπλήρωση των υποχρεώσεων του οργανισμού έναντι των καταναλωτών, όπως η παροχή στους καταναλωτές της δυνατότητας να ασκούν τα δικαιώματα ή τις προτιμήσεις τους όσον αφορά την ιδιωτικότητα, θα πρέπει επίσης να είναι εκπαιδευμένο και επαρκώς ικανό.

ζ) Το προσωπικό που συμβάλλει στο σχεδιασμό και την εκτέλεση του προϊόντος θα πρέπει να ενημερωθεί για τις ευθύνες του όσον αφορά την ιδιωτικότητα και όσοι παρέχουν εξειδικευμένες συμβολές θα πρέπει να εκπαιδευτούν για το πώς να το κάνουν αυτό αποτελεσματικά.

η) Οι γνώσεις, οι δεξιότητες και οι ικανότητες σχετικά με τις απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό θα πρέπει επίσης να ενσωματώνονται στις συμβάσεις και στις συμφωνίες επιπέδου υπηρεσιών με τρίτους, συμπεριλαμβανομένων εκείνων στους οποίους μεταβιβάζονται τα ΔΠΧ.

θ) Η εκπαίδευση θα πρέπει να περιλαμβάνει την ανταλλαγή ορθών πρακτικών και να επεκτείνεται σε όσους συνεισφέρουν από τρίτους, συμπεριλαμβανομένων εκείνων στους οποίους μεταβιβάζονται τα ΔΠΧ.

4.8 Διασφάλιση της γνώσης των αντιμέτρων για την ιδιωτικότητα

4.8.1 Απαίτηση

Τα πρόσωπα που είναι υπεύθυνα για το σχεδιασμό και τη λειτουργία των αντιμέτρων ιδιωτικότητας θα πρέπει να εξασφαλίζουν ότι υπάρχει η απαραίτητη εκπαίδευση για να διασφαλιστεί ότι οι ομάδες είναι επαρκώς ενημερωμένες τόσο για τις απαιτήσεις ιδιωτικότητας του προϊόντος όσο και για τις πολιτικές και τις διαδικασίες της ιδιωτικότητας του οργανισμού.

4.8.2 Επεξήγηση

Ο οργανισμός θα πρέπει να διαθέτει εμπειρογνωμοσύνη σε θέματα της ιδιωτικότητας, εάν πρόκειται να ηγηθεί των προσπαθειών για τη διάδοση της γνώσης στο προσωπικό που συμμετέχει στο σχεδιασμό και την ανάπτυξη προϊόντων και στον κύκλο ζωής των δεδομένων. Η εμπειρογνωμοσύνη αυτή μπορεί να βρίσκεται εντός του οργανισμού ή να είναι εξωτερική. Η διάδοση της γνώσης [29] των αντιμέτρων ιδιωτικότητας για το προϊόν και των πολιτικών ιδιωτικότητας του οργανισμού πρέπει να γίνεται πριν και κατά τη διάρκεια ενός έργου, ώστε το προσωπικό να μπορεί να ενσωματώσει τις γνώσεις αυτές στις βασικές του δεξιότητες. Αυτό θα τους επιτρέψει να προσδιορίσουν τα καλύτερα μέσα για την εφαρμογή των αντιμέτρων ιδιωτικότητας ως μέρος της ανάπτυξης του προϊόντος και να διασφαλίσουν ότι ευθυγραμμίζονται με τους στόχους του οργανισμού για την ιδιωτικότητα. Θα πρέπει να τίθενται στη διάθεση του προσωπικού κατάλληλοι πόροι ώστε να διασφαλίζεται ότι οι ερωτήσεις μπορούν να αντιμετωπιστούν όπως απαιτείται σε όλα τα στάδια ανάπτυξης του προϊόντος και κατά τη διάρκεια του κύκλου ζωής του προϊόντος και των ΔΠΧ.

Παρακάτω, ανά κατηγορία αντιμέτρου, παρατίθενται λίστες αντιμέτρων για τους οποίους το φυσικό πρόσωπο που λογοδοτεί μπορεί να έχει γνώση και να διασφαλίσει ότι οι ομάδες του διαθέτουν επαρκείς δεξιότητες και γνώσεις.

Τα αντίμετρα συμμόρφωσης και τα διοικητικά αντίμετρα περιλαμβάνουν, για παράδειγμα, ευαισθητοποίηση και κατάρτιση σε θέματα της ιδιωτικότητας, αξιολόγηση αντικτύπου ιδιωτικότητας, πρόγραμμα διακυβέρνησης και ιδιωτικότητας, αρχεία των δραστηριοτήτων επεξεργασίας, κείμενο συγκατάθεσης, συμφωνία επεξεργασίας δεδομένων, δεσμευτικούς εταιρικούς κανόνες, ελέγχους ή συμφωνίες με τρίτα μέρη.

Τα τεχνικά αντίμετρα περιλαμβάνουν, για παράδειγμα, αντίμετρα φυσικών συσκευών, χρόνος ζωής (TTL – Time To Leave - ένας μηχανισμός που περιορίζει τη διάρκεια ζωής των δεδομένων σε έναν υπολογιστή ή ένα δίκτυο), κρυπτογράφηση των ΔΠΧ (κατά τη μεταφορά και μη), από-ταυτοποίηση (de-identification) και ανωνυμοποίηση (anonymization), ελέγχους πρόσβασης (access controls), άλλες τεχνολογίες που ενισχύουν την ιδιωτικότητα.

Οι υπηρεσίες βελτίωσης της ιδιωτικότητας μπορεί να περιλαμβάνουν, μεταξύ άλλων, ένα σύνολο εργαλείων ή ένα πλαίσιο συναίνεσης, υπηρεσία διαγραφής ΔΠΧ, υπηρεσία εξαγωγής ΔΠΧ, υπηρεσία κρυπτογράφησης ΔΠΧ, εργαλεία αποταυτοποίησης ή ανωνυμοποίησης, ενημερωμένους καταλόγους ΔΠΧ, εντοπισμό ΔΠΧ των καταναλωτών.

Το φυσικό πρόσωπο που λογοδοτεί υποστηρίζεται από διάφορους ειδικούς σε θέματα της ιδιωτικότητας που βοηθούν στην εκτέλεση των ακόλουθων καθηκόντων:

— συστάσεις σχετικά με τους ελέγχους συμμόρφωσης με βάση τη νομοθεσία, τις πολιτικές, τις απαιτήσεις και τις αξιολογήσεις κινδύνου παραβίασης της ιδιωτικότητας,

— συστάσεις και τυποποίηση τεχνικών ελέγχων, εργαλείων και άλλων μέσων υποστήριξης κατά την εφαρμογή των ελέγχων, εντοπισμός κενών στην προστασία της ιδιωτικότητας στις πλατφόρμες και καθοδήγηση των ελέγχων στις πλατφόρμες,

— διατήρηση του συνολικού προγράμματος για την ιδιωτικότητα και των έργων για την ιδιωτικότητα σε ολόκληρο τον οργανισμό,

— διασφάλιση της παρακολούθησης των τεχνικών ελέγχων, της προτεραιοποίησης, ώστε να σημειώνεται πρόοδος και να εφαρμόζεται σε ολόκληρο τον οργανισμό, για παράδειγμα, διατήρηση δεδομένων σε ολόκληρο τον οργανισμό, έργα απογραφής δεδομένων, έργα εξαγωγής ή διαγραφής δεδομένων.

4.8.3 Οδηγία

α) Κάθε υπεύθυνο μέρος που συνεισφέρει τεχνογνωσία θα πρέπει να εκπαιδεύεται στην ιδιωτικότητα, ώστε να διασφαλίζεται ότι οι ορθές πρακτικές ενσωματώνονται στο προϊόν με δομημένο και διαφανή τρόπο.

β) Κάθε υπεύθυνο μέρος που συνεισφέρει τεχνογνωσία θα πρέπει να διαθέτει την κατάλληλη τεχνογνωσία σε θέματα της ιδιωτικότητας και να κατανοεί τη διαδικασία, ώστε να διασφαλίζεται ότι ενσωματώνονται οι ορθές πρακτικές ιδιωτικότητας στο προϊόν με δομημένο τρόπο.

γ) Οι νομικές και κανονιστικές υποχρεώσεις που σχετίζονται με το προϊόν, σε συνδυασμό με τις εθελοντικές πολιτικές προστασίας της ιδιωτικότητας που επιλέγει να υιοθετήσει ο οργανισμός για το προϊόν του, θα πρέπει να αποτελούν την πηγή των στόχων ελέγχου της ιδιωτικότητας για το προϊόν. Αυτοί είναι οι στόχοι που θα καθοδηγήσουν τους σχεδιαστές και τους προγραμματιστές στο σχεδιασμό των αντιμέτρων ιδιωτικότητας.

4.9 Διαχείριση εγγράφων και πληροφοριών

4.9.1 Απαίτηση

Ο οργανισμός θα πρέπει να δημιουργεί και να διατηρεί τεκμηριωμένες πληροφορίες για να αποδεικνύει ότι ο σχεδιασμός και η λειτουργία των αντιμέτρων ιδιωτικότητας είναι αποτελεσματικά.

4.9.2 Επεξήγηση

Εάν ο σχεδιασμός και η λειτουργία των αντιμέτρων ιδιωτικότητας ενός προϊόντος πρόκειται να ενσωματωθούν στον κύκλο ζωής του προϊόντος, τότε η τεκμηρίωση από το στάδιο του σχεδιασμού θα αποτυπώσει τις βασικές πληροφορίες που θα χρησιμοποιηθούν από το προσωπικό του οργανισμού και από τρίτους αργότερα στον κύκλο ζωής. Οι τεκμηριωμένες πληροφορίες λαμβάνουν συχνά τη μορφή ενός εγγράφου που ενημερώνεται με λεπτομέρειες σχετικά με το σχεδιασμό των αντιμέτρων ιδιωτικότητας, πληροφορίες σχετικά με τις δοκιμές τους και τη λειτουργία τους αργότερα στον κύκλο ζωής.

Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες (π.χ. πολιτικές, διαδικασίες, οδηγίες που πρέπει να ακολουθούνται) και αποθηκεύει αρχεία για την παρακολούθηση των εκτελούμενων δραστηριοτήτων. Αυτό βοηθάει όταν οι εργαζόμενοι εκτελούν τις δραστηριότητες (επειδή πρέπει να γνωρίζουν τις πολιτικές, τις διαδικασίες και τις οδηγίες και να επανεξετάζουν τα αρχεία των προηγούμενων ή παρόμοιων δραστηριοτήτων). Οι τεκμηριωμένες πληροφορίες για τις απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό περιλαμβάνουν [30] τα ακόλουθα:

— αξιολόγηση κινδύνου παραβίασης της ιδιωτικότητας,

— ΔΠΧ / ροή δεδομένων,

— τις λειτουργικές και μη λειτουργικές απαιτήσεις ιδιωτικότητας του προϊόντος και της υπηρεσίας,

— αντίμετρα ιδιωτικότητας που θα εφαρμοστούν στο προϊόν και την υπηρεσία,

— αποτελέσματα των δοκιμών, αποφάσεις αποδοχής και εγκρίσεις για την παράδοση,

— επικοινωνία με τους καταναλωτές όσον αφορά την ιδιωτικότητα

4.9.3 Οδηγία

α) Ο οργανισμός θα πρέπει να διαχειρίζεται τεκμηριωμένες πληροφορίες που έχουν εγκριθεί από τις αρμόδιες αρχές και είναι αναγνώσιμες και διαθέσιμες σε όλους τους προβλεπόμενους παραλήπτες.

ΣΗΜΕΙΩΣΗ Για περισσότερες πληροφορίες σχετικά με τις τεκμηριωμένες πληροφορίες με τη χρήση ενός Συστήματος Διοίκησης Πληροφοριών Ιδιωτικότητας και Συστήματος Διοίκησης Ασφάλειας Πληροφοριών, ανατρέξτε στο ISO/IEC 27701, ISO/IEC 27001 και ISO/IEC 27002.

β) Οι τεκμηριωμένες πληροφορίες θα πρέπει να ελέγχονται ώστε να διασφαλίζεται ότι είναι διαθέσιμες και κατάλληλες για χρήση, όπου και όταν χρειάζονται, και ότι προστατεύονται επαρκώς (π.χ. από την απώλεια της εμπιστευτικότητας, την ακατάλληλη χρήση ή την απώλεια της ακεραιότητας).

γ) Για τον έλεγχο των τεκμηριωμένων πληροφοριών, ο οργανισμός θα πρέπει να αντιμετωπίσει τις ακόλουθες δραστηριότητες, κατά περίπτωση:

— διανομή, πρόσβαση, ανάκτηση και χρήση,

— αποθήκευση και διατήρηση, συμπεριλαμβανομένης της αναγνωσιμότητας,

— έλεγχος των αλλαγών (π.χ. έλεγχος έκδοσης),

— διατήρηση και απόρριψη.

δ) Οι τεκμηριωμένες πληροφορίες εξωτερικής προέλευσης, οι οποίες κρίνονται από τον οργανισμό απαραίτητες για το σχεδιασμό και τη λειτουργία των αντιμέτρων της ιδιωτικότητας, θα πρέπει να προσδιορίζονται κατά περίπτωση και να ελέγχονται.

5 Απαιτήσεις επικοινωνίας του καταναλωτή

5.1 Επισκόπηση

Οι καταναλωτές των προϊόντων που επεξεργάζονται ΔΠΧ αναμένουν πληροφορίες στο σημείο συλλογής ή όταν μπορεί να ληφθεί μια απόφαση που επηρεάζει την ιδιωτικότητα, οι οποίες περιέχουν σαφείς, συνοπτικές, προσιτές, ουσιαστικές και επαληθεύσιμες εξηγήσεις και παρατηρήσεις σχετικά με το πώς και γιατί ένα προϊόν θα επεξεργάζεται ή όχι ΔΠΧ και θα διαχειρίζεται την ιδιωτικότητα. Ο στόχος είναι να διευκολυνθεί η ασφαλής, τεκμηριωμένη λήψη αποφάσεων από τον καταναλωτή πριν από την απόκτηση ή τη χρήση. Οι καταναλωτές των προϊόντων που επεξεργάζονται ΔΠΧ θέλουν επίσης να γνωρίζουν πότε περιστατικά ή σφάλματα στον τρόπο επεξεργασίας των ΔΠΧ τους θέτουν τους ίδιους ή τα ΔΠΧ τους σε κίνδυνο, ή πότε υπάρχουν αλλαγές στους σκοπούς για τους οποίους θα επεξεργάζονται τα ΔΠΧ.

Η διαφάνεια και η συνεχής επικοινωνία υποστηρίζουν τη λογοδοσία. Δίνουν τη δυνατότητα στους καταναλωτές και άλλους να συγκρίνουν τις λεπτομέρειες της επεξεργασίας με τις εξηγήσεις και τις δεσμεύσεις και να αναλάβουν δράση (π.χ. να υποβάλουν ένα παράπονο ή να σταματήσουν να χρησιμοποιούν το προϊόν) και να αμφισβητήσουν το φυσικό πρόσωπο που λογοδοτεί, όταν αυτό δικαιολογείται. Παίρνουν πολλές μορφές από τις διεπαφές με τον καταναλωτή, τα αρχεία βοήθειας τις οδηγίες του προϊόντος μέσω του πακεταρίσματος, των προθέσεων μάρκετινγκ και των σεναρίων εξυπηρέτησης του καταναλωτή μέχρι τις συχνές ερωτήσεις, τις ανακοινώσεις και τις πολιτικές.

Ευκαιρίες για διαφάνεια και επικοινωνία με τον καταναλωτή παρουσιάζονται σε όλα τα στοιχεία του κύκλου ζωής του προϊόντος και του οικοσυστήματός του που αντιμετωπίζει ο καταναλωτής. Το φυσικό πρόσωπο που λογοδοτεί μπορεί να έχει αρμοδιότητες για τη δημιουργία επικοινωνιών, ανακοινώσεων και τεκμηρίωσης σχετικά με το προϊόν που εστιάζουν στην ιδιωτικότητας. Το υπεύθυνο μέρος που δημιουργεί επικοινωνίες, ανακοινώσεις και τεκμηρίωση σχετικά με το προϊόν που εστιάζουν στην ιδιωτικότητα των καταναλωτών μπορεί να είναι το ίδιο πρόσωπο με το φυσικό πρόσωπο που λογοδοτεί (βλ. 4.6.1 Απαίτηση).

5.2 Παροχή (provision) πληροφοριών ιδιωτικότητας

5.2.1 Απαίτηση

Ο οργανισμός θα πρέπει να ενημερώνει τους χρήστες σχετικά με τις ρυθμίσεις απορρήτου που μπορούν να ρυθμιστούν από τον καταναλωτή. Ο οργανισμός θα πρέπει να διατηρεί και να θέτει στη διάθεση άλλων χρηστών πληροφορίες σχετικά με τις ρυθμίσεις ή τα χαρακτηριστικά απορρήτου του προϊόντος, ώστε να μπορούν να διαμορφώνουν το προϊόν σύμφωνα με τους στόχους τους όσον αφορά την προστασία της ιδιωτικότητας.

5.2.2 Επεξήγηση

Μόλις το προϊόν κυκλοφορήσει στους καταναλωτές, η δυνατότητα του οργανισμού να αλλάξει τα αντίμετρα μπορεί να είναι περιορισμένη. Εάν η διαδικασία δοκιμής της λειτουργίας των ελέγχων του προϊόντος πριν από την κυκλοφορία δεν είναι ισχυρή, μπορεί να κυκλοφορήσουν προϊόντα που δεν διαχειρίζονται κατάλληλα τους κινδύνους προστασίας της ιδιωτικότητας.

Οι καταναλωτές θα πρέπει να γνωρίζουν τον τρόπο με τον οποίο ένα προϊόν επεξεργάζεται τα ΔΠΧ προκειμένου να λαμβάνουν τεκμηριωμένες αποφάσεις για τη χρήση ή την απόκτηση προϊόντων που επεξεργάζονται ΔΠΧ. Συνήθως, αυτή η διαφάνεια και η επικοινωνία έχει τη μορφή εγχειριδίου σχετικά με τις ρυθμίσεις ή τα χαρακτηριστικά απορρήτου του προϊόντος, ειδοποίησης απορρήτου ή/και τεκμηρίωσης του προϊόντος που εξηγεί πτυχές του τρόπου με τον οποίο το προϊόν επεξεργάζεται ΔΠΧ, συμβάσεις και ΣΕΥ (SLAs), οδηγίες για την απαίτηση υποστήριξης ή την αποστολή παραπόνων – λαμβάνει επίσης τη μορφή ετικετών διεπαφής χρήστη, συσκευασίας και δηλώσεων μάρκετινγκ.

ΣΗΜΕΙΩΣΗ Περαιτέρω πληροφορίες σχετικά με το περιεχόμενο των ανακοινώσεων απορρήτου παρέχονται από ISO/IEC 29184.

Κατά τη διάρκεια της περιόδου υποστήριξης του προϊόντος, η ενημέρωση του καταναλωτή σχετικά με τις αλλαγές στους κινδύνους παραβίασης της ιδιωτικότητας τον βοηθά να έχει τη δυνατότητα να διαχειρίζεται αποτελεσματικά τους εν λόγω κινδύνους. Εάν η εν λόγω επικοινωνία δεν σχεδιαστεί έτσι ώστε να είναι αποτελεσματική, οι καταναλωτές μπορεί να διαπιστώσουν ότι το προϊόν τους εκθέτει σε σημαντικούς υπολειπόμενους κινδύνους παραβίασης της ιδιωτικότητας.

Η υποστήριξη μπορεί να περιλαμβάνει τεχνικές διορθώσεις στο λογισμικό ή το υλικό που αλλάζουν τα αντίμετρα ιδιωτικότητας που ενσωματώθηκαν στο προϊόν κατά την ανάπτυξη.

Οι καταναλωτές συχνά χρειάζονται υποστήριξη για να κατανοήσουν πώς να εγκαταστήσουν, να ρυθμίσουν και να λειτουργήσουν ένα προϊόν και αν έχουν προβλήματα ή παράπονα. Τα καταναλωτικά προϊόντα συχνά περιλαμβάνουν υπηρεσίες που παρέχονται από διαφορετικούς παρόχους και αυτό πρέπει να γίνεται σαφές στον καταναλωτή, ώστε να γνωρίζει με ποιον πρέπει να επικοινωνήσει και ποιος είναι υπεύθυνος. Η διασφάλιση ότι οι καταναλωτές γνωρίζουν πού μπορούν να ζητήσουν υποστήριξη και ότι οι δραστηριότητες υποστήριξης θα λειτουργούν για την ιδιωτικότητα είναι απαραίτητη για τη διατήρηση της εμπιστοσύνης των καταναλωτών σε τρίτους.

5.2.3 Οδηγία

α) Οι πληροφορίες πηγής για τις επικοινωνίες, τις ανακοινώσεις και την τεκμηρίωση που επικεντρώνονται στην ιδιωτικότητα θα πρέπει να περιλαμβάνουν τα εξής:

— σύντομη, συνεκτική επισκόπηση των ρυθμίσεων ή των λειτουργιών προστασίας της ιδιωτικότητας του προϊόντος, συμπεριλαμβανομένων των συνεπειών της επαναδιαμόρφωσης των ρυθμίσεων αυτών από τις προεπιλεγμένες ρυθμίσεις ιδιωτικότητας,

— δήλωση ιδιωτικότητας ή/και τεκμηρίωση του προϊόντος που εξηγεί τον τρόπο με τον οποίο το προϊόν επεξεργάζεται τα ΔΠΧ – αυτό θα περιλαμβάνει τα ΔΠΧ που επεξεργάζεται, τους σκοπούς για τους οποίους επεξεργάζεται τα ΔΠΧ – με ποιους μοιράζονται τα δεδομένα (και για ποιους σκοπούς),

— συμβάσεις και ΣΕΥ,

— οδηγίες για την αίτηση υποστήριξης ή την αποστολή παραπόνων και πώς ο καταναλωτής μπορεί να ασκήσει τα διαθέσιμα δικαιώματα ιδιωτικότητας,

— έλεγχοι που ενεργοποιούνται ως μέρος του σχεδιασμού του προϊόντος για την προστασία των ΔΠΧ και του καταναλωτή από αθέμιτη και μη εξουσιοδοτημένη πρόσβαση και χρήση των ΔΠΧ,

— τη διαφάνεια της μηχανικής μάθησης, για παράδειγμα, αλλά όχι μόνο: στα μοντέλα όπου είναι σαφές ποια έκδοση του μοντέλου χρησιμοποιείται, τι προορίζεται να κάνει το μοντέλο και ποιος δημιούργησε το μοντέλο για ποιους σκοπούς, στα σύνολα δεδομένων όπου είναι σαφές

πώς συλλέχθηκαν τα ΔΠΧ, αν καθαρίστηκαν ή όχι και αν ελέγχθηκαν για μεροληψία, στην ανιχνευσιμότητα – για να βρεθεί ποιο μοντέλο (συμπεριλαμβανομένης της έκδοσης) και ποια σύνολα δεδομένων και ΔΠΧ χρησιμοποιήθηκαν κατά τη διάρκεια μιας αλγοριθμικής απόφασης,

— οντότητα που είναι υπεύθυνη για τη λήψη αποφάσεων σχετικά με τον τρόπο επεξεργασίας των ΔΠΧ και για τις αντιδράσεις σχετικά με την κοινοποίηση συμβάντων και τη διαχείριση της παραβίασης της ιδιωτικότητας.

β) Τα επιχειρηματικά μοντέλα θα πρέπει να προσδιορίζονται όταν τα δεδομένα συλλέγονται και διαβιβάζονται σε τρίτους για εμπορικούς σκοπούς, δηλαδή για σκοπούς κέρδους.

γ) Η επικοινωνιακή στρατηγική θα πρέπει όχι μόνο να λαμβάνει υπόψη την ευαίσθητη φύση των δεδομένων που συλλέγονται από το προϊόν που χρησιμοποιείται από άτομα ειδικές ανάγκες και την ποικιλομορφία των αναγκών των καταναλωτών (π.χ. ακουστικές, οπτικές ή απτικές), αλλά και να ενσωματώνει τις εν λόγω εκτιμήσεις κατά την ανάπτυξη γνωστοποιήσεων, ανακοινώσεων και άλλων ελέγχων προστασίας της ιδιωτικότητας εντός του προϊόντος.

δ) Ο οργανισμός θα πρέπει να ορίσει τους κατάλληλους ρόλους για την τήρηση της εν λόγω τεκμηρίωσης.

ε) Το δημόσιο σημείο επαφής θα πρέπει να περιλαμβάνει την ταυτότητα του οργανισμού, τη γεωγραφική διεύθυνση και τα στοιχεία επικοινωνίας, καθώς και πληροφορίες σχετικά με το πότε ο καταναλωτής μπορεί να αναμένει απάντηση.

ζ) Ο οργανισμός θα πρέπει να σχεδιάζει και να εφαρμόζει ελέγχους για την ψηφιακή κληρονομιά των καταναλωτών [31] σε περίπτωση θανάτου ενός καταναλωτή και να τους γνωστοποιεί στους καταναλωτές.

η) Ο οργανισμός θα πρέπει να διασφαλίσει ότι η επικοινωνία περιγράφει τον τρόπο με τον οποίο σχεδιάζει και λειτουργεί τα αντίμετρα ιδιωτικότητας επί της ψηφιακής κληρονομιάς των χρηστών [31] και καθοδήγηση σχετικά με τον τρόπο με τον οποίο οι καταναλωτές μπορούν να εφαρμόσουν αυτούς τα αντίμετρα.

θ) Η πολυλειτουργική ομάδα θα πρέπει να καθορίσει μια περίοδο πριν από την απόσυρση, κατά την οποία οι καταναλωτές θα ενημερωθούν για την προγραμματισμένη απόσυρση του προϊόντος.

ι) Οι πληροφορίες για τον καταναλωτή σχετικά με την απόσυρση του προϊόντος πρέπει να περιλαμβάνουν τα εξής:

— ημερομηνία λήξης/διάρκεια ζωής για τα φυσικά προϊόντα [32],

— επιλογές των καταναλωτών για να συνεχίσουν να χρησιμοποιούν το προϊόν [32],

— οποιαδήποτε καταναλωτικά εναλλακτικά προϊόντα,

— μηχανισμούς σχολίων των καταναλωτών, εάν οι ενέργειες για το τέλος της ζωής των προϊόντων παρουσιάζουν απρόβλεπτες δυσκολίες για τους καταναλωτές,

— το γεγονός ότι ο οργανισμός θα συνεχίσει να διατηρεί/επεξεργάζεται τα ΔΠΧ,

— σκοπός της διατήρησης/επεξεργασίας τωμ ΔΠΧ μετά το τέλος της ζωής του προϊόντος,

— τύπους ΔΠΧ,

— διατήρηση (ή τα κριτήρια που χρησιμοποιούνται για τον καθορισμό της περιόδου διατήρησης).

5.3 Ευθύνη για την παροχή πληροφοριών για την ιδιωτικότητα

5.3.1 Απαίτηση

Το φυσικό πρόσωπο που λογοδοτεί θα πρέπει να διασφαλίζει ότι το υπεύθυνο μέρος που απευθύνεται στον καταναλωτή παρέχει ειδοποιήσεις ή τεκμηρίωση για την προστασία των ΔΠΧ, ώστε οι καταναλωτές να κατανοούν τον τρόπο με τον οποίο θα γίνεται η επεξεργασία των ΔΠΧ τους καθ' όλη τη διάρκεια του κύκλου ζωής των προσωπικών δεδομένων.

5.3.2 Επεξήγηση

Αυτό διασφαλίζει ότι τα προϊόντα που επεξεργάζονται ΔΠΧ σχεδιάζονται με προσοχή και ότι οι καταναλωτές τέτοιων προϊόντων θα έχουν πρόσβαση σε πληροφορίες σχετικά με τον τρόπο επεξεργασίας των ΔΠΧ τους σε τέτοια προϊόντα. Σε ορισμένες περιπτώσεις, το φυσικό πρόσωπο λογοδοσίας με αρμοδιότητες που αφορούν τον καταναλωτή θα είναι το ίδιο με το μέρος που είναι υπεύθυνο για τον σχεδιασμό του προϊόντος (ή των επαναλήψεων/αναβαθμίσεων του προϊόντος).

5.3.3 Οδηγία

α) Οι εν λόγω επικοινωνίες, ειδοποιήσεις ή τεκμηρίωση θα πρέπει να είναι διαθέσιμες στους καταναλωτές πριν από την πώληση ή την άδεια χρήσης του προϊόντος και καθ' όλη τη διάρκεια του κύκλου ζωής του προϊόντος και ΔΠΧ.

β) Η πολυλειτουργική ομάδα θα πρέπει να ενημερώνει τους καταναλωτές, τις πωλήσεις και την υποστήριξη σχετικά με τις ενέργειες προστασίας της ιδιωτικότητας που ενδέχεται να χρειαστεί να λάβουν ως αποτέλεσμα της παύσης των πωλήσεων, της υποστήριξης ή της οργανωτικής επεξεργασίας δεδομένων προϊόντων.

ΣΗΜΕΙΩΣΗ Το ISO/IEC 29184 παρέχει περισσότερες εξηγήσεις σχετικά με τις ορθές πρακτικές που πρέπει να ακολουθούνται για την παροχή ειδοποιήσεων.

5.4 Απόκριση σε ερωτήματα και παράπονα καταναλωτών

5.4.1 Απαίτηση

Το φυσικό πρόσωπο που λογοδοτεί θα πρέπει να παρέχει στο υπεύθυνο μέρος που αντιμετωπίζει τον καταναλωτή, τόσο τους πόρους όσο και τα μέσα κλιμάκωσης για την αποτελεσματική απάντηση σε ερωτήματα και παράπονα των καταναλωτών σχετικά με την επεξεργασία των ΔΠΧ [33] [34] [35] [36] [37].

5.4.2 Επεξήγηση

Καθώς ανακύπτουν ζητήματα που χρήζουν διευκρίνισης, το φυσικό πρόσωπο που λογοδοτεί έχει την υποχρέωση να υποστηρίζει τον καταναλωτή που αντιμετωπίζει το υπεύθυνο μέρος.

5.4.3 Οδηγία

α) Οι πόροι αυτοί πρέπει να περιλαμβάνουν τα εξής:

— εκπαίδευση και τεκμηρίωση για τις οδηγίες των καταναλωτών και των δραστηριοτήτων τεχνικής υποστήριξης (συμπεριλαμβανομένης της διατήρησης της ιδιωτικότητας κατά τη διάρκεια των επιχειρήσεων υποστήριξης),

— Επιλογή συχνών ερωτήσεων (FAQ) σχετικά με τεχνικά ζητήματα και ζητήματα χρήσης από τους καταναλωτές που σχετίζονται με τα αντίμετρα ιδιωτικότητας εντός του προϊόντος,

— ανεξάρτητοι εναλλακτικοί μηχανισμοί που είναι διαθέσιμοι στους καταναλωτές όταν τα παράπονα δεν μπορούν να επιλυθούν άμεσα,

— οδηγίες σχετικά με το πού και πώς μπορεί να απευθυνθεί ο καταναλωτής για βοήθεια.

5.5 Επικοινωνία με ποικιλόμορφους πληθυσμούς καταναλωτών

5.5.1 Απαίτηση

Ο οργανισμός θα πρέπει να επικοινωνεί με τους καταναλωτές μέσω διαφόρων καναλιών, μέσων και γλωσσών στις αγορές για τις οποίες έχει σχεδιαστεί το προϊόν, με τρόπο που δεν περιορίζει τους καταναλωτές να κατανοήσουν το προϊόν, τις ρυθμίσεις απορρήτου και τον τρόπο επεξεργασίας των ΔΠΧ.

5.5.2 Επεξήγηση

Διασφάλιση ότι οι καταναλωτές λαμβάνουν τεκμηρίωση που μπορούν να κατανοήσουν και γνωρίζουν πού μπορούν να λάβουν υποστήριξη και ότι οι δραστηριότητες υποστήριξης θα ανταποκρίνονται στις ανάγκες τους.

Στο πλαίσιο των απαιτήσεων ιδιωτικότητας ήδη από τον σχεδιασμό, ο οργανισμός που σχεδίασε το προϊόν έχει την ευθύνη να διασφαλίσει ότι οι καταναλωτές που αγοράζουν ή χρησιμοποιούν το προϊόν διαθέτουν έναν μηχανισμό μέσω του οποίου μπορούν να επικοινωνούν με τον μεταπωλητή ή τον κατασκευαστικό οργανισμό σχετικά με ερωτήσεις ή παράπονα σχετικά με την ιδιωτικότητα μέχρι και μετά την απόσυρση του προϊόντος, το ονομαστικό τέλος της ζωής ή τον τερματισμό της υποστήριξης.

5.5.3 Οδηγία

α) Οι ρυθμίσεις απορρήτου και τα μέτρα διαχείρισης απορρήτου θα πρέπει να λαμβάνουν υπόψη τα χαρακτηριστικά των καταναλωτών-στόχων, συμπεριλαμβανομένων των ευάλωτων καταναλωτών της ομάδας-στόχου. Ειδικότερα, είναι σημαντικό να λαμβάνονται υπόψη οι ανήλικοι, οι ηλικιωμένοι και τα άτομα με χαμηλό επίπεδο γνώσεων πληροφορικής.

β) Ο οργανισμός θα πρέπει να διασφαλίζει με σύμβαση (εάν πρόκειται για τρίτο μέρος) ή με εσωτερική συμφωνία ΣΕΥ (εάν πρόκειται για μέλος του ίδιου οργανισμού) ότι το υπεύθυνο μέρος που έχει επαφή με τον καταναλωτή παρέχει στους καταναλωτές του προϊόντος ένα μέσο για να υποβάλλουν ερωτήσεις, να υποβάλλουν παράπονα, να ζητούν υποστήριξη ή να αντιμετωπίζουν τα δικαιώματά τους όσον αφορά την ιδιωτικότητα.

γ) Θα πρέπει να συντάσσεται σαφής και εύκολα κατανοητή τεκμηρίωση και να είναι εύκολα προσβάσιμη στους ενδιαφερόμενους καταναλωτές, συμπεριλαμβανομένων των εκτιμήσεων για τους ευάλωτους καταναλωτές και τη γλώσσα των χωρών στις οποίες προωθείται το προϊόν ή η υπηρεσία. Η τεκμηρίωση μπορεί να περιλαμβάνει: έγγραφα σχετικά με τις ρυθμίσεις και τα αντίμετρα ιδιωτικότητας, την επεξεργασία των ΔΠΧ, τον σκοπό και τις σχετικές προστασίες για τη μείωση της βλάβης από την επεξεργασία των ΔΠΧ που σχετίζεται με την προστασία της ιδιωτικότητας.

δ) Η επικοινωνία με τους καταναλωτές θα πρέπει να είναι δυνατή μέσω ποικίλων διαύλων επικοινωνίας, επιτρέποντας σχόλια, ερωτήσεις προς επίλυση και παράπονα.

ε) Η αποτελεσματικότητα των εν λόγω διαύλων θα πρέπει να παρακολουθείται, να επανεξετάζεται και να αναθεωρείται ώστε να διασφαλίζεται ότι παρέχουν αποδεκτή καταναλωτική εμπειρία για τους καταναλωτές του προϊόντος.

5.6 Προετοιμασία επικοινωνιών παραβίασης δεδομένων (data breach)

5.6.1 Απαίτηση

Ο οργανισμός θα πρέπει να δημιουργεί, να δοκιμάζει και να διατηρεί ανθεκτικές ρυθμίσεις για την επικοινωνία με τα ενδιαφερόμενα μέρη μετά από παραβίαση της ιδιωτικότητας.

5.6.2 Επεξήγηση

Η επικοινωνία με τους καταναλωτές των προϊόντων σε περίπτωση παραβίασης της ιδιωτικότητας είναι ζωτικής σημασίας για να διασφαλιστεί ότι αυτοί που επηρεάζονται θα είναι σε θέση να διαχειριστούν τυχόν εναπομείναντες κινδύνους για την ιδιωτικότητα.[36][37] Επιπλέον, οι ρυθμιστικές αρχές μπορούν επίσης να θέσουν προθεσμίες για τους οργανισμούς για την αναφορά παραβιάσεων της ιδιωτικότητας.

ΣΗΜΕΙΩΣΗ Αναφορά στο ISO/IEC 27035-1 και ISO/IEC 27035-2.

5.6.3 Οδηγία

α) Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο να συμπεριλάβει, μεταξύ άλλων, τα εξής:

— ποιο περιεχόμενο καλύπτει η επικοινωνία (π.χ. αιτία, είδος δεδομένων που παραβιάστηκαν, ποιες ενέργειες μπορεί να κάνει ο καταναλωτής, ποιες ενέργειες έγιναν από τον οργανισμό, επαφή για περαιτέρω πληροφορίες),

— ποιο κανάλι επικοινωνίας χρησιμοποιούν για την επικοινωνία με τα άτομα που επηρεάζονται (π.χ. ηλεκτρονικό ταχυδρομείο),

— τι γίνεται αν ο οργανισμός δεν διαθέτει στοιχεία επικοινωνίας,

— ποιος στέλνει την ειδοποίηση και πότε,

— σε ποιες γλώσσες ετοιμάζεται η κοινοποίηση,

— ποιος υπογράφει την επικοινωνία

β) Η επικοινωνία αυτή θα πρέπει να προετοιμάζεται εκ των προτέρων και να αποτελεί μέρος των προετοιμασιών για τη διαχείριση της παραβίασης της ιδιωτικότητας.

6 Απαιτήσεις διαχείρισης ρίσκου (risk management)

6.1 Επισκόπηση

Όπως και άλλοι επιχειρησιακοί κίνδυνοι, η επεξεργασία ΔΠΧ επωφελείται από μια προσέγγιση διαχείρισης κινδύνου [38] [39]. Η προληπτική και αποτελεσματική διαχείριση και ο μετριασμός των κινδύνων παραβίασης ιδιωτικότητας σε μια προσπάθεια να αποτραπεί μια τέτοια ή δυσμενείς συνέπειες, αντικατοπτρίζει την έννοια των απαιτήσεων ιδιωτικότητας ήδη από τον σχεδιασμό. Ο σκοπός της διαχείρισης κινδύνου στο πλαίσιο αυτό είναι ο έλεγχος των κινδύνων παραβίασης της ιδιωτικότητας στους οποίους εκτίθενται οι καταναλωτές σε σχέση με τα εν λόγω καταναλωτικά προϊόντα.

Οι πληροφορίες σχετικά με το οικοσύστημα στο οποίο έχει σχεδιαστεί και λειτουργεί το προϊόν μπορούν να δώσουν πληροφορίες για το εύρος και την κλίμακα του δυνητικού κινδύνου παραβίασης της ιδιωτικότητας. Για παράδειγμα, τα κριτήρια αποδοχής βάσει των οποίων ο οργανισμός μπορεί να αξιολογήσει τη σημασία των κινδύνων παραβίασης της ιδιωτικότητας που εντοπίζονται στην αξιολόγηση κινδύνου, προκειμένου να λάβει αποφάσεις σχετικά με την αποδοχή ή την αντιμετώπιση του κινδύνου. Οι οργανισμοί μπορούν να κοινοποιήσουν τα κριτήρια στα υποκείμενα των δεδομένων και σε άλλα ενδιαφερόμενα μέρη. Όταν η άμεση επικοινωνία δεν είναι εφικτή, μπορούν να χρησιμοποιηθούν μηχανισμοί διαφάνειας και ανατροφοδότησης.

Οι κίνδυνοι προστασίας της ιδιωτικής ζωής που σχετίζονται με τα καταναλωτικά προϊόντα μπορούν να λαμβάνουν υπόψη τα γεγονότα προστασίας της ιδιωτικής ζωής ως πιθανά

προβλήματα που μπορεί να αντιμετωπίσουν τα άτομα, τα οποία προκύπτουν από τις λειτουργίες του συστήματος, του προϊόντος ή της υπηρεσίας με δεδομένα, είτε σε ψηφιακή είτε σε μη ψηφιακή μορφή, μέσω ενός πλήρους κύκλου ζωής, από τη συλλογή των δεδομένων έως τη διάθεσή τους .

Για τις πηγές κινδύνων παραβίασης της ιδιωτικότητας πρέπει να ληφθούν υπόψη κατά τη διάρκεια μιας αξιολόγησης, οι οργανισμοί μπορούν να ανατρέξουν σε εσωτερικά μητρώα κινδύνων, εφόσον χρησιμοποιούνται από τον οργανισμό, και σε εξωτερικούς πόρους [43].

Οποιαδήποτε χρήση των ΔΠΧ των καταναλωτών που σχετίζεται με ένα καταναλωτικό προϊόν, είτε ο καταναλωτής χρησιμοποιεί άμεσα το προϊόν είτε όχι, μπορεί να ενσωματώσει την προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό.

Η καθοδήγηση και οι πόροι για τη διαχείριση του κινδύνου παραβίασης της ιδιωτικότητας [39] [40] [41] [42] [43] [44] εμφανίζονται παγκοσμίως σε διάφορα έγγραφα και πρότυπα και μπορεί να επιβάλλονται από διάφορες αρχές προστασίας δεδομένων [40].

6.2 Διεξαγωγή αποτίμησης κινδύνων παραβίασης της ιδιωτικότητας

6.2.1 Απαίτηση

Ο οργανισμός θα πρέπει να υιοθετεί μια δομημένη προσέγγιση για την αξιολόγηση των κινδύνων παραβίασης της ιδιωτικότητας που αποδεικνύει ότι οι κίνδυνοι παραβίασης της ιδιωτικότητας έχουν ληφθεί επαρκώς υπόψη κατά το σχεδιασμό και τη λειτουργία των αντιμέτρων ιδιωτικότητας καθ' όλη τη διάρκεια του κύκλου ζωής των ΔΠΧ.

6.2.2 Επεξήγηση

Οι αξιολόγηση των κινδύνων παραβίασης της ιδιωτικότητας βοηθούν έναν οργανισμό να εντοπίσει τους κινδύνους παραβίασης της ιδιωτικότητας που δημιουργεί το προϊόν, να τους ιεραρχήσει και να καθορίσει τις κατάλληλες προσεγγίσεις διαχείρισης κινδύνου για την αποδοχή, την αποφυγή, τον μετριασμό, την αντιμετώπιση ή τη μεταφορά κάθε κινδύνου. Οι αποφάσεις αντιμετώπισης του κινδύνου (συμπεριλαμβανομένης της μείωσης του κινδύνου) ή αποδοχής λαμβάνονται με βάση καθορισμένα κριτήρια κινδύνου. Ορισμένοι προσδιορισμένοι κίνδυνοι μπορούν να κλιμακωθούν ή να ανατεθούν σε άλλους για τη λήψη αποφάσεων εκτός του φυσικού προσώπου που λογοδοτεί λόγω έλλειψης εξουσίας ή πόρων. Η διαδικασία αυτή μπορεί να τεκμηριώνεται με διάφορους τρόπους, μεταξύ άλλων με εκτίμηση αντικτύπου ιδιωτικότητας [44][45][45][46].

Υπάρχουν διάφορες εισροές που είναι χρήσιμες για τη διενέργεια αξιολόγησης κινδύνου παραβίασης της ιδιωτικότητας. Σε αυτές περιλαμβάνονται η κατανόηση του οικοσυστήματος στο οποίο θα λειτουργεί το προϊόν, ο καθορισμός κριτηρίων κινδύνου και η επιλογή μιας μεθοδολογίας αξιολόγησης κινδύνου, καθώς και πιο απτές εισροές, όπως ένας χάρτης δεδομένων, περιπτώσεις χρήσης του προϊόντος και ένα σύνολο απαιτήσεων ιδιωτικότητας που αφορούν το προϊόν.

Οι τεκμηριωμένες πληροφορίες παρέχουν τη βάση του πλαισίου, της διαδικασίας και των ορίων για μια τεκμηριωμένη εκτίμηση αντικτύπου ιδιωτικότητας και υποστηρίζουν τη συνεχή διαχείριση του κινδύνου. Οι τεκμηριωμένες πληροφορίες περιλαμβάνουν ρητή τεκμηρίωση των λειτουργικών και μη λειτουργικών απαιτήσεων προστασίας της ιδιωτικότητας. Παραδείγματα τεκμηριωμένων αναπαραστάσεων πληροφοριών περιλαμβάνουν, για παράδειγμα, την τεκμηρίωση των εργασιών και των διαδικασιών συμμόρφωσης σε λογιστικά φύλλα, τα στοιχεία των ιστοριών καταναλωτών, τις περιπτώσεις χρήσης, τις περιπτώσεις κατάχρησης, το σχεδιασμό διεπαφών, το διάγραμμα ροής δεδομένων, τα διαγράμματα ακολουθίας ή τα διαγράμματα δραστηριοτήτων που δείχνουν σαφώς την ενσωμάτωση των απαιτήσεων προστασίας της ιδιωτικότητας, τα διαγράμματα επιχειρηματικών μοντέλων που δείχνουν τις ροές των ΔΠΧ στις τεχνολογικές πλατφόρμες και τα διαγράμματα των αρχιτεκτονικών προστασίας της ιδιωτικότητας. Η οργανωτική τεκμηρίωση που σχετίζεται με την ιδιωτικότητα (π.χ. πολιτικές απορρήτου, εκπαιδευτικό υλικό για την ιδιωτικότητα, τεκμηρίωση του προσωπικού που απευθύνεται σε διαβουλεύσεις για την ιδιωτικότητα) μπορεί να αποτελεί μέρος μιας ευρύτερης, οργανωτικής προσέγγισης διαχείρισης πληροφοριών για την ιδιωτικότητα.

6.2.3 Οδηγία

α) Οι αξιολογήσεις κινδύνου παραβίασης της ιδιωτικότητας θα πρέπει να παράγουν ένα σύνολο κινδύνων κατά προτεραιότητα, ώστε να βοηθούν τους οργανισμούς να σταθμίζουν τα οφέλη της επεξεργασίας των ΔΠΧ έναντι των κινδύνων και για τα άτομα και να καθορίζουν την κατάλληλη αντίδραση (π.χ. αντιμετώπιση του κινδύνου ή αποφάσεις αποδοχής με βάση την ανοχή του οργανισμού σε κινδύνους).

β) Ο οργανισμός θα πρέπει να διεξάγει αξιολόγηση κινδύνου παραβίασης της ιδιωτικότητας πριν από την παραγωγή ή την κυκλοφορία του καταναλωτικού προϊόντος.

γ) Θα πρέπει να παραχθεί ένας χάρτης δεδομένων (data map) ή αρχεία των δραστηριοτήτων επεξεργασίας. Αυτά μπορούν να αποτελέσουν χρήσιμη εισροή, διότι απεικονίζουν το πλαίσιο και τη ροή της επεξεργασίας των ΔΠΧ, συμπεριλαμβανομένων πιθανών απρόβλεπτων συνεπειών μιας συγκεκριμένης προτεινόμενης ροής, όπως η απροσδόκητη ένωση δεδομένων καταγραφής (logs) μέσω ενός κοινού αναγνωριστικού ή η ακούσια ανάμειξη δεδομένων σε ένα κοινό αποθηκευτικό χώρο (shared storage container), μπορεί να είναι απεικονίζονται με διαφορετικούς τρόπους και μπορούν να περιέχουν διαφορετικά επίπεδα λεπτομέρειας ανάλογα με τις οργανωτικές ανάγκες. Οι χάρτες δεδομένων μπορούν να περιλαμβάνουν το λειτουργικό περιβάλλον, τους ιδιοκτήτες ή τους χειριστές αυτών των στοιχείων, τον συγκεκριμένο τύπο επεξεργασίας κατά τη διάρκεια του κύκλου ζωής των ΔΠΧ και τα συγκεκριμένα στοιχεία των ΔΠΧ που υποβάλλονται σε επεξεργασία κατά τη διάρκεια του κύκλου ζωής του καταναλωτικού προϊόντος.

δ) Οι σχετικές με το προϊόν απαιτήσεις ιδιωτικότητας θα πρέπει να προκύπτουν αρχικά από διάφορες πηγές, όπως το νομικό περιβάλλον (π.χ. νόμοι, κανονισμοί, συμβάσεις), οργανωτικές

πολιτικές ή πολιτιστικές αξίες, σχετικά πρότυπα και αρχές προστασίας της ιδιωτικότητας. Όσο πιο ευαίσθητες είναι οι πληροφορίες ή όσο μεγαλύτερος είναι ο κίνδυνος για τα δικαιώματα των ατόμων, τόσο μεγαλύτερη είναι η υποχρέωση του οργανισμού να λάβει μέτρα για την προστασία των δεδομένων και να αποδείξει ότι αυτό έχει ληφθεί υπόψη και πραγματοποιηθεί κατά τη στιγμή του σχεδιασμού. Οι απαιτήσεις αυτές επικαιροποιούνται ή επεκτείνονται με βάση τα αποτελέσματα των αξιολογήσεων κινδύνου παραβίασης της ιδιωτικότητας.

ε) Ο οργανισμός θα πρέπει να αξιολογεί τους κινδύνους παραβίασης της ιδιωτικότητας που προκύπτουν από τη χρήση τρίτων, συμπεριλαμβανομένων εκείνων στους οποίους μεταβιβάζονται τα ΔΠΧ στο πλαίσιο του κύκλου ζωής του προϊόντος.

ζ) Κίνδυνοι παραβίασης της ιδιωτικότητας για την λήξη του προϊόντος θα πρέπει να εξετάζονται και τα ΔΠΧ σε όλο το οικοσύστημα του προϊόντος.

η) Ο οργανισμός θα πρέπει να αξιολογεί τους κινδύνους διατήρησης των ΔΠΧ που σχετίζονται με το προϊόν μετά την απόσυρση και μετά το τέλος της χρήσης από τον καταναλωτή.

θ) Οι πιθανοί κίνδυνοι παραβίασης της ιδιωτικότητας που ενέχει η χρησιμοποιούμενη τεχνολογία θα πρέπει επίσης να αποτελούν στοιχείο της αξιολόγησης κινδύνου παραβίασης της ιδιωτικότητας, ιδίως όταν ενσωματώνονται νέες τεχνολογίες στο προϊόν.

ι) Οι ανάγκες των καταναλωτών για την ιδιωτικότητα μπορούν να αποτελέσουν χρήσιμες εισροές για την αξιολόγηση των κινδύνων παραβίασης της ιδιωτικότητας. Οι οργανισμοί θα πρέπει να εξετάζουν τα όσα είναι γνωστά σχετικά με τα συμφέροντα των ατόμων για την ιδιωτικότητα ως χρήσιμα στοιχεία για τη διαδικασία αξιολόγησης των κινδύνων παραβίασης της ιδιωτικότητας.

6.3 Αποτίμηση των δυνατοτήτων της ιδιωτικότητας τρίτων μερών

6.3.1 Απαίτηση

Ο οργανισμός θα πρέπει να λαμβάνει υπόψη τις ικανότητες διαχείρισης του κινδύνου τηε ιδιωτικότητας των τρίτων που επεξεργάζονται τα ΔΠΧ, να σχεδιάζουν ή λειτουργούν τα αντίμετρα ιδιωτικότητας.

6.3.2 Επεξήγηση

Η χρήση των ΔΠΧ σε ένα καταναλωτικό προϊόν μπορεί να είναι πολύπλοκη, ιδίως όταν εμπλέκονται πολλοί ενδιαφερόμενοι και απαιτήσεις. Για παράδειγμα, ένας "εικονικός βοηθός" μπορεί να περιλαμβάνει προϊόντα ή συστήματα που λειτουργούν στο σπίτι (οικιακός εξοπλισμός) καθώς και συστήματα που λειτουργούν εξωτερικά (οργανωτικοί διακομιστές), με κάθε στοιχείο να λειτουργεί σε πολλαπλούς κύκλους ζωής. Πέρα από τον κύκλο ζωής της φυσικής οντότητας του καταναλωτικού προϊόντος, μπορεί να εμπλέκονται και άλλοι κύκλοι ζωής, όπως ο κύκλος ζωής των ΔΠΧ, οι κύκλοι ζωής του οργανωτικού διακομιστή, ο κύκλος ζωής της ανάπτυξης του συστήματος κ.λπ. Κάθε κύκλος ζωής μπορεί να περιλαμβάνει πολυλειτουργική συνεργασία σε δραστηριότητες όπως ο έλεγχος ποιότητας και η πιστοποίηση

που επηρεάζουν άλλα στοιχεία ανάπτυξης ή λειτουργίας του προϊόντος. Η λειτουργία ενός καταναλωτικού προϊόντος μπορεί επομένως να περιλαμβάνει ένα πολύπλοκο δίκτυο ενδιαφερομένων και απαιτήσεων, δημιουργώντας την ανάγκη προσδιορισμού, ευθυγράμμισης και συντονισμού των ρόλων και των αρμοδιοτήτων των ενδιαφερομένων στο οικοσύστημα.

Όταν τρίτα μέρη επεξεργάζονται ΔΠΧ για την υποστήριξη του κύκλου ζωής του προϊόντος, η επεξεργασία τους μπορεί να ληφθεί υπόψη κατά τον καθορισμό του κύκλου ζωής των ΔΠΧ και των σχετικών αντιμέτρων ιδιωτικότητας. Αυτό μπορεί να σημαίνει ότι ο κύκλος ζωής των ΔΠΧ παρατείνεται λόγω τρίτων που επεξεργάζονται τα ΔΠΧ πριν από την έναρξη ή μετά το τέλος του κύκλου ζωής του προϊόντος, συμπεριλαμβανομένων εκείνων στους οποίους μεταβιβάζονται τα ΔΠΧ.

6.3.3 Οδηγία

α) Οι ικανότητες προστασίας της ιδιωτικότητας των τρίτων μερών θα πρέπει να αξιολογούνται μέσω κατάλληλης δέουσας επιμέλειας, αξιολόγησης κινδύνων και συμφωνιών που καθορίζουν τις υποχρεώσεις, τις ευθύνες και την επανεξέταση των επιδόσεών τους, συμπεριλαμβανομένων ελέγχων και αναθεωρήσεων.

β) Ο ρόλος των τρίτων σε αυτή τη διαδικασία είναι κεντρικός. Μπορούν να ενέχουν ιδιαίτερους κινδύνους παραβίασης της ιδιωτικότητας και να παρέχουν ιδιαίτερα αντίμετρα ιδιωτικότητας, τα οποία μπορούν να επηρεάσουν σημαντικά τους κινδύνους παραβίασης της ιδιωτικότητας που ενέχει το προϊόν. Ως εκ τούτου, τα τρίτα μέρη θα πρέπει να παρέχουν πληροφορίες που θα επιτρέψουν στον οργανισμό να αποσαφηνίσει αυτούς τους κινδύνους. Η εν λόγω ανταλλαγή πληροφοριών θα πρέπει να αποτελεί μέρος κάθε σύμβασης ή συμφωνίας επιπέδου υπηρεσιών με το τρίτο μέρος, συμπεριλαμβανομένων εκείνων στους οποίους μεταφέρονται τα ΔΠΧ.

γ) Ο οργανισμός θα πρέπει να εφαρμόσει τεχνικούς μηχανισμούς διακυβέρνησης από τρίτους και λειτουργικές διαδικασίες για τη ρύθμιση της κοινής χρήσης δεδομένων και των κινδύνων παραβίασης της ιδιωτικότητας.

δ) Οι σχέσεις του οργανισμού με τρίτους, συμπεριλαμβανομένων εκείνων στους οποίους μεταβιβάζονται τα ΔΠΧ, θα πρέπει να βασίζονται σε συμβάσεις ή άλλα μέτρα.

ε) Ο οργανισμός θα πρέπει να συμπεριλάβει στις συμβάσεις με τρίτους ρήτρες που καθορίζουν τις υποχρεώσεις του τρίτου μέρους σε περίπτωση που ο καταναλωτής ασκήσει οποιαδήποτε δικαιώματα σε προσωπικές πληροφορίες ή αν το προϊόν αποσυρθεί.

ζ) Οι επιδόσεις των τρίτων μερών, συμπεριλαμβανομένων εκείνων στα οποία μεταβιβάζονται τα ΔΠΧ, θα πρέπει να αξιολογούνται περιοδικά με κατάλληλα μέσα (π.χ. εξέταση εκθέσεων, έλεγχοι) και να ακολουθούνται από κατάλληλες ενέργειες.

η) Οι μη-αποδεκτές επιδόσεις θα πρέπει να επανεξετάζονται με το τρίτο μέρος και να διορθώνονται όπως απαιτείται.

6.4 Καθορισμός και τεκμηρίωση των απαιτήσεων για τα αντίμετρα ιδιωτικότητας

6.4.1 Απαίτηση

Ο οργανισμός θα πρέπει να καθορίζει και να τεκμηριώνει τις απαιτήσεις ιδιωτικότητας που θα καθορίζουν το σχεδιασμό και τη λειτουργία των αντιμέτρων ιδιωτικότητας καθ' όλη τη διάρκεια του κύκλου ζωής των ΔΠΧ.

6.4.2 Επεξήγηση

Οι απαιτήσεις της ιδιωτικότητας αποτελούν τη βάση για το σχεδιασμό ή την επιλογή των αντιμέτρων της ιδιωτικότητας. Οι τεχνικές δραστηριότητες περιλαμβάνουν τον προσδιορισμό των απαιτήσεων για την ανάπτυξη και την εφαρμογή των αντιμέτρων της ιδιωτικότητας για την επίτευξη των επιθυμητών αποτελεσμάτων προστασίας της ιδιωτικότητας. Η παρούσα απαίτηση επικεντρώνεται στο τελευταίο.

Τα αντίμετρα (δηλαδή τα μέσα) που επιλέγει ένας οργανισμός για τη διαχείριση των κινδύνων παραβίασης της ιδιωτικότητας ποικίλλουν. Εξαιτίας αυτού, οι καταναλωτές χρειάζονται γενικά πρόσβαση στις πληροφορίες που εξηγούν τον τρόπο με τον οποίο η προστασία της ιδιωτικότητας στο προϊόν διαχειρίζεται και πώς να χειρίζονται τα αντίμετρα ιδιωτικότητας στα οποία έχουν πρόσβαση σε ένα συγκεκριμένο προϊόν μέχρι και τη λήξη του προϊόντος.

Πολλά άλλα πρότυπα διαχείρισης, τεχνολογίας, ποιότητας, ασφάλειας και άλλα πρότυπα που σχετίζονται με τις πληροφορίες περιλαμβάνουν αντίμετρα ιδιωτικότητας. Τα αντίμετρα ιδιωτικότητας που προέρχονται από οποιαδήποτε σχετική πηγή μπορούν να ενσωματωθούν στη διαδικασία σχεδιασμού του προϊόντος.

6.4.3 Οδηγία

α) Οι απαιτήσεις θα πρέπει να καθορίζονται με βάση τα αποτελέσματα της αξιολόγησης κινδύνου παραβίασης της ιδιωτικότητας.

β) Τα αποτελέσματα της αξιολόγησης κινδύνου παραβίασης της ιδιωτικότητας μπορεί να οδηγήσουν σε αλλαγές στο αρχικό σύνολο των αντιμέτρων της ιδιωτικότητας που αφορούν το προϊόν.

γ) Τα αντίμετρα ιδιωτικότητας που σχετίζονται με οποιοδήποτε προϊόν από το οποίο εξαρτάται το προϊόν στο πεδίο εφαρμογής θα πρέπει να επανεξεταστούν ως προς τη συνοχή τους με τον επιδιωκόμενο σκοπό.

δ) Τα αποτελέσματα της αξιολόγησης κινδύνου θα πρέπει να τροφοδοτούν ένα επικαιροποιημένο σύνολο τεκμηριωμένων απαιτήσεων για τα αντίμετρα της ιδιωτικότητας.

ε) Οι εκτιμώμενες ανάγκες και προτιμήσεις των καταναλωτών όσον αφορά την ιδιωτικότητα θα πρέπει επίσης να λαμβάνονται υπόψη κατά τον καθορισμό των απαιτήσεων για τα αντίμετρα της ιδιωτικότητας.

ζ) Η πολυλειτουργική ομάδα θα πρέπει να εντοπίσει κάθε καταναλωτική χρήση των οργανωτικών πόρων επεξεργασίας που συνεχίζεται και μετά την παύση των πωλήσεων ή της υποστήριξης του προϊόντος.

6.5 Παρακολούθηση και επικαιροποίηση της αποτίμησης κινδύνων

6.5.1 Απαίτηση

Μετά την κυκλοφορία του προϊόντος στην αγορά, ο οργανισμός θα πρέπει να παρακολουθεί τους κινδύνους παραβίασης της ιδιωτικότητας που συνδέονται με το χρησιμοποιούμενο προϊόν και να επικαιροποιεί το σχεδιασμό και τη λειτουργία των αντιμέτρων της ιδιωτικότητας, όπου χρειάζεται, ώστε να ικανοποιούνται συνεχώς οι απαιτήσεις προστασίας της ιδιωτικότητας.

6.5.2 Επεξήγηση

Αλλαγές στο προϊόν ή στο οργανωτικό πλαίσιο μπορεί να προκαλέσουν νέους κινδύνους για παραβίασης της ιδιωτικότητας ή να καταστήσουν αναγκαία την επικαιροποίηση των τεκμηριωμένων πληροφοριών, της αξιολόγησης κινδύνου παραβίασης της ιδιωτικότητας, των απαιτήσεων προστασίας της ιδιωτικότητας και των εφαρμοζόμενων αντιμέτρων στο πλαίσιο της διαχείρισης του κινδύνου προστασίας της ιδιωτικότητας. Οι επικαιροποιήσεις μπορεί να είναι: α) επικαιροποιημένες εισροές για την αξιολόγησης κινδύνου παραβίασης της ιδιωτικότητας, β) επικαιροποιημένοι κίνδυνοι παραβίασης της ιδιωτικότητας και καθορισμοί αντιμετώπισης ή αποδοχής του κινδύνου, γ) επικαιροποιημένη εφαρμογή των αντιμέτρων της ιδιωτικότητας, συμπεριλαμβανομένης της επαναξιολόγησης της καταλληλότητας των αντιμέτρων της ιδιωτικότητας και της δυνατότητας συμπερίληψης ή ανάπτυξης νέων αντιμέτρων. Κατά την εφαρμογή της διαδικασίας σχεδιασμού έως τη φάση της απόσυρσης του κύκλου ζωής του προϊόντος, οι δυνατότητες μπορεί να περιλαμβάνουν ότι ο καταναλωτής σταματά σκόπιμα και μόνιμα να χρησιμοποιεί το προϊόν (παραδίδει το προϊόν για επαναχρησιμοποίηση ως δώρο ή μέσω μιας αγοράς μεταχειρισμένων προϊόντων ή πεθαίνει).

6.5.3 Οδηγία

α) Ο οργανισμός θα πρέπει να μοντελοποιήσει τη χρήση του προϊόντος κατά τη φάση του σχεδιασμού, συμπεριλαμβανομένης της χρήσης μετά την κυκλοφορία και μετά την απόσυρση, και να αξιολογήσει κατά πόσον, όταν το προϊόν αποτύχει, εξακολουθεί να πληροί τις απαιτήσεις της ιδιωτικότητας.

β) Οι επικαιροποιήσεις των τεκμηριωμένων πληροφοριών, της αξιολόγησης του κινδύνου παραβίασης της ιδιωτικότητας, των απαιτήσεων της ιδιωτικότητας και της λειτουργίας αντιμέτρων της ιδιωτικότητας θα πρέπει να είναι επαναληπτικές κατά τη διάρκεια του κύκλου ζωής του προϊόντος.

γ) Ο οργανισμός θα πρέπει να διασφαλίζει ότι κάθε έκδοση, και το σύνολο όλων των εκδόσεων του προϊόντος, ότι οι κίνδυνοι παραβίασης της ιδιωτικότητας διαχειρίζονται με τρόπο που να αποτρέπει την απώλεια αποτελεσματικότητας των αντιμέτρων της ιδιωτικότητας.

δ) Η παρακολούθηση μπορεί να αφορά άμεσα αλλαγές στο προϊόν και τη σχετική επεξεργασία ΔΠΧ, ή μπορεί να είναι εξωτερική του προϊόντος, όπως οι οργανωτικοί στόχοι ή το νομικό και κανονιστικό περιβάλλον. Οι ενημερώσεις του προϊόντος μετά την κυκλοφορία του μπορεί να απαιτούν νέα ή επικαιροποιημένη επικοινωνία με τους καταναλωτές. Ο οργανισμός θα πρέπει να διασφαλίζει ότι αξιολογούνται νέοι ή αναδυόμενοι κίνδυνοι για την ιδιωτικότητα, συμπεριλαμβανομένων τυχόν ανατροφοδοτήσεων και παραπόνων των καταναλωτών.

ε) Ο οργανισμός θα πρέπει να διασφαλίζει ότι τυχόν αλλαγές στη λειτουργικότητα του προϊόντος ή άλλες ρυθμίσεις δεν οδηγούν σε απώλεια της αποτελεσματικότητας της λειτουργίας των αντιμέτρων της ιδιωτικότητας κατά τρόπο που να αυξάνει τους υπολειπόμενους κινδύνους παραβίασης της ιδιωτικότητας, χωρίς να λαμβάνονται υπόψη πρόσθετα ή νέα αντισταθμιστικά αντίμετρα ή βελτιώσεις των αντιμέτρων.

6.6 Συμπερίληψη των κινδύνων της ιδιωτικότητας στον σχεδιασμό της ανθεκτικότητας της κυβερνοασφάλειας (cybersecurity resilience)

6.6.1 Απαίτηση

Ο οργανισμός θα πρέπει να λαμβάνει υπόψη τον κίνδυνο για τα ΔΠΧ στις πολιτικές και τις διαδικασίες του για την ασφάλεια των πληροφοριών.

ΣΗΜΕΙΩΣΗ Μεταξύ των εκτιμήσεων είναι και ο αντίκτυπος των διαταραχών στην ανθεκτικότητα των αντιμέτρων της ιδιωτικότητας.

6.6.2 Επεξήγηση

Η οργανωτική ανθεκτικότητα είναι η ικανότητα ενός οργανισμού να απορροφά και να προσαρμόζεται σε ένα μεταβαλλόμενο περιβάλλον. Οι λειτουργίες των οργανισμών και οι αλυσίδες εφοδιασμού προϊόντων μπορεί να υπόκεινται σε καθημερινές διαταραχές. Εάν τα αντίμετρα πρόκειται να λειτουργούν συνεχώς, θα πρέπει να γίνονται προετοιμασίες για την πρόληψη, τον εντοπισμό, την ανάκαμψη και την επανάληψη των διαταραχών που επηρεάζουν τα ΔΠΧ.

Η συνθετότητα είναι μια αρχή σχεδιασμού συστημάτων που ασχολείται με τις αλληλεπιδράσεις των συστατικών στοιχείων. Για παράδειγμα, η προστασία της ιδιωτικότητας δεν διατηρείται απαραίτητα επειδή ένα σύστημα μπορεί να ενσωματωθεί στο προϊόν και μερικές φορές το προϊόν χρησιμοποιείται ως συστατικό ενός μεγαλύτερου συστήματος. Ως εκ τούτου, η κατανόηση των κινδύνων για την ιδιωτικότητα εντός του συστήματος καθώς και ως συστατικό στοιχείο άλλων συστημάτων είναι απαραίτητη κατά τον σχεδιασμό ανθεκτικότητας στην κυβερνοασφάλεια.

6.6.3 Οδηγία

Οδηγίες σχετικά με την οργανωτική ανθεκτικότητα μπορείτε να βρείτε στο ISO 22316 [46].

7 Ανάπτυξη, αξιοποίηση και λειτουργία σχεδιασμένων αντιμέτρων της ιδιωτικότητας

7.1 Επισκόπηση

Τα αντίμετρα της ιδιωτικότητας σχεδιάζονται, αναπτύσσονται, διαχειρίζονται και λειτουργούν κατά τη διάρκεια του κύκλου ζωής ενός προϊόντος, ώστε να διασφαλίζεται ότι επιτυγχάνονται (και συνεχίζουν να επιτυγχάνονται) οι επιδιωκόμενοι στόχοι της ιδιωτικότητας στο προϊόν και ότι τα αντίμετρα αυτά δεν υποβαθμίζονται ή δεν λειτουργούν με μη προβλεπόμενους τρόπους.

Οι εξελισσόμενες απαιτήσεις της ιδιωτικότητας ή οι εξελισσόμενες ανάγκες ή προτιμήσεις των καταναλωτών για την της ιδιωτικότητα μπορούν επίσης να προκαλέσουν την ανάγκη σχεδιασμού και εφαρμογής νέων αντιμέτρων ιδιωτικότητας κατά τη διάρκεια του κύκλου ζωής ενός καταναλωτικού προϊόντος [47].

Η συντονισμένη προσέγγιση του σχεδιασμού, της ανάπτυξης, της διάθεσης, της διαχείρισης, της λειτουργίας και της εξέλιξης των αντιμέτρων ιδιωτικότητας ενός προϊόντος συμβάλλει στην αποδοτικότητα, την αποτελεσματικότητα και τη συνεχή προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό.

Η ευκαιρία για μεγαλύτερη αποτελεσματικότητα και αποδοτικότητα αυξάνεται εάν η ανάπτυξη, η ανάπτυξη, η διαχείριση και η λειτουργία των αντιμέτρων της ιδιωτικότητας ενσωματωθεί στη συνολική προσέγγιση ενός οργανισμού για την ανάπτυξη, τη διαχείριση, τη λειτουργία και την εξέλιξη των αντιμέτρων.

Η διαχείριση αυτών των ελέγχων μπορεί να αποτελεί μέρος των συστημάτων διαχείρισης υπηρεσιών (SMS) ενός οργανισμού, όπως ορίζεται στο ISO 20000-1 [48].

Σημείωση Το ISO 20000-1 καθορίζει τις απαιτήσεις ενός οργανισμού για την καθιέρωση, εφαρμογή, διατήρηση και συνεχή βελτίωση ενός συστήματος διαχείρισης υπηρεσιών (SMS). Οι απαιτήσεις περιλαμβάνουν την οργάνωση, το σχεδιασμό, τη μετάβαση, την παροχή και τη βελτίωση των υπηρεσιών για την ικανοποίηση των απαιτήσεων των υπηρεσιών και την παροχή αξίας.

7.2 Ενσωμάτωση του σχεδιασμού και της λειτουργίας των αντιμέτρων της ιδιωτικότητας στους κύκλους ανάπτυξης και διαχείρισης του προϊόντος

7.2.1 Απαίτηση

Ο οργανισμός θα πρέπει να ενσωματώνει το σχεδιασμό και τη λειτουργία των αντιμέτρων της ιδιωτικότητας για το καταναλωτικό προϊόν στον κύκλο ανάπτυξης και διαχείρισης του προϊόντος.

7.2.2 Επεξήγηση

Ο σχεδιασμός και η λειτουργία των αντιμέτρων της ιδιωτικότητας υλοποιεί τον προβλεπόμενο σχεδιασμό ιδιωτικότητας του προϊόντος και τις συναφείς πρακτικές, διαδικασίες και πολιτικές

που απαιτούνται για την επίτευξη των στόχων απορρήτου του προϊόντος. Η συγκεκριμένη προσέγγιση ανάπτυξης και διαχείρισης και η μηχανική των ελέγχων ποικίλλουν ανάλογα με τη φύση του προϊόντος και το πλαίσιο στο οποίο σχεδιάζεται να χρησιμοποιηθεί. Οι απαιτήσεις της διαδικασίας για το σχεδιασμό, την κατασκευή, την ανάπτυξη και τη λειτουργία νέων ή τροποποιημένων αντιμέτρων της ιδιωτικότητας μπορούν να τεκμηριωθούν ως εξής [49]:

— Απαιτήσεις ιδιωτικότητας και περιγραφή αντιμέτρων,

— Πληροφοριακά συστήματα και εργαλεία διαχείρισης που υποστηρίζουν την τεκμηρίωση του κύκλου ζωής του οργανισμού και τη διαχείριση των απαιτήσεων και των αντιμέτρων,

— Τεχνολογικές αρχιτεκτονικές ελέγχου της ιδιωτικότητας,

— Διοικητικές και άλλες διαχειριστικές διαδικασίες που υποστηρίζουν τα αντίμετρα ιδιωτικότητας,

— Μέθοδοι μέτρησης και μετρικές που περιγράφουν τους αναπτυγμένους ελέγχους, την ανάπτυξή τους και την απόδοσή τους σε λειτουργία.

7.2.3 Οδηγία

α) Ο οργανισμός θα πρέπει να διατηρεί μια ενιαία πηγή συνεπών και ακριβών πληροφοριών σχετικά με όλα τα αντίμετρα ιδιωτικότητας, η οποία θα είναι ευρέως διαθέσιμη σε όσους είναι εξουσιοδοτημένοι να έχουν πρόσβαση σε αυτήν.

β) Ο οργανισμός θα πρέπει να διασφαλίζει ότι όλα τα τρέχοντα και προγραμματισμένα αντίμετρα ιδιωτικότητας παρέχονται για την ικανοποίηση των απαιτήσεων της ιδιωτικότητας. Αυτό επιτυγχάνεται μέσω ενός συνεχούς κύκλου διαπραγμάτευσης, συμφωνίας, παρακολούθησης, υποβολής εκθέσεων και αναθεώρησης των αντιμέτρων της ιδιωτικότητας σε σχέση με τις απαιτήσεις της ιδιωτικότητας και μέσω της ανάληψης δράσεων για τη διόρθωση ή τη βελτίωση της λειτουργίας των αντιμέτρων ιδιωτικότητας.

γ) Ο οργανισμός θα πρέπει να διασφαλίζει τη συνεχή λειτουργία των αντιμέτρων της ιδιωτικότητας με τη διαχείριση των κινδύνων που μπορούν να επηρεάσουν τις εν λόγω υπηρεσίες και, ως εκ τούτου, να εξασφαλίζει ελάχιστα επίπεδα υπηρεσιών που σχετίζονται με τη συνέχεια (βλ. Clause 6)

δ) Ο οργανισμός θα πρέπει να διασφαλίζει ότι η ασφάλεια (π.χ. εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) των αντιμέτρων της ιδιωτικότητας ευθυγραμμίζεται με τους προσδιορισμένους στόχους της ιδιωτικότητας.

ε) Ο οργανισμός θα πρέπει να διασφαλίζει ότι όλες οι συμβάσεις και συμφωνίες με τρίτους υποστηρίζουν τις απαιτήσεις της ιδιωτικότητας του προϊόντος και ότι όλα τα τρίτα μέρη αποδεικνύουν τις συμβατικές τους δεσμεύσεις.

ζ) Ο οργανισμός θα πρέπει να συνεργάζεται στενά με όσους συνεισφέρουν την εμπειρία τους από τρίτους, ώστε να διασφαλίζεται ότι η συμμετοχή τους διατηρείται σε όλο τον κύκλο ζωής των ΔΠΧ.

η) Τα τρίτα μέρη θα πρέπει να παρέχουν πληροφορίες που θα επιτρέπουν στον οργανισμό να διευκρινίζει τα ζητήματα της ιδιωτικότητας που προκύπτουν, και αυτή η ανταλλαγή πληροφοριών θα πρέπει να αποτελεί μέρος της σύμβασης και της συμφωνίας επιπέδου υπηρεσιών με το τρίτο μέρος.

7.3 Σχεδιασμός αντιμέτρων ιδιωτικότητας

7.3.1 Απαίτηση

Ο οργανισμός θα πρέπει να σχεδιάζει τα αντίμετρα ιδιωτικότητας ώστε να ανταποκρίνονται στις απαιτήσεις που προκύπτουν από την αξιολόγηση κινδύνου παραβίασης της ιδιωτικότητας.

7.3.2 Επεξήγηση

Οι απαιτήσεις πληρούνται από τους λειτουργικούς ελέγχους. Ο τρόπος με τον οποίο σχεδιάζεται το αντίμετρο βασίζεται στον κίνδυνο και στο επιθυμητό αποτέλεσμα ή στον στόχο της εφαρμογής του αντιμέτρου. Τα εφαρμοζόμενα αντίμετρα συνδυάζονται για να δημιουργήσουν ικανότητες προστασίας της ιδιωτικότητας.

Τα αντίμετρα ιδιωτικότητας για το προϊόν και τη σχετική επεξεργασία των ΔΠΧ περιλαμβάνουν, μεταξύ άλλων, τα εξής :

— Αντίμετρα ιδιωτικότητας που προκύπτουν από την υπάρχουσα γνώση του οργανισμού, συμπεριλαμβανομένης της γνώσης που προέρχεται από τη διαχείριση της συγκατάθεσης και τη διαχείριση των προτιμήσεων απορρήτου,

— Αντίμετρα ιδιωτικότητας που πληρούν τις απαιτήσεις ή/και αντιμετωπίζουν τους κινδύνους που εντοπίστηκαν κατά την αξιολόγηση κινδύνου παραβίασης της ιδιωτικότητας.

7.3.3 Οδηγία

α) Ο οργανισμός θα πρέπει να σχεδιάζει αντίμετρα ιδιωτικότητας ώστε να ανταποκρίνεται στις απαιτήσεις και τις ανάγκες των καταναλωτών για την προστασία της ιδιωτικότητας καθ' όλη τη διάρκεια της ζωής των ΔΠΧ [34] [50] [51] [52].

β) Ο οργανισμός θα πρέπει να σχεδιάσει αντίμετρα ιδιωτικότητας για να ικανοποιήσει τις απαιτήσεις του και να αντιμετωπίσει τους κινδύνους που εντοπίστηκαν κατά την αξιολόγηση κινδύνου παραβίασης της ιδιωτικότητας.

7.4 Εφαρμογή αντιμέτρων ιδιωτικότητας

7.4.1 Απαίτηση

Ο οργανισμός θα πρέπει να σχεδιάζει, να αναπτύσσει, να δοκιμάζει, να επικυρώνει και να εφαρμόζει τα αντίμετρα της ιδιωτικότητας για την ικανοποίηση των απαιτήσεων ιδιωτικότητας

και να παρακολουθεί την αποτελεσματικότητά τους καθ' όλη τη διάρκεια του κύκλου ζωής των ΔΠΧ.

7.4.2 Επεξήγηση

Η μηχανική, η ανάπτυξη, η δοκιμή και η επικύρωση των αντιμέτρων της ιδιωτικότητας διασφαλίζει ότι το προϊόν, η σχετική επεξεργασία των ΔΠΧ και τα αντίμετρα της ιδιωτικότητας ανταποκρίνονται στους στόχους και τις απαιτήσεις προστασίας της ιδιωτικότητας του οργανισμού.

7.4.3 Οδηγία

α) Ο οργανισμός θα πρέπει να εφαρμόζει αντίμετρα για την εκπλήρωση των απαιτήσεων καθ' όλη τη διάρκεια του κύκλου ζωής των προϊόντων και του κύκλου ζωής των ΔΠΧ

β) Η εφαρμογή του αντίμετρου ιδιωτικότητας θα πρέπει να συνάδει με την επιχειρησιακή αρχιτεκτονική του οργανισμού και τις σχετικές αρχιτεκτονικές ασφάλειας και απορρήτου.

γ) Ο οργανισμός θα πρέπει να χρησιμοποιεί βέλτιστες πρακτικές κατά την εφαρμογή των αντιμέτρων, συμπεριλαμβανομένων των μεθοδολογιών, εννοιών και αρχών της μηχανικής της ιδιωτικότητας.

ΣΗΜΕΙΩΣΗ Έγγραφα όπως οι παραπομπές [52] [49] [53] παρέχουν περισσότερες πληροφορίες σχετικά με τις βέλτιστες πρακτικές.

δ) Οι αξιολογήσεις κινδύνου θα πρέπει να καθοδηγούν και να ενημερώνουν τις αποφάσεις σχετικά με το κόστος, το όφελος και τους συμβιβασμούς κινδύνου κατά τη χρήση διαφορετικών τεχνολογιών ή πολιτικών για την εφαρμογή του αντιμέτρου [54].

ε) Τα αντίμετρα ιδιωτικότητας θα πρέπει να ελέγχονται για να διασφαλίζεται ότι πληρούν τις απαιτήσεις της ιδιωτικότητας.

ζ) Η βιωσιμότητα της εφαρμογής των προτεινόμενων αντιμέτρων προστασίας της ιδιωτικότητας θα πρέπει να περιλαμβάνεται στο πλαίσιο κάθε διαδικασίας αξιολόγησης των επιλογών προϊόντος για πιθανά νέα προϊόντα. Όταν η αξιολόγηση της βιωσιμότητας υποδεικνύει ότι το προϊόν δεν μπορεί να ανταποκριθεί στις απαιτήσεις της ιδιωτικότητας, το προϊόν μπορεί να επανεξεταστεί ή να εγκαταλειφθεί.

η) Το αποτέλεσμα θα πρέπει να είναι ένα σύνολο εφαρμοζόμενων αντιμέτρων της ιδιωτικότητας που πληρούν τις καθορισμένες απαιτήσεις και είναι έτοιμα για μετάβαση στην υπηρεσία.

7.5 Σχεδιασμός δοκιμών αντιμέτρων ιδιωτικότητας

7.5.1 Απαίτηση

Ο οργανισμός θα πρέπει να αναλαμβάνει δοκιμές αντιμέτρων και να θέτει κριτήρια αποδοχής των αντιμέτρων που αποδεικνύουν την προβλεπόμενη λειτουργική αποτελεσματικότητα των αντιμέτρων της ιδιωτικότητας καθ' όλη τη διάρκεια του κύκλου ζωής των ΔΠΧ.

7.5.2 Επεξήγηση

Η διασφάλιση της αποτελεσματικότητας των αντιμέτρων της ιδιωτικότητας απαιτεί τη συνολική δοκιμή του σχεδιασμού και της προβλεπόμενης λειτουργίας κάθε αντίμετρου της ιδιωτικότητας που πρέπει να ελεγχθεί (π.χ. περιπτώσεις χρήσης και κατάχρησης και δοκιμές παλινδρόμησης). Ο σχεδιασμός ενός αντιμέτρου θα δοκιμαστεί κατά την ανάπτυξη του προϊόντος και η λειτουργία του αντιμέτρου θα δοκιμαστεί πριν από την κυκλοφορία και καθ' όλη τη διάρκεια της περιόδου υποστήριξης μέχρι την απόσυρση και, σε ορισμένες περιπτώσεις, κατά τη διάρκεια της περιόδου μετά την απόσυρση.

7.5.3 Οδηγία

α) Όλες οι δοκιμές του σχεδιασμού και της λειτουργίας των αντιμέτρων της ιδιωτικότητας θα πρέπει να σχεδιάζονται εκ των προτέρων έτσι ώστε να ελέγχονται για την ορθότητά τους σύμφωνα με ένα προκαθορισμένο σχέδιο και να εγκρίνονται σε κατάλληλο επίπεδο διοίκησης.

β) Τα κριτήρια αποδοχής πρέπει επίσης να σχεδιάζονται και να εγκρίνονται εκ των προτέρων.

γ) Η ανάπτυξη των κριτηρίων αποδοχής θα πρέπει να ακολουθεί μια σαφή μεθοδολογία, για παράδειγμα: καθορισμός του αναμενόμενου αποτελέσματος της διαδικασίας προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό (δηλαδή αποτελεσματική προστασία των εκτιμώμενων κινδύνων), καθορισμός των απαιτήσεων της ιδιωτικότητας που πρέπει να εφαρμοστούν για την παροχή αποτελεσματικής προστασίας των κινδύνων (π.χ. περιορισμός του σκοπού, ελαχιστοποίηση των δεδομένων, διαφάνεια κ.λπ.) και καθορισμός των τεχνολογιών ή διαδικασιών που υλοποιούν αποτελεσματικά τις αρχές σχεδιασμού (π.χ. ανωνυμοποίηση δεδομένων, σχεδιασμός προσβάσιμης διεπαφής χρήστη κ.λπ.).

δ) Η δοκιμή θα πρέπει να πληροί τα κριτήρια αποδοχής, εάν το αντίμετρο πρέπει να θεωρηθεί αποτελεσματικό.

ε) Θα πρέπει να καθοριστεί μια μέθοδος δοκιμής για να διασφαλιστεί ότι καθένα από τα κριτήρια πληρούνται αποτελεσματικά (π.χ. διαφορική προστασία της ιδιωτικότητας για να διασφαλιστεί η ελαχιστοποίηση των δεδομένων, μέθοδοι σχεδιασμού της εμπειρίας του χρήστη για να διασφαλιστεί η χρηστικότητα της οπτικής διεπαφής).

ζ) Όταν η δοκιμή δείχνει ότι ένα αντίμετρο δεν είναι αποτελεσματικό, ο σχεδιασμός ή η λειτουργία του θα πρέπει να επανεξεταστεί, να αναθεωρηθεί και να δοκιμαστεί εκ νέου προτού θεωρηθεί ότι είναι αποτελεσματικό στη διαχείριση των κινδύνων παραβίασης της ιδιωτικότητας.

η) Ο οργανισμός θα πρέπει να προβεί σε μοντελοποίηση απειλών για την ιδιωτικότητα με βάση σενάρια δοκιμών σχετικά με τον κίνδυνο της ιδιωτικότητας και των δεδομένων. Θα πρέπει να εξετάσει το ενδεχόμενο να ενισχύσει τις υφιστάμενες διαδικασίες μοντελοποίησης απειλών για την ασφάλεια στην ανάπτυξη, εάν είναι δυνατόν.

θ) Ο οργανισμός θα πρέπει να επανεξετάζει ετησίως τα σχέδια δοκιμών των αντιμέτρων της ιδιωτικότητας για να διασφαλίζει τη βιωσιμότητα και τη συνάφεια.

ι) Οι δοκιμές θα πρέπει να επαναλαμβάνονται σε περίπτωση αλλαγών που μπορεί να έχουν επιπτώσεις στα αντίμετρα ιδιωτικότητας.

κ) Τα προϊόντα υλικού και λογισμικού και οι επιχειρηματικές διαδικασίες θα πρέπει να υιοθετούν μέτρα προστασίας της ιδιωτικότητας, ασφάλειας και ελέγχου.

7.6 Διαχείριση της μετάβασης των αντιμέτρων ιδιωτικότητας

7.6.1 Απαίτηση

Ο οργανισμός θα πρέπει να διασφαλίζει ότι η μετάβαση ενός προϊόντος σε νέα, τροποποιημένα ή αποσυρόμενα αντίμετρα ιδιωτικότητας εξακολουθεί να πληροί τις απαιτήσεις ιδιωτικότητας.

7.6.2 Επεξήγηση

Η μετάβαση του αντιμέτρου διασφαλίζει ότι οι νέα, τροποποιημένα ή αποσυρθέντα αντίμετρα ιδιωτικότητας ανταποκρίνονται στους στόχους του οργανισμού, όπως αυτοί τεκμηριώνονται στα στάδια της στρατηγικής και του σχεδιασμού του προϊόντος κατά τον κύκλο ζωής. Το στάδιο αυτό είναι επίσης υπεύθυνο για τη μετάβαση του προϊόντος από τη μια κατάσταση του κύκλου ζωής στην άλλη (από τον σχεδιασμό στην ανάπτυξη, από την ανάπτυξη στην λειτουργία και από την λειτουργία στο τέλος της ζωής), ενώ παράλληλα ελέγχει τον κίνδυνο και υποστηρίζει την οργανωτική γνώση για τη λήψη αποφάσεων.

7.6.3 Οδηγία

α) Ο οργανισμός θα πρέπει να διασφαλίζει ότι όλα τα σχετικά σχέδια για τη μετάβαση των αντιμέτρων ιδιωτικότητας είναι έτοιμα πριν από τη μετάβαση και ότι οι σχετικές δραστηριότητες υποστήριξης και συντονισμού των αντιμέτρων ιδιωτικότητας διαχειρίζονται ώστε να διασφαλίζεται η ομαλή και επιτυχής μετάβαση των νέων, αλλαγμένων ή αποσυρθέντων αντιμέτρων.

β) Η διαδικασία αλλαγών είναι υπεύθυνη για τον έλεγχο του κύκλου ζωής όλων των αλλαγών προϊόντων, επιτρέποντας την πραγματοποίηση επωφελών αλλαγών με την ελάχιστη δυνατή διαταραχή των προϊόντων που βασίζονται στην τεχνολογία πληροφοριών. Ο οργανισμός θα πρέπει να διασφαλίζει ότι οι αλλαγές διαχειρίζονται συστηματικά ώστε να βελτιστοποιείται η έκθεση στον κίνδυνο παραβίασης της ιδιωτικότητας, να ελαχιστοποιούνται οι επιπτώσεις στην προστασία της ιδιωτικότητας, να επιτυγχάνονται οι υλοποιήσεις με την πρώτη προσπάθεια και να ενημερώνονται έγκαιρα όλα τα ενδιαφερόμενα μέρη. Η δεύτερη διαδικασία, η διαχείριση

αλλαγών, είναι υπεύθυνη για τον έλεγχο του κύκλου ζωής όλων των αλλαγών, επιτρέποντας την πραγματοποίηση επωφελών αλλαγών με την ελάχιστη δυνατή διαταραχή των υπηρεσιών πληροφορικής.

γ) Ο οργανισμός θα πρέπει να διασφαλίζει ότι τα περιουσιακά στοιχεία της τεχνολογίας πληροφοριών που απαιτούνται για την υλοποίηση των αντιμέτρων ιδιωτικότητας ελέγχονται κατάλληλα και ότι ακριβείς και αξιόπιστες πληροφορίες σχετικά με τα εν λόγω περιουσιακά στοιχεία είναι διαθέσιμες όταν και όπου χρειάζονται. Οι πληροφορίες αυτές περιλαμβάνουν λεπτομέρειες σχετικά με τον τρόπο διαμόρφωσης των περιουσιακών στοιχείων και τις σχέσεις μεταξύ τους.

δ) Ο οργανισμός θα πρέπει να είναι υπεύθυνος για το σχεδιασμό, τον προγραμματισμό και τον έλεγχο της κατασκευής, της δοκιμής και της ανάπτυξης των εκδόσεων προϊόντων ιδιωτικότητας, ώστε να παρέχονται όλες οι νέες λειτουργίες ιδιωτικότητας που απαιτούνται από το αναπτυγμένο προϊόν, προστατεύοντας παράλληλα την ακεραιότητα των υφιστάμενων υπηρεσιών ιδιωτικότητας.

ε) Ο οργανισμός θα πρέπει να διασφαλίζει ότι τα υφιστάμενα, νέα ή τροποποιημένα αντίμετρα ιδιωτικότητας επικυρώνονται σύμφωνα με τις προδιαγραφές σχεδιασμού κατά τη διάρκεια της μετάβασης. Ενώ η επικύρωση εξασφαλίζει την ικανοποίηση των απαιτήσεων του οργανισμού, η δοκιμή αφορά την ικανοποίηση των προδιαγραφών. Η προκύπτουσα χρησιμότητα (καταλληλότητα για το σκοπό) και η εγγύηση (καταλληλότητα για χρήση) των αντιμέτρων ιδιωτικότητας που παραδίδονται μέσω της ανάπτυξης θα αντικατοπτρίζει την αποδοτικότητα και την αποτελεσματικότητα της διαδικασίας επικύρωσης.

ζ) Ο οργανισμός θα πρέπει να παρέχει συνεπή και τυποποιημένα μέσα για τον προσδιορισμό της απόδοσης μιας αλλαγής των αντιμέτρων ιδιωτικότητας στο πλαίσιο των πιθανών επιπτώσεων στα επιχειρηματικά αποτελέσματα και στα υφιστάμενα και προτεινόμενα αντίμετρα ιδιωτικότητας. Οι πληροφορίες αυτές επιτρέπουν στη διαχείριση των αλλαγών να λαμβάνει τις κατάλληλες αποφάσεις στο πλαίσιο των στόχων της ιδιωτικότητας.

η) Ο οργανισμός θα πρέπει να διασφαλίζει ότι η συστηματική συλλογή, κατηγοριοποίηση και αποθήκευση δεδομένων, πληροφοριών και γνώσεων που σχετίζονται με τη μετάβαση μεταξύ του σχεδιασμού, της ανάπτυξης και της εφαρμογής του αντίμετρου ιδιωτικότητας και εφαρμογή. Τα βήματα αυτά επιτρέπουν τη διαθεσιμότητα πληροφοριών και δεδομένων στο σωστό μέρος και τη σωστή στιγμή, υποστηρίζουν τεκμηριωμένες αποφάσεις στο μέλλον και βελτιώνουν την αποτελεσματικότητα μειώνοντας την ανάγκη αναδημιουργίας ή επαναδιαβίβασης της υπάρχουσας γνώσης.

7.7 Διαχείριση της λειτουργίας των αντιμέτρων ιδιωτικότητας

7.7.1 Απαίτηση

Ο οργανισμός θα πρέπει να διασφαλίζει ότι οι υπηρεσίες και οι έλεγχοι που επηρεάζουν την ιδιωτικότητα θα λειτουργούν αποτελεσματικά και αποδοτικά, συμπεριλαμβανομένης της

εκπλήρωσης των αιτημάτων των καταναλωτών, της επίλυσης αποτυχιών των υπηρεσιών, της επίλυσης προβλημάτων και της εκτέλεσης συνήθων επιχειρησιακών καθηκόντων.

7.7.2 Επεξήγηση

Η λειτουργία ελέγχου συντονίζει και εκτελεί τις δραστηριότητες και τις διαδικασίες που απαιτούνται για την παροχή και τη διαχείριση των αντιμέτρων ιδιωτικότητας σε συμφωνημένα επίπεδα υπηρεσιών προς τους εσωτερικούς χρήστες του οργανισμού και τους εξωτερικούς καταναλωτές. Η λειτουργία ελέγχου διαχειρίζεται επίσης την τεχνολογία που χρησιμοποιείται για την παροχή και την υποστήριξη των αντιμέτρων ιδιωτικότητας. Σε αυτό το στάδιο πραγματοποιείται η πραγματική αξία του αντιμέτρου από τον οργανισμό, τους καταναλωτές και τους χρήστες. Έτσι, το στάδιο αυτό είναι υπεύθυνο για τη διατήρηση, τη συντήρηση και τη συνεχή βελτίωση των ενεργών αντιμέτρων ιδιωτικότητας σύμφωνα με τις ανάγκες των καταναλωτών.

7.7.3 Οδηγία

α) Ο οργανισμός θα πρέπει να διασφαλίζει την παρακολούθηση, τον εντοπισμό και την αποκατάσταση περιστατικών που επηρεάζουν την ιδιωτικότητα κατά τη λειτουργία του προϊόντος από τον καταναλωτή, ερμηνεύοντας και κατανοώντας τα συμβάντα και καθορίζοντας τις απαιτούμενες ενέργειες ελέγχου και αποκατάστασης.

β) Ο οργανισμός θα πρέπει να αναπτύξει αποτελεσματικές πολιτικές και διαδικασίες διαχείρισης περιστατικών ιδιωτικότητας για να διασφαλίσει τη διατήρηση των συμφωνηθέντων επιπέδων ποιότητας των υπηρεσιών ελέγχου αντιμέτρων ιδιωτικότητας.

γ) Ο οργανισμός θα πρέπει να αποκαθιστά την κανονική λειτουργία του ελέγχου ιδιωτικότητας το συντομότερο δυνατό μετά την ανίχνευση γεγονότων που επηρεάζουν την ιδιωτικότητα, ώστε να ελαχιστοποιούνται οι αρνητικές επιπτώσεις στις λειτουργίες του οργανισμού και στην ιδιωτικότητα των καταναλωτών.

δ) Ο οργανισμός θα πρέπει να παρέχει στους καταναλωτές ένα κανάλι για να ζητούν και να λαμβάνουν τυποποιημένες πληροφορίες και υποστήριξη για τα αντίμετρα ιδιωτικότητας για τους οποίους υπάρχει μια προκαθορισμένη διαδικασία εξουσιοδότησης και εξειδίκευσης. Παρέχει επίσης πληροφορίες στους καταναλωτές σχετικά με τη διαθεσιμότητα της αποκατάστασης των υπηρεσιών αντιμέτρων ιδιωτικότητας και τη διαδικασία για την απόκτηση των υπηρεσιών αντιμέτρων ιδιωτικότητας.

ε) Ο οργανισμός θα πρέπει να διαχειρίζεται τον κύκλο ζωής όλων των προβλημάτων του προϊόντος από τον αρχικό εντοπισμό μέχρι την περαιτέρω διερεύνηση, την τεκμηρίωση και την ενδεχόμενη άρση των προβλημάτων αυτών. Προσπαθεί να ελαχιστοποιήσει τις δυσμενείς επιπτώσεις των περιστατικών και των προβλημάτων ιδιωτικότητας των καταναλωτών που μπορεί να οφείλονται σε υποκείμενα σφάλματα σχεδιασμού, ανάπτυξης ή λειτουργίας της υποδομής που υποστηρίζει το προϊόν και να αποτρέψει προληπτικά την επανάληψη περιστατικών ιδιωτικότητας που σχετίζονται με τα σφάλματα αυτά.

ζ) Ο οργανισμός θα πρέπει να είναι υπεύθυνος να επιτρέπει στους χρήστες του οργανισμού να κάνουν κατάλληλη χρήση των υπηρεσιών, δεδομένων ή άλλων περιουσιακών στοιχείων ΤΠ που επηρεάζουν την ιδιωτικότητα. Η διαχείριση πρόσβασης συμβάλλει στην προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των περιουσιακών στοιχείων, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση ή να τα τροποποιούν. Η διαχείριση πρόσβασης εφαρμόζει πολιτικές διαχείρισης της ασφάλειας πληροφοριών στο πλαίσιο της διαδικασίας υποστήριξης της ιδιωτικότητας και μερικές φορές αναφέρεται ως διαχείριση δικαιωμάτων ή διαχείριση ταυτότητας.

7.8 Προετοιμασία και διαχείριση μιας παραβίασης ιδιωτικότητας

7.8.1 Απαίτηση

Ο οργανισμός θα πρέπει να σχεδιάζει, εφαρμόζει και λειτουργεί, σε συνεργασία με τα σχετικά τρίτα μέρη, αντίμετρα που προλαμβάνουν, εντοπίζουν και αποκαθιστούν περιστατικά, επαναφέρουν τις κανονικές λειτουργίες που προκύπτουν από λειτουργικές διαταραχές και παραβιάσεις της ιδιωτικότητας και επιτρέπουν την επικοινωνία με τους ενδιαφερόμενους φορείς.

7.8.2 Επεξήγηση

Είναι πιθανό ότι ένας οργανισμός δεν θα είναι ποτέ πλήρως προστατευμένος από μια παραβίαση ιδιωτικότητας, αλλά η λειτουργική διαταραχή και ο αντίκτυπος στους καταναλωτές δεν είναι. Η διαχείριση της παραβίασης της ιδιωτικότητας αποτελεί μέρος των ρυθμίσεων ανθεκτικότητας του οργανισμού και εξασφαλίζει μια απρόσκοπτη προσέγγιση για την πρόληψη, τον εντοπισμό, την ανάκτηση από την παραβίαση ιδιωτικότητας, την επανέναρξη των εργασιών μετά την παραβίαση και την επικοινωνία σχετικά με την παραβίαση της ιδιωτικότητας.

7.8.3 Οδηγία

α) Η εξάσκηση των διαδικασιών παραβίασης της ιδιωτικότητας, η ταξινόμηση των περιστατικών, η κλιμάκωση στην ανώτερη διοίκηση και η δοκιμή των σχεδίων επικοινωνίας με τους καταναλωτές είναι κεντρικής σημασίας για τις ρυθμίσεις ανθεκτικότητας ενός οργανισμού. Αναφερθείτε στο 5.6.1 Απαίτηση σε αυτή τη δραστηριότητα.

Περαιτέρω καθοδήγηση μπορεί να βρεθεί στα ακόλουθα έγγραφα:

ΣΗΜΕΙΩΣΗ: Αναφερθείτε στο ISO/IEC 27035-1 και ISO/IEC 27035-2, ISO/IEC 29180:2012 [55] και ISO 22316 [46] .

β) Εντοπισμός και ενσωμάτωση των κινδύνων για τα ΔΠΧ κατά τον σχεδιασμό του σχεδιασμού ανθεκτικότητας της κυβερνοασφάλειας.

7.9 Λειτουργία αντιμέτρων ιδιωτικότητας για τις διαδικασίες και τα προϊόντα από τα οποία εξαρτάται το συγκεκριμένο προϊόν καθ' όλη τη διάρκεια του κύκλου ζωής των ΔΠΧ

7.9.1 Απαίτηση

Ο οργανισμός θα πρέπει να σχεδιάζει και λειτουργεί, σε συνεργασία με τα σχετικά τρίτα μέρη, αντίμετρα ιδιωτικότητας στις υπηρεσίες που υποστηρίζουν το προϊόν, με τρόπο που να πληροί με συνέπεια τις απαιτήσεις ιδιωτικότητας.

ΣΗΜΕΙΩΣΗ Οι συγκεκριμένες διαδικασίες που χρησιμοποιούνται για την υποστήριξη ενός προϊόντος θα διαφέρουν ανάλογα με τις ανάγκες και το τμήμα της αγοράς του συγκεκριμένου προϊόντος (καθώς και άλλους παράγοντες).

7.9.2 Επεξήγηση

Ο οργανισμός συνήθως σχεδιάζει και εφαρμόζει αντίμετρα ιδιωτικότητας στο πλαίσιο υποστηρικτικών διαδικασιών, όπως οι πωλήσεις, η διανομή και το μάρκετινγκ, η υποστήριξη και οι λειτουργίες απόσυρσης προϊόντων. Ένα καταναλωτικό προϊόν μπορεί να σχεδιαστεί με τέτοιο τρόπο ώστε κατά τη μετάβαση των δεδομένων, να μην υπάρχει ανάγκη να υπάρχει ενδιάμεση αποθήκευση με το σημείο πώλησης, εκτός εάν η συσκευή έχει χαλάσει. Οι απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό, μπορεί επίσης να εξετάσει την αποφυγή της ανάγκης συλλογής δεδομένων μέσω της εγγραφής σε μια υπηρεσία, λειτουργώντας ανεξάρτητα ή αλληλεπιδρώντας με μια υπηρεσία με ανώνυμο τρόπο.

Καθ' όλη τη διάρκεια του κύκλου ζωής του προϊόντος, το προϊόν θα επεξεργάζεται ΔΠΧ με μυριάδες τρόπους για διαδικασίες που είναι απαραίτητες για την πώληση, την εμπορία, τη διανομή, την υποστήριξη και την απόσυρση του προϊόντος. Κάποιες από αυτές θα είναι προϋπάρχουσες και κάποιες άλλες θα σχεδιαστούν και θα εφαρμοστούν με βάση την προσέγγιση των απαιτήσεων ιδιωτικότητας ήδη από τον σχεδιασμό. Ο σημαντικός παράγοντας είναι ότι καμία διαδικασία που σχετίζεται με ΔΠΧ δεν παρέχει λιγότερη προστασία της ιδιωτικότητας σε όσους αλληλεπιδρούν με το προϊόν ή σε όσους τα ΔΠΧ οποίων επεξεργάζεται το προϊόν από ό,τι η διαδικασία που έχει σχεδιαστεί και υλοποιηθεί στο ίδιο το προϊόν.

7.9.3 Οδηγία

α) Οι απαιτήσεις ιδιωτικότητας για προϊόντα από τα οποία εξαρτάται το υπό εξέταση προϊόν θα πρέπει να επανεξετάζονται ως προς τη συνέπειά τους, διότι η υπόσχεση της απαίτησης ιδιωτικότητας ήδη από τον σχεδιασμό είναι τόσο ισχυρή όσο και η αντιμετώπιση των κινδύνων παραβίασης της ιδιωτικότητας σε όλο το οικοσύστημα του προϊόντος.

β) Τα υλικά μάρκετινγκ και πωλήσεων πρέπει να αντικατοπτρίζουν την πραγματική λειτουργικότητα του προϊόντος.

γ) Το προσωπικό της διανομής και των σημείων πώλησης θα πρέπει να έχει εκπαιδευτεί και να είναι σε θέση να ενημερώνει τον καταναλωτή για τους κινδύνους παραβίασης της

ιδιωτικότητας που συνδέονται με το καταναλωτικό προϊόν και να τους μετριάζει (π.χ. κατά την υποστήριξη του προϊόντος εγγραφή, εγκατάσταση και ενεργοποίηση).

8 Απαιτήσεις για το τέλος του κύκλου ζωής των ΔΠΧ

8.1 Επισκόπηση

Το τέλος του κύκλου ζωής ενός καταναλωτικού προϊόντος δεν είναι πάντα το ίδιο με το τέλος του κύκλου ζωής των ΔΠΧ. Στο τέλος του κύκλου ζωής του προϊόντος μπορούν να συμβούν διάφορα γεγονότα: για παράδειγμα, ο οργανισμός μπορεί να αποσύρει το προϊόν από την αγορά ή να διακόψει σταδιακά την υποστήριξη πριν από το τέλος της προβλεπόμενης χρήσης από τον καταναλωτή. Οι καταναλωτές έχουν επίσης βασικό ρόλο στον επηρεασμό του τέλους του κύκλου ζωής ενός προϊόντος και των συναφών υπολειπόμενων κινδύνων παραβίασης της ιδιωτικότητας, όταν ο καταναλωτής μπορεί επίσης να διαθέσει, να μεταβιβάσει, να πωλήσει ή να συνεχίσει να χρησιμοποιεί το προϊόν μετά τον τερματισμό της υποστήριξης από τον οργανισμό. Το τέλος της χρήσης από τον καταναλωτή, αλλά όχι το τέλος του κύκλου ζωής των ΔΠΧ, μπορεί επίσης να προκύψει από το θάνατο ή την ανικανότητα του καταναλωτή. Η ευθύνη του οργανισμού για τα ΔΠΧ μπορεί να συνεχιστεί ακόμη και μετά τη λήξη της υποστήριξης του προϊόντος από τον προμηθευτή. Συνεπώς, το τέλος του κύκλου ζωής των ΔΠΧ είναι εξίσου σημαντικό να λαμβάνεται υπόψη στο σχεδιασμό του προϊόντος. Η προσεκτική εξέταση και ο προγραμματισμός κατά το στάδιο του σχεδιασμού για την ενδεχόμενη διαγραφή των ΔΠΧ που σχετίζονται με το προϊόν αντικατοπτρίζει τις απαιτήσεις ιδιωτικότητας ήδη από τον σχεδιασμό.

Οι καταναλωτές διαδραματίζουν καθοριστικό ρόλο στον επηρεασμό του τέλους του κύκλου ζωής ενός προϊόντος και των σχετικών υπολειπόμενων κινδύνων παραβίασης της ιδιωτικότητας. Όταν οι καταναλωτές έχουν διακριτική ευχέρεια σε αυτό το στάδιο, είναι σημαντικό να ενημερώνονται για τις ευθύνες τους όσον αφορά τη διαχείριση των δικών τους κινδύνων και των κινδύνων παραβίασης της ιδιωτικότητας των άλλων όταν συνεχίζουν να χρησιμοποιούν το προϊόν. Η ευθύνη για τα ΔΠΧ μπορεί να συνεχιστεί ακόμη και μετά τη λήξη της υποστήριξης του προϊόντος από τον προμηθευτή.

8.2 Σχεδιασμός αντιμέτρων ιδιωτικότητας για την απόσυρση και το τέλος χρήσης

8.2.1 Απαίτηση

Με τα σχετικά τρίτα μέρη, ο οργανισμός θα πρέπει να σχεδιάζει και να εφαρμόζει αντίμετρα ιδιωτικότητας για τη διαχείριση των κινδύνων που διατρέχουν τα ΔΠΧ κατά την διάρκεια και μετά την απόσυρση του προϊόντος και κατά το τέλος της χρήσης του καταναλωτικού προϊόντος.

8.2.2 Επεξήγηση

Η λογοδοσία του οργανισμού για τα ΔΠΧ εκτείνεται μέχρι το τέλος του κύκλου ζωής των ΔΠΧ (το σημείο στο οποίο τα ΔΠΧ των καταναλωτών δεν υφίστανται πλέον επεξεργασία). Αυτό το σημείο μπορεί να συμβεί πολύ μετά το τέλος του κύκλου ζωής του προϊόντος, οπότε η λογοδοσία θα πρέπει να σχεδιαστεί για μακροπρόθεσμη ανθεκτικότητα.

Η απόσυρση ενός προϊόντος δεν αποτελεί απαραίτητα το τέλος του κύκλου ζωής των σχετικών ΔΠΧ. Είναι πιθανόν τα ΔΠΧ των καταναλωτών να χρειαστεί να υποβληθούν σε επεξεργασία για μερικά χρόνια μετά την απόσυρση του προϊόντος και, ως εκ τούτου, ο οργανισμός μπορεί να εξετάσει τους κινδύνους παραβίασης της ιδιωτικότητας αυτής της περιόδου κατά τη διάρκεια της ανάπτυξης, όπως και κάθε άλλο μέρος του κύκλου ζωής του προϊόντος. Συνεπώς, τα αντίμετρα της ιδιωτικότητας επιβιώνουν κατά την επίσημη ζωή του προϊόντος και μπορούν να λαμβάνουν υπόψη τις διάφορες περιπτώσεις χρήσης μετά την απόσυρση που εξετάστηκαν κατά την ανάπτυξη. Εάν οι κίνδυνοι παραβίασης της ιδιωτικότητας αυτής της περιόδου δεν αντιμετωπιστούν κατάλληλα, οι κίνδυνοι για τα ΔΠΧ του καταναλωτή μπορούν να παραταθούν επ' αόριστον.

Για παράδειγμα, ο καθορισμός οργανωτικών περιόδων διατήρησης για τα ΔΠΧ προστατεύει την ιδιωτικότητα. Αυτό μπορεί να συμβάλει στη διαχείριση του κινδύνου και του κόστους του κύκλου ζωής και να βοηθήσει στην αποφυγή ρυθμιστικών μέτρων ή κακής δημοσιότητας εάν ο χειρισμός των ΔΠΧ μετά τη χρήση προκαλέσει περιστατικά. Όταν τα ΔΠΧ διατηρούνται επ' αόριστον, το ρίσκο της διαχείρισής τους μπορεί να αυξηθεί. Γενικά, οι οργανισμοί προσδιορίζουν πόσο καιρό τα ΔΠΧ που διατηρούνται από τον οργανισμό ή το προϊόν παραμένουν απαραίτητα για τη λειτουργία του προϊόντος και τα διαγράφουν με ασφάλεια όταν δεν είναι πλέον απαραίτητα.

8.2.3 Οδηγία

α) Κατά το σχεδιασμό του προϊόντος θα πρέπει να λαμβάνεται υπόψη το τέλος της ζωής του, συμπεριλαμβανομένων των περιπτώσεων που οι καταναλωτές μεταβιβάζουν το προϊόν σε άλλους καταναλωτές μέσω δώρων ή μεταχειρισμένων αγορών, εάν ένας καταναλωτής πεθάνει, απόσυρση του προϊόντος από την πώληση, απόσυρση της υποστήριξης του προϊόντος.

β) Τα αντίμετρα ιδιωτικότητας θα πρέπει να λειτουργούν όσο διαρκεί η επεξεργασία των ΔΠΧ των καταναλωτών που σχετίζονται με το προϊόν.

γ) Σε περίπτωση που διαπιστωθούν αλλαγές στους κινδύνους παραβίασης της ιδιωτικότητας, οι αλλαγές στα αντίμετρα ιδιωτικότητας θα πρέπει να σχεδιάζονται και να δοκιμάζονται και να τίθενται σε λειτουργία με τον ίδιο τρόπο όπως κατά την ανάπτυξη του προϊόντος.

δ) Όπου απαιτείται ή είναι σκόπιμο και εφικτό, το προϊόν θα πρέπει να διαθέτει δυνατότητες που επιτρέπουν στον καταναλωτή να διαγράφει με ασφάλεια τα ΔΠΧ που είναι αποθηκευμένα στο προϊόν.

ε) Η συλλογή και η διατήρηση των ΔΠΧ θα πρέπει να γίνεται σύμφωνα με τις προσδιορισμένες ανάγκες του οργανισμού και να σχεδιάζεται για εφαρμογή σε επίπεδο τεχνικών και οργανωτικών διαδικασιών (προϋποτίθεται ότι ο οργανισμός τηρεί συγκεκριμένες νομικές υποχρεώσεις συλλογής και διατήρησης).

ζ) Η διατήρηση και η επεξεργασία των ΔΠΧ πέραν του τέλους της υποστήριξης του προϊόντος και της χρήσης του προϊόντος από τον καταναλωτή θα πρέπει να γίνεται μόνο για την εκπλήρωση έγκυρων οργανωτικών σκοπών, όπως έχει συμφωνηθεί από τον καταναλωτή, ή για την εκπλήρωση νομικών υποχρεώσεων.

η) Εάν τα ΔΠΧ που διατηρεί ο οργανισμός δεν χρειάζονται πλέον και έχουν φτάσει στο τέλος του κύκλου ζωής τους, ο βαθμός καταστροφής των δεδομένων θα πρέπει να καθορίζεται από την ευαισθησία των δεδομένων.

ΣΗΜΕΙΩΣΗ Ο NIST [56] περιλαμβάνει συστάσεις για την εξυγίανση των συσκευών αποθήκευσης και την καταστροφή των δεδομένων, οι οποίες κυμαίνονται από την εκκαθάριση των δεδομένων με αντικατάστασή τους έως την καταστροφή του φυσικού μέσου.

θ) Ο καταναλωτής θα πρέπει να ενημερώνεται για τους όρους διατήρησης και επεξεργασίας των δεδομένων του προϊόντος μετά το τέλος της υποστήριξης του προϊόντος.

ι) Τα ΔΠΧ θα πρέπει να καταστρέφονται με ασφάλεια ή να ανωνυμοποιούνται όταν τα ΔΠΧ δεν απαιτούνται πλέον για την ικανοποίηση συγκεκριμένων νόμιμων απαιτήσεων του οργανισμού ή νομικών απαιτήσεων [50] [19].

κ) Οι αλλαγές στα προτεινόμενα αντίμετρα ιδιωτικότητας θα πρέπει να αποτελούν μέρος της διαδικασίας έγκρισης πριν από την απόσυρση οποιουδήποτε προϊόντος.

λ) Η χρήση καταναλωτικών προϊόντων μετά το τέλος της υποστήριξης του προϊόντος θα πρέπει να λαμβάνεται υπόψη με συνεχή παρακολούθηση της αγοράς και να αντιμετωπίζονται με διορθωτικά μέτρα τυχόν εντοπισμένες απειλές ή τρωτά σημεία που θα μπορούσαν να προκαλέσουν σημαντικό κίνδυνο για την παραβίασης της ιδιωτικότητας των καταναλωτών.

μ) Οι περιπτώσεις χρήσης στο τέλος του κύκλου ζωής του καταναλωτή θα πρέπει να περιλαμβάνουν: τον καταναλωτή που παύει να χρησιμοποιεί το προϊόν (θάνατος του καταναλωτή, απόρριψη ή ανακύκλωση του προϊόντος) ή επαναχρησιμοποίηση, όπως η μεταβίβαση του προϊόντος μέσω δώρων ή αγορών μεταχειρισμένων προϊόντων,

ν) Όταν οι καταναλωτές έχουν διακριτική ευχέρεια όσον αφορά τις χρήσεις μετά την απόσυρση, θα πρέπει να ενημερώνονται για τις ευθύνες τους όσον αφορά τη διαχείριση των κινδύνων για την παραβίαση της ιδιωτικότητας των ίδιων και των άλλων σε κάθε χρήση μετά την απόσυρση.

ξ) Η πολυλειτουργική ομάδα θα πρέπει να ενημερώνει τους καταναλωτές, τις πωλήσεις και την υποστήριξη στο τέλος της διάρκειας ζωής του προϊόντος σχετικά με τις ενέργειες στις οποίες μπορούν να προβούν για την προστασία της ιδιωτικότητας των ΔΠΧ ως αποτέλεσμα του τέλους των πωλήσεων, της υποστήριξης ή άλλης οργανωτικής επεξεργασίας των ΔΠΧ.

ο) Η απόσυρση του προϊόντος μπορεί να πραγματοποιηθεί μερικά χρόνια μετά την κυκλοφορία, οπότε οι συνθήκες έχουν αλλάξει από την αρχική αξιολόγηση του κινδύνου

παραβίασης της ιδιωτικότητας. Πριν από την απόσυρση του προϊόντος, η αξιολόγηση κινδύνου παραβίασης της ιδιωτικότητας του προϊόντος θα πρέπει να επανεξετάζεται και να επικαιροποιείται, όπου χρειάζεται.

2. Πρότυπο διαδικασίας σχεδιασμού (Design Process Standard - IOPD) [57]

Εισαγωγή

Η ανάγκη για αυτό το πρότυπο είναι αποτέλεσμα διαφόρων παραγόντων. Αν και έχει καθοριστικό ρόλο στην κοινωνικοποίηση της έννοιας των απαιτήσεων της ιδιωτικότητας ήδη από τον σχεδιασμό, οι 7 θεμελιώδεις αρχές (Foundational Principles) που αναπτύχθηκαν από τον Επίτροπο Πληροφοριών και Προστασίας της Ιδιωτικής Ζωής του Οντάριο το 2009 (Information and Privacy Commissioner of Ontario in 2009) στερούνται ουσιαστικών και εφαρμόσιμων εργασιών/βημάτων, αφήνοντας τους επαγγελματίες αβέβαιους για το πώς να ενσωματώσουν τις αρχές στις διαδικασίες σχεδιασμού τους. Επιπλέον, ενώ τα τελευταία χρόνια έχουν εκδοθεί διάφορα πρότυπα σχετικά με την ιδιωτικότητα, η έλλειψη πιστοποιημένων προτύπων έχει δυσχεράνει τις πωλήσεις μεταξύ επιχειρήσεων, όπου οι πωλητές θέλουν να αποδείξουν στους πελάτες ότι έχουν ενσωματώσει τις απαιτήσεις ιδιωτικότητας ήδη από το σχεδιασμό των προϊόντων και των υπηρεσιών τους και οι αγοραστές θέλουν να διασφαλίσουν το ίδιο. Από το άρθρο 25 του Γενικού Κανονισμού για την Προστασία Δεδομένων ΓΚΠΔ (General Data Protection Regulation GDPR) απουσιάζει αισθητά η εντολή προς τους εκτελούντες την επεξεργασία ή τους πωλητές προϊόντων να τις απαιτήσεις ιδιωτικότητας ήδη από το σχεδιασμό. Το βάρος πέφτει στους υπευθύνους επεξεργασίας, σύμφωνα με την ορολογία του ΓΚΠΔ, να διασφαλίσουν ότι η προστασία των δεδομένων έχει σχεδιαστεί. Ωστόσο, ο εκτελών την επεξεργασία της διαδικασίας ή του προϊόντος είναι συχνά αυτός που έλαβε τις αποφάσεις σχεδιασμού και ο υπεύθυνος επεξεργασίας είναι απλώς ένας παθητικός καταναλωτής του προϊόντος ή της υπηρεσίας. Τέλος, το πρότυπο αυτό προέκυψε από την επιθυμία να μειωθούν οι συχνοί ισχυρισμοί των εταιρειών ότι εφαρμόζουν τις "απαιτήσεις ιδιωτικότητας ήδη από το σχεδιασμό" χωρίς ουσιαστική υποστήριξη του ισχυρισμού και συχνά χωρίς καμία επισημότητα σχετικά με το τι σημαίνουν οι απαιτήσεις ιδιωτικότητας ήδη από το σχεδιασμό για τη διαδικασία σχεδιασμού. Παρόλο που το πρότυπο αυτό δεν θα εμποδίσει άλλους να ισχυρίζονται ότι σχεδιάζουν με γνώμονα την προστασία της ιδιωτικότητας, δημιουργεί τουλάχιστον αμφιβολίες στους αγοραστές ως προς την εγκυρότητα αυτών των ισχυρισμών όταν δεν υποστηρίζονται από μια αναγνωρισμένη πιστοποίηση.

Το πρότυπο αυτό περιγράφει λεπτομερώς τα στοιχεία που είναι απαραίτητα σε μια διαδικασία σχεδιασμού για την ενσωμάτωση σκέψεων της ιδιωτικότητας και τη μείωση των κινδύνων παραβίασης της ιδιωτικότητας των ατόμων. Η διαδικασία μπορεί να αφορά το σχεδιασμό προϊόντων, υπηρεσιών ή επιχειρηματικών διαδικασιών και καλύπτει τον κύκλο ζωής από την ιδέα μέχρι την ανάπτυξη. Αν και οι περισσότεροι θα θεωρούσαν ότι η διαδικασία σχεδιασμού

είναι κατά τη διάρκεια της ιδέας και ενδεχομένως της ανάπτυξης ενός προϊόντος, μιας υπηρεσίας ή μιας επιχειρηματικής διαδικασίας, η ανάπτυξη είναι μια απαραίτητη φάση που πρέπει να εξεταστεί, διότι μετά την ανάπτυξή τους, σχεδόν πάντα περνούν από επαναλήψεις και επανασχεδιασμό. Επιπλέον, η ανάπτυξη μπορεί να αποκαλύψει ανακριβείς παραδοχές σχετικά με το πλαίσιο και τον κίνδυνο, οι οποίες απαιτούν επανεκτίμηση, επανασχεδιασμό και εκ νέου ανάπτυξη.

Ως τελική σημείωση, το παρόν πρότυπο καλύπτει την ιδιωτικότητα και δεν περιορίζεται στην "προστασία των δεδομένων" ή σε οποιαδήποτε συγκεκριμένη προσέγγιση δικαιοδοσίας. Η ιδιωτικότητα είναι μια ευρύτερη έννοια από την προστασία των δεδομένων και καλύπτει όλες τις αλληλεπιδράσεις μεταξύ ατόμων και άλλων στην κοινωνία και τους κοινωνικούς κανόνες που διέπουν αυτές τις αλληλεπιδράσεις. Το παρόν πρότυπο είναι σκόπιμα διφορούμενο ως προς αυτό. Όσοι επιθυμούν να επικεντρωθούν στην προστασία των δεδομένων ή σε οποιοδήποτε υποσύνολο των ανθρωπίνων δικαιωμάτων και της ελευθερίας μπορούν να επιλέξουν ένα μοντέλο κινδύνου (Risk Model) (βλ. Στοιχείο Ι.Β.), το οποίο εξετάζει τις βλάβες στην προστασία των δεδομένων ή σε άλλα δικαιώματα ως πιθανές ανησυχίες. Το πρότυπο αυτό υιοθετεί μια προσέγγιση της ιδιωτικότητας με βάση τον κίνδυνο (risk-based), σε αντίθεση με μια απολυταρχική προσέγγιση. Σε κάθε ανθρώπινη δραστηριότητα υπάρχουν πιθανότητες, συμπεριλαμβανομένης της πιθανότητας παραβίασης των προσδοκιών και των κανόνων της ιδιωτικότητας. Οι στόχοι είναι η αντιστάθμιση αυτών των κινδύνων έναντι των οφελών για τα άτομα και την κοινωνία (βλ. στοιχείο ΙΙ.Γ.) και η ελαχιστοποίηση αυτών των κινδύνων για τα άτομα και την κοινωνία (βλ. στοιχείο ΙΙ.Δ.2.).

Δομικοί ορισμοί

Στοιχείο (Component): Ένα συστατικό στοιχείο του παρόντος προτύπου. (Σημείωση: Τα στοιχεία είναι υψηλού επιπέδου περιγραφές αυτού του προτύπου και όχι στοιχεία ενός συστήματος).

Φάσεις (Phases): Τα στάδια του κύκλου ζωής του συστήματος που εφαρμόζονται σε αυτό το στοιχείο: ιδέα, ανάπτυξη και εγκατάσταση. Το “προαπαιτούμενο” αναφέρεται σε στοιχείο που βρίσκεται εκτός του κύκλου ζωής του συστήματος.

Στόχος (Objective): Στόχος ή επιθυμητό αποτέλεσμα του στοιχείου. Ο στόχος περιγράφει γιατί το στοιχείο είναι σημαντικό και τι πρόκειται να επιτύχει.

Περιγραφή (Description): Η λεπτομερής επεξήγηση του στοιχείου.

Οδηγίες εφαρμογής (Implementing Guidance): Περιγραφή των βημάτων, κοινές παγίδες ή διευκρινιστικές πληροφορίες σχετικά με τον τρόπο με τον οποίο ο οργανισμός εκτελεί στην πραγματικότητα το στοιχείο.

Πειστήρια (Evidence): Πληροφορίες που πρέπει να παρουσιάσει ο οργανισμός για να αποδείξει ότι διαθέτει το στοιχείο.

Αξιολόγηση (Evaluation): Πώς τα πειστήρια μετρώνται και κρίνονται για να διαπιστωθεί εάν είναι επαρκή για την επίτευξη του στόχου και αποτελεσματικά για την επίτευξη του στόχου.

Ουσιαστικοί Ορισμοί

Προσέγγιση (Approach): Μια μέθοδος, διεργασία ή διαδικασία για την επίτευξη ενός στόχου.

Αξιολογητής (Assessor): Μια οντότητα που συγκεντρώνει στοιχεία και αξιολογεί κατά πόσον τα στοιχεία αυτά δείχνουν ότι ο οργανισμός ανταποκρίνεται αποτελεσματικά στον στόχο.

Πλαίσιο (Context): Τα συγκεκριμένα στοιχεία που συμβάλλουν ή ανατρέπουν τα στοιχεία που βλάπτουν την ιδιωτικότητα από ένα σύστημα-στόχο, ευθυγραμμισμένα με τους παράγοντες κινδύνου που συνθέτουν το μοντέλο κινδύνου του οργανισμού. Για παράδειγμα, άτομα υψηλού κινδύνου (αφηρημένος παράγοντας) ⇒ εργαζόμενοι (εξειδικευμένο στοιχείο).

Κύκλος ζωής (Lifecycle): Παρόλο που η επιχειρηματική δραστηριότητα γύρω από ένα σύστημα μπορεί να “σπάσει” σε πολλές φάσεις κύκλου ζωής, αυτό το πρότυπο χρησιμοποιεί τρεις φάσεις υψηλού επιπέδου: αρχική ιδέα (ideation), ανάπτυξη (development) και εγκατάσταση (deployment). Τα σημεία οριοθέτησης μεταξύ κάθε φάσης μπορεί να μην είναι απαραίτητα καθαρά.

- **Αρχική Ιδέα** Η φάση κατά την οποία ο οργανισμός διερευνά και σχεδιάζει το περίγραμμα του επιθυμητού συστήματος. Η αρχική ιδέα απαντά γενικά στο ερώτημα "Τι σχεδιάζεται;". (π.χ. "μια υπηρεσία που παρέχει Χ").
- **Ανάπτυξη** Η φάση κατά την οποία ο οργανισμός προσπαθεί να σχεδιάσει και να κατασκευάσει το σύστημα. Η ανάπτυξη απαντά γενικά στο ερώτημα πώς ο οργανισμός σχεδιάζει να παρέχει το προϊόν, την υπηρεσία ή την επιχειρηματική διαδικασία (π.χ. "χρησιμοποιώντας μια εφαρμογή για κινητά που έχει πρόσβαση σε APIs σε έναν διακομιστή που εκτελείται σε ένα cloud").
- **Εγκατάσταση** Η φάση κατά την οποία ο οργανισμός καθιστά διαθέσιμο το σύστημα προς χρήση. Η φάση αυτή περιλαμβάνει επίσης τη συνεχή χρήση και λειτουργία του προϊόντος, της υπηρεσίας ή της επιχειρηματικής διαδικασίας.

Στοιχείο που βλάπτει την ιδιωτικότητα (Privacy Harm): Μια αρνητική συνέπεια που εμπίπτει στην ομπρέλα της ιδιωτικότητας.

Θέμα ιδιωτικότητας (Privacy Issue): Η ύπαρξη απειλής, ευπάθειας ή βλάβης που δημιουργεί κίνδυνο.

Σύστημα (System): Το προϊόν, η υπηρεσία ή η επιχειρηματική διαδικασία ή ένα στοιχείο ενός προϊόντος, μιας υπηρεσίας ή μιας επιχειρηματικής διαδικασίας.

Υπολειπόμενος κίνδυνος (Residual Risk): Ένα μέτρο του κινδύνου που παραμένει μετά από μια αλλαγή στο πλαίσιο, όπως η εφαρμογή αντιμέτρων.

Κίνδυνος (Risk): Ένα μέτρο της πιθανότητας και της σοβαρότητας ενός στοιχείου που βλάπτει την ιδιωτικότητα με τη χρήση των παραγόντων κινδύνου (Risk Factors) σύμφωνα με ένα συγκεκριμένο μοντέλο κινδύνου.

Μοντέλο κινδύνου (Risk Model): Μια αναπαράσταση που αναλύει βασικούς όρους και αφηρημένους παράγοντες που συμβάλλουν ή αναιρούν στοιχεία που βλάπτουν την ιδιωτικότητα (βλ. ορισμό NIST).

Παράγοντας κινδύνου (Risk Factor): Ένα στοιχείο που επιδρά, επηρεάζει ή καθορίζει την πιθανότητα ή τη σοβαρότητα του στοιχείου που βλάπτει την ιδιωτικότητα. Παραδείγματα περιλαμβάνουν τον αριθμό ή τους τύπους των ατόμων που διατρέχουν κίνδυνο, τους ρόλους τους στο σύστημα-στόχο ή τα δεδομένα που τα αφορούν.

Ανάληψη Κινδύνου (Risk Appetite): Πόσο κίνδυνο παραβίασης της ιδιωτικότητας είναι διατεθειμένος ο οργανισμός να επιτρέψει στις επηρεαζόμενες οντότητες να υποστούν μέσω των συστημάτων του.

Ανοχή κινδύνου (Risk Tolerance): Πόση απόκλιση από τη δηλωμένη διάθεση ανάληψης κινδύνου είναι διατεθειμένος να ανεχθεί ο οργανισμός.

Σύστημα-στόχος (Target System): Το σύστημα που σχεδιάζεται, αναπτύσσεται ή εγκαθίσταται στο πλαίσιο της διαδικασίας. Το σύστημα-στόχος διακρίνεται από ένα γενικό σύστημα

Το ακόλουθο διάγραμμα απεικονίζει τη βασική οργανωτική δομή του παρόντος προτύπου. Τα Προαπαιτούμενα δεν συνδέονται με μια συγκεκριμένη φάση του κύκλου ζωής. Οι Φάσεις εξηγούνται στην αρχή της ενότητας Συνιστώσες της Διαδικασίας Σχεδιασμού (Design Process Components).

I. ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ	
Α. ΔΙΑΚΥΒΕΡΝΗΣΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ (PRIVACY GOVERNANCE)	Β. ΜΟΝΤΕΛΟ ΚΙΝΔΥΝΟΥ (RISK MODEL)
Πειστήρια και αξιολόγηση	Πειστήρια και αξιολόγηση

Τα προαπαιτούμενα είναι οργανωτικά Στοιχεία που δεν σχετίζονται ειδικά με τη διαδικασία σχεδιασμού. Κάθε προαπαιτούμενο έχει τις δικές του απαιτήσεις Τεκμηρίων και αξιολόγησης.

	Γενικά Πειστήρια και Αξιολόγηση ισχύουν για όλα τα Στοιχεία της Διαδικασίας Σχεδιασμού					
Α. ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΚΑΙ ΚΑΤΑΓΡΑΦΗ ΣΤΟΧΟΥ	Β. ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΚΑΙ ΚΑΤΑΓΡΑΦΗ ΑΠΑΙΤΗΣΕΩΝ	Γ. ΕΚΤΕΛΕΣΗ ΑΝΑΛΥΣΗΣ ΣΥΜΒΙΒΑΣΜΟΥ (TRADE-OFF ANALYSIS)	Δ. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΠΑΡΑΒΙΑΣΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ		Ε. ΕΠΑΛΗΘΕΥΣΗ ΠΛΑΙΣΙΟΥ ΚΑΙ ΑΠΑΙΤΗΣΕΩΝ	Ζ. ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΠΛΑΙΣΙΟΥ
Πειστήρια και αξιολόγηση	Πειστήρια και αξιολόγηση	Πειστήρια και αξιολόγηση	1. ΕΚΤΕΛΕΣΗ ΑΞΙΟΛΟΓΗΣΗΣ ΚΙΝΔΥΝΟΥ		Πειστήρια και αξιολόγηση	Πειστήρια και αξιολόγηση
			α. Πλαισίωση των παραγόντων κινδύνου	Π & Α		
			β. Συγκέντρωση θεμάτων ιδιωτικότητας	Π & Α		
			γ. Εκτίμηση κινδύνων	Π & Α		
			2. ΑΝΤΑΠΟΚΡΙΣΗ ΣΤΟΥΣ ΚΙΝΔΥΝΟΥΣ			
			Πειστήρια και αξιολόγηση			

Όλα τα Στοιχεία της Διαδικασίας Σχεδιασμού ευθυγραμμίζονται με ένα ή περισσότερα από τα στάδια του κύκλου ζωής του προϊόντος, της υπηρεσίας ή της επιχειρηματικής διαδικασίας. Τα στάδια παρουσιάζονται σε πολύ υψηλό επίπεδο για να αποφευχθεί η σύγκρουση με οργανισμούς που μπορεί να έχουν πιο λεπτομερή στάδια.

Όλα τα Στοιχεία της Διαδικασίας Σχεδιασμού έχουν απαιτήσεις Πειστηρίων και Αξιολόγησης πέραν των γενικών απαιτήσεων Πειστηρίων και Αξιολόγησης για ολόκληρη τη διαδικασία σχεδιασμού. Το στοιχείο ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΠΑΡΑΒΙΑΣΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ χωρίζεται σε δύο υποστοιχεία, το πρώτο από τα οποία υποδιαιρείται περαιτέρω. Καθένα από τα επιμέρους στοιχεία έχει απαιτήσεις Πειστηρίων και Αξιολόγησης.

Ι. Προαπαιτούμενα

Στοιχείο: Ι.Α. Διακυβέρνηση Ιδιωτικότητας
Φάση: Προαπαιτούμενο
Στόχος: Να υπάρχει η διακυβέρνηση για την επιτυχή ενσωμάτωση της ιδιωτικότητας στο σχεδιασμό των συστημάτων.
Περιγραφή: Ο οργανισμός πρέπει να διαθέτει μια λειτουργία διακυβέρνησης για τη διαχείριση της ιδιωτικότητας κατά την αρχική ιδέα, την ανάπτυξη και την εγκατάσταση συστημάτων. Αυτή η λειτουργία διακυβέρνησης πρέπει να περιλαμβάνει: • Πολιτικές, πρότυπα και διαδικασίες • Ανθρώπινους πόρους με κατάλληλους ρόλους και αρμοδιότητες • Εκπαίδευση των πόρων αυτών ανάλογα με το ρόλο και τις αρμοδιότητές τους • Ιδιοκτησία ή λογοδοσία για καθένα από τα σημεία της διαδικασίας σχεδιασμού • Ένα σύνολο αξιών ιδιωτικότητας σύμφωνα με τις αποστολές και τους στόχους του οργανισμού • Ένα πλαίσιο ελέγχου που προσδιορίζει την πηγή των ελέγχων, τις κανονιστικές οδηγίες και τις πολιτικές ή τα πρότυπα της εταιρείας που χρησιμοποιούνται για τον μετριασμό των κινδύνων παραβίασης της ιδιωτικότητας. • Ένα ισχυρό σύνολο εργαλείων για κοινά σενάρια για τον μετριασμό των πιθανών κινδύνων παραβίασης της ιδιωτικότητας στο μοντέλο κινδύνου
Οδηγίες εφαρμογής: Ο οργανισμός θα πρέπει να αξιοποιήσει τις βέλτιστες πρακτικές του κλάδου, κοινές διαδικασίες διαχείρισης προγραμμάτων και έργων για την ιδιωτικότητα ή μια αναγνωρισμένη πλαίσιο ιδιωτικότητας για την οργάνωση και τη δημιουργία των πολιτικών και των διαδικασιών της. Ο οργανισμός θα πρέπει να εμπλέξει τα ενδιαφερόμενα μέρη για να διασφαλίσει την επιτυχία.
Πειστήρια • **Τεκμηρίωση (Documentation)**: Οι πολιτικές, τα πρότυπα και οι διαδικασίες συμπεριλαμβανομένου του HR, λογοδοσία και διακυβέρνηση, τους κινδύνους και τα αντίμετρα, καθώς και την εκπαίδευση που σχετίζεται με τη διαδικασία σχεδιασμού του οργανισμού. Η τεκμηρίωση περιλαμβάνει περαιτέρω εγκρίσεις, ανασκοπήσεις, εσωτερικές επικοινωνίες και εκθέσεις ελέγχου (audit reports). • **Ανθρώπινο δυναμικό**: Περιγραφές θέσεων εργασίας και απαιτούμενα προσόντα • **Εκπαίδευση**: Σχεδιασμός προγράμματος και περιεχομένου εκπαίδευσης, αρχείων εκπαίδευσης και κριτικής ή αποτελεσμάτων της εκπαίδευσης. • **Λογοδοσία**: Οργανογράμματα με ρόλους και αρμοδιότητες που σχετίζονται με τη διαδικασία σχεδιασμού

Αξιολόγηση: Ο αξιολογητής θα εξετάσει τα πειστήρια για να διαπιστώσει αν:

- Οι πολιτικές, τα πρότυπα και οι διαδικασίες του οργανισμού έχουν τεκμηριωθεί, εγκριθεί, επανεξεταστεί, κοινοποιηθεί και είναι εύκολα διαθέσιμα στο προσωπικό του οργανισμού.
- Ο οργανισμός ορίζει και διατυπώνει με σαφήνεια τις περιγραφές θέσεων εργασίας και τα απαιτούμενα επαγγελματικά προσόντα για όλο το προσωπικό της διαδικασίας σχεδιασμού.
- Η υποχρεωτική εκπαίδευση του οργανισμού αφορά τις γνώσεις και τις δεξιότητες που απαιτούνται για την εκτέλεση των ρόλων και των αρμοδιοτήτων στη διαδικασία σχεδιασμού και απαιτεί από τα άτομα να ολοκληρώνουν αξιολογήσεις για να αποδεικνύουν την κατανόησής τους σε σχέση με τα καθήκοντά τους.
- Ο οργανισμός διαθέτει σαφώς καθορισμένη δομή αναφοράς, σαφώς προσδιορισμένη εποπτεία από την εκτελεστική διοίκηση και υπεύθυνους επιχειρησιακών διαδικασιών για τις ευθύνες διακυβέρνησης και λογοδοσίας στη διαδικασία σχεδιασμού.
- Ο οργανισμός χρησιμοποιεί τυποποιημένους κινδύνους παραβίασης της ιδιωτικότητας, αντίμετρα και μια βιβλιοθήκη/αποθετήριο απαιτήσεων που περιέχει μια συλλογή από διασφαλίσεις, αντίμετρα, τεχνικές και διαδικασίες που μπορούν να αξιοποιηθούν για τους κινδύνους που προσδιορίζονται στο μοντέλο κινδύνου.

Στοιχείο: Ι.Β. Μοντέλο κινδύνου

Φάση: Προαπαιτούμενο

Στόχος: Να διεξάγονται οι αξιολογήσεις κινδύνου με συνεπή και δομημένο τρόπο. Η ύπαρξη ενός καθορισμένου μοντέλου ή διαδικασίας κινδύνου επιτρέπει στον οργανισμό να αξιολογεί με συνέπεια τη κατάσταση του κινδύνου σε διαφορετικά συστήματα καθώς και στα ίδια συστήματα με την πάροδο του χρόνου.

Περιγραφή: Ο οργανισμός πρέπει να ενσωματώνει (α) ένα ή περισσότερα μοντέλα κινδύνου παραβίασης της ιδιωτικότητας ως βάση για την ανάλυση κινδύνου παραβίασης της ιδιωτικότητας, (β) μια διαδικασία με την οποία αναπτύσσονται μοντέλα κινδύνου παραβίασης της ιδιωτικότητας για συγκεκριμένα συστήματα ως βάση για την ανάλυση κινδύνου παραβίασης της ιδιωτικότητας, ή (γ) έναν συνδυασμό των (α) και (β).

Ένα μοντέλο κινδύνου παραβίασης ιδιωτικότητας ή μια διαδικασία ανάπτυξης μοντέλου πρέπει να αντιμετωπίζει:

i. Απειλές
ii. Ευπάθειες
iii. Ανεπιθύμητες συνέπειες

iv. Πιθανότητα
v. Σοβαρότητα των επιπτώσεων (severity of impact)

Ο οργανισμός πρέπει να έχει ρητά καθορίσει μια επιχειρησιακή διάθεση ανάληψης κινδύνων για την της ιδιωτικότητα και ανοχή κινδύνου ιδιωτικότητας.

ΣΗΜΕΙΩΣΗ: Τα μέτρα της πιθανότητας και της σοβαρότητας των επιπτώσεων θα μπορούσαν να περιλαμβάνουν αιτιολόγηση για τη χρήση σταθερής τιμής. Για παράδειγμα, ένας οργανισμός μπορεί να επιθυμεί να υποθέσει ότι οι απειλές πρόκειται να συμβούν και να αγνοήσει ένα ποιοτικό μέτρο πιθανότητας, εστιάζοντας την προσοχή του στη μέτρηση της σοβαρότητας των επιπτώσεων.

Οδηγίες εφαρμογής: Το μοντέλο κινδύνου του οργανισμού πρέπει τουλάχιστον να εστιάζει στους κινδύνους για τα άτομα που επηρεάζονται από το σύστημα. Το μοντέλο κινδύνου μπορεί επίσης να περιλαμβάνει οργανωτικούς κινδύνους, ομαδικούς κινδύνους και κοινωνικούς κινδύνους.

Το μοντέλο κινδύνου είναι ένα γενικό μοντέλο που εφαρμόζεται σε κάθε ένα από τα συστήματα-στόχους. Η εφαρμογή αυτή γίνεται στο στάδιο του υποσυνόλου "Συγκέντρωση θεμάτων ιδιωτικότητας" της αξιολόγησης κινδύνου. Για παράδειγμα, το μοντέλο κινδύνου μπορεί να θεωρήσει τον κίνδυνο ανεπιθύμητης αλληλογραφίας (spamming) ως έναν από τους κινδύνους που απασχολούν τον οργανισμό. Κατά τη διάρκεια της αξιολόγησης κινδύνου, ο οργανισμός θα προσδιόριζε ότι ένα συγκεκριμένο σύστημα ενέχει τον κίνδυνο ανεπιθύμητης αλληλογραφίας επειδή επιτρέπει στους ανθρώπους να στέλνουν μηνύματα σε άλλους χρήστες του συστήματος.

Πειστήρια

- Τεκμηρίωση του μοντέλου κινδύνου παραβίασης της ιδιωτικότητας ή/και της διαδικασίας ανάπτυξης μοντέλου κινδύνου για συγκεκριμένο σύστημα. Η τεκμηρίωση της διαδικασίας μπορεί να υπάρχει ανεξάρτητα ή να ενσωματώνεται σε σχετικό εργαλείο. Σε κάθε περίπτωση, η τεκμηρίωση θα πρέπει να ορίζει ή/και να περιγράφει τη διαδικασία για τον καθορισμό των σχετικών μοντέλων κινδύνου παραβίασης της ιδιωτικότητας. Θα πρέπει επίσης να περιγράφει τον τρόπο χρήσης των μοντέλων.
- Τεκμηρίωση της οργανωτικής ανοχής και διάθεσης ανάληψης κινδύνων παραβίασης της ιδιωτικότητας σύμφωνα με το μοντέλο κινδύνου και/ή την τεκμηρίωση μιας διαδικασίας για τον εντοπισμό της οργανωτικής ανοχής και διάθεσης ανάληψης κινδύνου παραβίασης της ιδιωτικότητας.

Αξιολόγηση: Ο αξιολογητής θα εξετάσει τα πειστήρια για να διαπιστώσει αν το μοντέλο κινδύνου ή η διαδικασία ανάπτυξης μοντέλου κινδύνου είναι επαρκώς αντικειμενικό ώστε να μπορεί να επαναληφθεί και αν το μοντέλο κινδύνου καλύπτει:

- Απειλές
- Ευπάθειες
- Δυσμενείς συνέπειες για τα άτομα, τουλάχιστον
- Ποσοτικά ή ποιοτικά μέτρα της πιθανότητας ή της συχνότητας των απειλών, των ευπαθειών και των συνεπειών
- Ποσοτικά ή ποιοτικά μέτρα του μεγέθους ή του αντίκτυπου των συνεπειών

Ο αξιολογητής θα εξετάσει την ανοχή και τη διάθεση ανάληψης κινδύνου για να διαπιστώσει αν είναι συνεπής με το μοντέλο κινδύνου ή αν η διαδικασία προσδιορισμού της ανοχής και της διάθεσης ανάληψης οργανωτικού κινδύνου παραβίασης της ιδιωτικότητας θα ανταποκρίνεται επαρκώς στις ποσοτικές ή ποιοτικές μετρήσεις του μοντέλου κινδύνου.

II. Διαδικασία σχεδιασμού

Γενικές Απαιτήσεις Πειστηρίων για Όλα τα Στοιχεία του Κύκλου Ζωής

- Ο οργανισμός πρέπει να διαθέτει τεκμηριωμένη πολιτική, πρότυπο ή διαδικασία που να καλύπτει τα κομμάτια του Στοιχείου. Οι εν λόγω πολιτικές, πρότυπα ή διαδικασίες μπορεί να έχουν διαδικασίες εξαίρεσης (exception processes) που επιτρέπουν την κλιμάκωση αποφάσεων εκτός της κανονικής διαδικασίας.
- Ο οργανισμός πρέπει να διαθέτει πειστήρια για το σύστημα(α)-στόχο που να αποδεικνύουν τη συμμόρφωση με την τεκμηριωμένη πολιτική, το πρότυπο ή τη διαδικασία και που να αφορούν τα στοιχεία της Περιγραφής του στοιχείου.

Γενική Αξιολόγηση για όλα τα Στοιχεία του Κύκλου Ζωής

Ο αξιολογητής θα εξετάσει τα πειστήρια και θα καθορίσει εάν:

- κάθε Στοιχείο της συνιστώσας αντιμετωπίζεται επαρκώς στην τεκμηριωμένη πολιτική, πρότυπο ή διαδικασία.
- η πολιτική, το πρότυπο ή η διαδικασία που αντιμετωπίζει το Στοιχείο είναι επαρκώς τεκμηριωμένα ώστε να μπορεί να επαναληφθεί με παρόμοια αποτελέσματα (δηλ. αντικειμενικότητα).
- οι ελάχιστες απαιτήσεις της πολιτικής, του προτύπου ή της διαδικασίας ανταποκρίνονται στον στόχο του Στοιχείου.

Ο αξιολογητής θα επιλέξει ένα σύστημα-στόχο και θα εξετάσει τα πειστήρια για να διαπιστώσει εάν:

- ο οργανισμός ακολούθησε τις τεκμηριωμένες πολιτικές, πρότυπα και διαδικασίες που σχετίζονται με το Στοιχείο.
- η τεκμηρίωση για το επιλεγμένο σύστημα-στόχο καλύπτει κάθε ένα από τα κομμάτια της Περιγραφής του Στοιχείου.

Στοιχείο: ΙΙ.Α. Προσδιορισμός και τεκμηρίωση του συστήματος-στόχου
Φάση: Αρχική ιδέα και Ανάπτυξη
Στόχος: Να οριοθετηθεί η ανάλυση. Η οριοθέτηση του συστήματος-στόχου βοηθά τους οργανισμούς να αποφύγουν την παράλειψη σημαντικών στοιχείων του συστήματος και να αποφύγουν την υπερβολική ανάλυση. Ο στόχος της τεκμηρίωσης είναι να διασφαλιστεί ότι ο οργανισμός διαθέτει επαρκείς λεπτομέρειες και συμφωνία σχετικά με το σύστημα-στόχο.
Περιγραφή: Ο οργανισμός πρέπει να περιγράψει το σύστημα σε μια περίπτωση χρήσης υψηλού επιπέδου, με επαρκείς λεπτομέρειες για να δεσμεύσει την ανάλυση. Η περίπτωση χρήσης υψηλού επιπέδου θα πρέπει να περιλαμβάνει: • Τον σκοπό/στόχο/αντικείμενο του συστήματος • Τα προβλεπόμενα στοιχεία του συστήματος • Πώς θα χρησιμοποιηθεί το σύστημα • Ποιος θα χρησιμοποιήσει το σύστημα • Εάν και τι είδους προσωπικές πληροφορίες θα επεξεργάζεται το σύστημα
Οδηγίες εφαρμογής: Η περίπτωση χρήσης υψηλού επιπέδου πρέπει να τεκμηριώνεται με τρόπο που να είναι χρήσιμος σε όσους στον οργανισμό εργάζονται πάνω στο σύστημα. Η τεκμηρίωση μπορεί να περιλαμβάνει, για παράδειγμα: • Προδιαγραφές προϊόντος • Αρχιτεκτονικά διαγράμματα • Διαγράμματα ροής δεδομένων • Μητρώα δεδομένων (Data registers) • Έγγραφο επιχειρηματικών απαιτήσεων (Business requirements document BRD) • Έγγραφα επιχειρηματικής υπόθεσης (Business case document) • Ιστορίες χρηστών • Προσχέδιο • Ταξίδι του χρήστη (User journey)
Πειστήρια: Βλέπε “Γενικές Απαιτήσεις Πειστηρίων για Όλα τα Στοιχεία του Κύκλου Ζωής”

Αξιολόγηση: Βλέπε “Γενική αξιολόγηση για όλα τα στοιχεία του κύκλου ζωής”

Ο αξιολογητής θα επανεξετάσει τα πειστήρια του συστήματος-στόχου για να διαπιστώσει εάν η περίπτωση χρήσης υψηλού επιπέδου τεκμηριώνεται με τρόπο που να είναι χρήσιμο σε όσους εργάζονται στο σύστημα στον οργανισμό.

Στοιχείο: ΙΙ.Β. Προσδιορισμός και τεκμηρίωση απαιτήσεων (λειτουργικών και μη)

Φάση: Αρχική ιδέα και Ανάπτυξη

Στόχος: Να διατυπώσει ρητά τους στόχους και τα επιθυμητά χαρακτηριστικά που πρέπει να ικανοποιούνται για να καθοδηγήσει την ανάπτυξη και να χρησιμεύσει ως βάση για τις δραστηριότητες επαλήθευσης για την απόδειξη της συμμόρφωσης με τις απαιτήσεις. Αυτό επιβάλλει τη συστηματική εξέταση του τι επιδιώκει το σύστημα και πώς σκοπεύει να το επιτύχει. Ο στόχος περιλαμβάνει τη δυνατότητα επίλυσης των σχέσεων μεταξύ των απαιτήσεων. Επιπλέον, η ρητή δήλωση των απαιτήσεων διευκολύνει τις επιλογές διαχείρισης κινδύνων.

Περιγραφή: Ο οργανισμός πρέπει να διαθέτει πολιτική, πρότυπο ή διαδικασία για τον σαφή καθορισμό και την τεκμηρίωση των λειτουργικών και μη λειτουργικών απαιτήσεων για τα συστήματα-στόχους. Οι απαιτήσεις μπορεί να αφορούν ολόκληρη την επιχείρηση ή συγκεκριμένο σύστημα. Τεκμηρίωση των απαιτήσεων θα πρέπει να διατίθενται σε άλλους που εργάζονται στο σύστημα.

Οδηγίες εφαρμογής: Οι λειτουργικές απαιτήσεις αφορούν τα στοιχεία εκείνα που υποστηρίζουν άμεσα τους σκοπούς ή τους στόχους του συστήματος. Οι μη λειτουργικές απαιτήσεις αφορούν οριζόντιες ανησυχίες (χαρακτηριστικά ποιότητας) που δεν συμβάλλουν άμεσα στην επίτευξη των σκοπών ή των στόχων του συστήματος. Το απόρρητο αποτελεί παράδειγμα ποιοτικού χαρακτηριστικού, όπως και η ασφάλεια, η χρηστικότητα και η προσβασιμότητα.

Ο οργανισμός θα πρέπει να καθορίζει τις απαιτήσεις με δύο διαφορετικούς τρόπους: βασικές και ειδικές για το σύστημα.

- Οι βασικές απαιτήσεις είναι ένα τυποποιημένο σύνολο απαιτήσεων που κάθε σύστημα πρέπει να λαμβάνει υπόψη του και να ικανοποιεί, κατά περίπτωση. Κάθε βασική απαίτηση δεν είναι εξίσου εφαρμόσιμη σε κάθε σύστημα. Επομένως, κάθε απαίτηση πρέπει να αξιολογείται ως προς την εφαρμοσιμότητά της και οι αποφάσεις για την εξαίρεση ή την προσαρμογή συγκεκριμένων βασικών απαιτήσεων πρέπει να αιτιολογούνται. Για την ιδιωτικότητα, οι βασικές απαιτήσεις τείνουν να είναι καλύτερες, αλλά όχι αποκλειστικά, κατάλληλες για να διασφαλίζουν ότι τα

συστήματα εφαρμόζουν μη λειτουργικές απαιτήσεις που αφορούν τις υποχρεώσεις συμμόρφωσης και τις οργανωτικές αξίες της ιδιωτικότητας.

- Οι ειδικές για το σύστημα απαιτήσεις είναι οι απαιτήσεις που απορρέουν από τους στόχους ενός συγκεκριμένου συστήματος. Μια βασική μέθοδος εντοπισμού των μη λειτουργικών απαιτήσεων ιδιωτικότητας ειδικά για το σύστημα είναι η διενέργεια ανάλυσης κινδύνου παραβίασης της ιδιωτικότητας των λειτουργικών απαιτήσεων του συστήματος. Οι αποφάσεις για τον μετριασμό συγκεκριμένων κινδύνων θα οδηγήσουν σε απαιτήσεις ιδιωτικότητας ειδικά για το σύστημα. Οι λειτουργικές απαιτήσεις ιδιωτικότητας, λόγω της φύσης τους, τείνουν να προσδιορίζονται μέσω της ευρύτερης διαδικασίας καθορισμού των απαιτήσεων του συστήματος.

Οι απαιτήσεις είναι το τι, όχι το πώς.

Για παράδειγμα, μια βασική απαίτηση απορρήτου είναι ότι τα συστήματα πρέπει να λαμβάνουν τη συγκατάθεση του ατόμου για επικοινωνίες μάρκετινγκ (η οποία προκύπτει από τους σχετικούς νόμους στις δικαιοδοσίες στις οποίες δραστηριοποιείται ο οργανισμός). Μια ειδική για το σύστημα απαίτηση είναι ότι ένα συγκεκριμένο σύστημα αποστέλλει ένα αρχικό μήνυμα ηλεκτρονικού ταχυδρομείου σε ένα άτομο που επιλέγει να λάβει επικοινωνίες μάρκετινγκ για να επιβεβαιώσει την επιλογή του πριν προστεθεί στον κατάλογο επικοινωνιών.

Πειστήρια: Επειδή οι βασικές απαιτήσεις, αν και συνιστώνται ανεπιφύλακτα, δεν είναι απολύτως απαραίτητες, η απόδειξή τους είναι υποχρεωτική μόνο εάν ο οργανισμός ισχυρίζεται ότι χρησιμοποιούνται (για τους περισσότερους οργανισμούς μάλλον χρησιμοποιούνται). Σε όλες τις περιπτώσεις, ωστόσο, η απόδειξη των ειδικών απαιτήσεων του συστήματος είναι απαραίτητη.

- Βασικές απαιτήσεις: Ο οργανισμός πρέπει να αποδείξει πώς τεκμηριώνονται. Αυτό θα μπορούσε να λάβει τη μορφή εγγράφων ή το περιεχόμενο ενός αποθετηρίου απαιτήσεων. Το αποθετήριο απαιτήσεων μπορεί να έχει τη μορφή ειδικής βάσης δεδομένων ή συστατικού ενός ευρύτερου εργαλείου ανάπτυξης (development tool). Ο οργανισμός πρέπει επίσης να διαθέτει σχετική τεκμηρίωση διαδικασιών που διέπουν τη συντήρηση και τη χρήση των βασικών απαιτήσεων.
- Ειδικές απαιτήσεις συστήματος: Ο οργανισμός πρέπει να παρέχει τεκμηρίωση του τρόπου με τον οποίο προκύπτουν στο πλαίσιο των δραστηριοτήτων του κύκλου ζωής του συστήματός του.

Αξιολόγηση: Αν ο οργανισμός χρησιμοποιεί βασικές απαιτήσεις, ο αξιολογητής θα εξετάσει την τεκμηρίωση της διαδικασίας για να διασφαλίσει ότι διέπει τη δημιουργία και τη χρήση των βασικών απαιτήσεων. Ο αξιολογητής θα επιλέξει και θα εξετάσει ένα δείγμα βασικών απαιτήσεων από οποιοδήποτε αποθετήριο απαιτήσεων που χρησιμοποιεί ο οργανισμός. Ο αξιολογητής θα επανεξετάσει την τεκμηρίωση σχετικά με τον τρόπο με τον οποίο

προκύπτουν οι ειδικές απαιτήσεις του συστήματος. Ο αξιολογητής θα επιλέξει και θα επανεξετάσει ένα δείγμα ειδικών απαιτήσεων συστήματος για το σύστημα-στόχο που έχει επιλεγεί για επανεξέταση.

Στοιχείο: ΙΙ.Γ. Εκτέλεση ανάλυσης συμβιβασμού

Φάση: Αρχική ιδέα και Ανάπτυξη

Στόχος: Για να εξασφαλιστεί ότι οι συμβιβασμοί εντοπίζονται και επιλύονται ρητά, αποφεύγοντας ανεπίσημες ή εγγενείς λύσεις που μπορεί να αποδειχθούν προβληματικές και πιθανόν να μην έχουν τεκμηριωθεί, αποτρέποντας έτσι κάθε προσπάθεια μεταγενέστερης ανακατασκευής, αν παραστεί ανάγκη.

Περιγραφή: Η ανάλυση συμβιβασμού είναι:

- Προσδιορισμός των σημείων απόφασης κατά τη διάρκεια της αρχικής ιδέας ή της ανάπτυξης
- Διατύπωση των διαθέσιμων επιλογών
- Προσδιορισμός των ανταγωνιστικών ιδιοτήτων/προτεραιοτήτων που παρουσιάζουν οι διαθέσιμες επιλογές
- Σύγκριση των επιλογών με βάση τις ιδιότητες/προτεραιότητες έναντι των απαιτήσεων του συστήματος
- Καθορισμός αποδεκτού σχεδιασμού

Η τεκμηρίωση της ανάλυσης συμβιβασμού θα πρέπει να περιλαμβάνει τόσο τις αποφάσεις όσο και τις αιτιολογήσεις

Οδηγίες εφαρμογής: Η ανάλυση συμβιβασμού είναι ευθύνη του ιδιοκτήτη του συστήματος. Ο ιδιοκτήτης θα πρέπει να ορίσει άτομα με επαρκή κατανόηση του χώρου σχεδιασμού ώστε να λάβουν αποφάσεις και να συμπεριλάβουν τη συμβολή των ενδιαφερομένων μερών.

Η ανάλυση συμβιβασμού προϋποθέτει την ύπαρξη εύλογων εναλλακτικών λύσεων σχεδιασμού επαρκούς λεπτομέρειας για την υποστήριξη συστηματικών συγκρίσεων. Συνεπώς, πρέπει να συνδέεται κατάλληλα με τον κύκλο ζωής του έργου. Σε τελική ανάλυση, ωστόσο, είναι μια μορφή ανάλυσης αποφάσεων.

Α. Θα πρέπει να χρησιμοποιούνται συγκεκριμένες μέθοδοι εκτέλεσης της ανάλυσης, ώστε αυτή να είναι συστηματική.

Οι μέθοδοι που χρησιμοποιούνται στη μηχανική συστημάτων (systems engineering) περιλαμβάνουν μεταξύ άλλων:

1. Σύγκριση πλεονεκτημάτων και μειονεκτημάτων

2. Διαγράμματα επιρροής (Influence diagrams)
3. Δέντρα αποφάσεων (Decision trees)
4. Διαδικασία αναλυτικής ιεραρχίας
5. Καταμέτρηση Borda (Borda counting)

Β. Τα αποτελέσματα μιας ανάλυσης συμβιβασμού θα πρέπει να τεκμηριώνονται με κάποιο τρόπο, αν και ο βαθμός τυπικότητας μπορεί να ποικίλλει. Είναι σημαντικό η τεκμηρίωση, ανεξαρτήτως της μορφής της, να διατηρείται και να είναι προσβάσιμη, ώστε να είναι δυνατή η επανεξέταση των αποφάσεων συμβιβασμού, αν χρειαστεί.

Οι εταιρείες μπορούν να διεξάγουν ανάλυση συμβιβασμού για κοινά σενάρια που εφαρμόζονται σε πολλαπλά σχέδια. Οι αναλύσεις αυτές μπορούν να ενσωματωθούν στα πρότυπα σχεδιασμού.

Πειστήρια

- Ο οργανισμός πρέπει να παρέχει τεκμηρίωση που να αποδεικνύει την πρόβλεψη για ανάλυση συμβιβασμού αποτελεσμάτων στο πλαίσιο των διαδικασιών του κύκλου ζωής του οργανισμού, συμπεριλαμβανομένων των προδιαγεγραμμένων ή προτεινόμενων μεθόδων. Η εν λόγω τεκμηρίωση μπορεί να διαθέτει διαδικασία εξαιρέσεων (exception process) που επιτρέπει την κλιμάκωση των αποφάσεων εκτός της κανονικής διαδικασίας συμβιβασμού.
- Ο οργανισμός πρέπει να διαθέτει δείγματα των αποτελεσμάτων των αναλύσεων συμβιβασμού που πραγματοποιήθηκαν.

Για τα πρότυπα σχεδιασμού, ο οργανισμός πρέπει να παρέχει τεκμηρίωση της ανάλυσης συμβιβασμών που έγινε κατά την ανάπτυξη των προτύπων ή αιτιολόγηση των αποφάσεων σχεδιασμού που λήφθηκαν χωρίς ανάλυση συμβιβασμών.

Αξιολόγηση: Ο αξιολογητής θα επανεξετάσει τις ελάχιστες απαιτήσεις της διαδικασίας ανάλυσης συμβιβασμού για να διασφαλίσει ότι ανταποκρίνεται στο Στόχο του Στοιχείου, δηλαδή ότι ο οργανισμός, ανεξάρτητα από την τυπικότητα, πρέπει να:

- να προσδιορίζει ρητά τις ευκαιρίες λήψης αποφάσεων στο σχεδιασμό που έχουν πολλαπλούς δυνητικά αντικρουόμενους στόχους, χαρακτηριστικά ή/και περιορισμούς,
- να επιλύει τις αποφάσεις αυτές, και
- να τεκμηριώνει τις αποφάσεις και τις αιτιολογήσεις.

Το/τα ενδεικτικά δείγματα, που επιλέγονται από τον αξιολογητή, πρέπει να δείχνουν την οργάνωση ως εξής την τεκμηριωμένη διαδικασία.

Στοιχείο: ΙΙ.Δ. Εκτέλεση ανάλυσης συμβιβασμού
Φάση: Αρχική ιδέα, Ανάπτυξη και Εγκατάσταση
Στόχος: Επίτευξη αποδεκτού επιπέδου κινδύνου παραβίασης της ιδιωτικότητας

Υπο-Στοιχείο: ΙΙ.Δ.1. Εκτέλεση εκτίμησης κινδύνου
Φάση: Αρχική ιδέα, Ανάπτυξη και Εγκατάσταση
Στόχος: Να κατανοηθεί το επίπεδο κινδύνου

Υπο-Στοιχείο: ΙΙ.Δ.1.α Πλαισίωση παραγόντων κινδύνου
Στόχος: Ευθυγράμμιση του πλαισίου του συστήματος-στόχου με τους παράγοντες του μοντέλου κινδύνου. Αυτό επιτρέπει την αξιολόγηση κινδύνου παραβίασης της ιδιωτικότητας με τη χρήση του μοντέλου κινδύνου του οργανισμού.
Περιγραφή: Ο οργανισμός προσδιορίζει και τεκμηριώνει το πλαίσιο που περιβάλλει το σύστημα-στόχο. Τα στοιχεία του πλαισίου που εξετάζονται πρέπει να αντιστοιχούν στους παράγοντες του μοντέλου κινδύνου που συμβάλλουν στον κίνδυνο παραβίασης της ιδιωτικότητας. Παραδείγματα αντίστοιχου πλαισίου σε παράγοντα κινδύνου περιλαμβάνουν: ένας παράγοντας ατόμων που διατρέχουν κίνδυνο σε ένα συγκεκριμένο πλαίσιο συστήματος-στόχου μπορεί να είναι οι εργαζόμενοι, τα δεδομένα που μπορεί να συσχετιστούν με το πλαίσιο ως μισθοδοσία, το πρόγραμμα και ποσοστά αμοιβής, οι φορείς απειλής (threat actors) μπορεί να συσχετιστούν με το πλαίσιο ως διευθυντές ή άλλοι εργαζόμενοι, και τα αντίμετρα μπορεί να συσχετιστούν με το πλαίσιο ως δεδομένα που είναι κρυπτογραφημένα με AES 256.
Οδηγίες εφαρμογής: Ο οργανισμός θα πρέπει να εξετάσει κάθε παράγοντα που συμβάλλει στον κίνδυνο εντός του μοντέλου κινδύνου και να προσδιορίσει τις συγκεκριμένες τιμές για τους παράγοντες αυτούς. Οι οργανισμοί θα πρέπει να καταγράφουν επίσημα αυτές τις αξίες και να τις θέτουν στη διάθεση του ατόμου που διενεργεί την αξιολόγηση κινδύνου. Οι αξίες θα πρέπει να προσδιορίζονται αντικειμενικά και να προέρχονται από πηγές, ή όταν βασίζονται σε υποκειμενικές εκτιμήσεις, θα πρέπει να περιγράφεται ρητά το σκεπτικό. Θα πρέπει να παρέχονται αιτιολογήσεις για τον αποκλεισμό ορισμένων τιμών, κατά παράβαση του μοντέλου κινδύνου.

Πειστήρια: Ο οργανισμός προσδιορίζει τα τμήματα της διαδικασίας εκτίμησης κινδύνου που πλαισιώνουν τους παράγοντες του μοντέλου κινδύνου. Ο οργανισμός έχει τεκμηριώσει τις τιμές για τους παράγοντες πλαισίου των συστημάτων-στόχων.
Αξιολόγηση: Βλέπε “Γενική αξιολόγηση για όλα τα στοιχεία του κύκλου ζωής” Ο αξιολογητής επιλέγει και επανεξετάζει τους παράγοντες του πλαισίου για τα συστήματα-στόχους (που επίσης επιλέγονται από τον αξιολογητή).

Υπο-Στοιχείο: ΙΙ.Δ.1.β Συγκέντρωση θεμάτων ιδιωτικότητας
Στόχος: Εντοπισμός πιθανών ζητημάτων ιδιωτικότητας στην τρέχουσα έκδοση του συστήματος-στόχου το συντομότερο δυνατό πριν από την ανάπτυξη, ώστε να μειωθεί το κόστος που συνδέεται με τον μετριασμό των ζητημάτων.
Περιγραφή: Ο οργανισμός, μέσω μιας συστηματικής διαδικασίας και χρησιμοποιώντας το δικό του μοντέλο κινδύνου ή ένα συγκεκριμένο για το σύστημα, προσδιορίζει και τεκμηριώνει τις απειλές, τις ευπάθειες και τις συνέπειες που μπορούν να εμφανιστούν στο σύστημα-στόχο.
Οδηγίες εφαρμογής: Ο οργανισμός εφαρμόζει μια συστηματική προσέγγιση μοντελοποίησης απειλών (threat-modeling) για τον εντοπισμό ζητημάτων ιδιωτικότητας για κάθε σύστημα-στόχο. Το μοντέλο κινδύνου που χρησιμοποιείται για αυτή την άσκηση ανάδειξης ζητημάτων θα καθορίσει την εστίαση και συνεπώς την κάλυψη της ανάλυσης. Ο οργανισμός θα πρέπει να αποτυπώνει τυχόν παραδοχές που έγιναν κατά τη διάρκεια της άσκησης ανάδειξης.
Πειστήρια: Ο οργανισμός έχει τεκμηριώσει τη συστηματική προσέγγιση που εφαρμόζεται και έχει καταγράψει τα εντοπισμένα ζητήματα στο σύστημα-στόχο.
Αξιολόγηση: Ο αξιολογητής θα καθορίσει εάν η προσέγγιση του οργανισμού για την ανάδειξη των ζητημάτων είναι επαρκώς συστηματική ώστε να εντοπίζει ολοκληρωμένα όλες τις απειλές, τις ευπάθειες και τις συνέπειες που προκύπτουν από το συγκεκριμένο μοντέλο κινδύνου για τον οργανισμό ή το σύστημα και ότι η προσέγγιση μπορεί να εφαρμοστεί με συνέπεια. Ο αξιολογητής θα επανεξετάσει τα ζητήματα που εντοπίστηκαν στο σύστημα-στόχο για να διασφαλίσει ότι αναφέρθηκαν όλες οι απειλές, τα τρωτά σημεία και οι συνέπειες.

Υπο-Στοιχείο: ΙΙ.Δ.1.γ Εκτίμηση κινδύνων
Στόχος: Να προσδιοριστεί ποιοι κίνδυνοι παραβίασης της ιδιωτικότητας υπερβαίνουν την οργανωτική ανοχή και διάθεση.
Περιγραφή: Χρησιμοποιώντας τα εντοπισμένα ζητήματα ιδιωτικότητας, ο οργανισμός διενεργεί αξιολόγηση για να μετρήσει τους κινδύνους παραβίασης της ιδιωτικότητας που εισάγει το σύστημα-στόχος. Οι κίνδυνοι συγκρίνονται με την ανοχή του οργανισμού για τον εντοπισμό μη-αποδεκτών κινδύνων που χρήζουν μετριασμού.
Οδηγίες εφαρμογής: Ποσοτικές και ποιοτικές μετρήσεις κινδύνων είναι αποδεκτές, ωστόσο, θα πρέπει να υπάρχουν αντικειμενικά κριτήρια για τις μετρήσεις ή τις εκτιμήσεις. Όπου επιτρέπεται ο υποκειμενικός προσδιορισμός, ο οργανισμός πρέπει να παρέχει καθοδήγηση σχετικά με τον τρόπο να προβεί στον εν λόγω προσδιορισμό, καθώς και την αιτιολόγηση της χρήσης υποκειμενικού προσδιορισμού αντί αντικειμενικών κριτηρίων. Ο κίνδυνος και η ανοχή κινδύνου μπορούν να εξεταστούν υπό το πρίσμα των αντισταθμιστικών οφελών για τα θιγόμενα άτομα ή την κοινωνία. Η εκτίμηση κινδύνου μπορεί να λαμβάνει υπόψη τους υφιστάμενους και τεκμηριωμένους ελέγχους και μετριασμούς. Η εκτίμηση κινδύνου πρέπει να ενσωματώνει το πλαίσιο στο οποίο λειτουργεί το σύστημα-στόχος. Οι αξιολογήσεις κινδύνων δεν είναι απαραίτητο να πραγματοποιούνται πάντα στο πλαίσιο ενός συγκεκριμένου συστήματος, και οι κίνδυνοι μπορούν να αξιολογούνται γενικά με μετριασμούς που εισάγονται μέσω προτύπων ή βασικών απαιτήσεων. Για παράδειγμα, οι κίνδυνοι ασφάλειας από μη εξουσιοδοτημένη πρόσβαση σε μεταδιδόμενα δεδομένα μπορούν να μετριαστούν μέσω της κρυπτογράφησης. Ένας οργανισμός δεν χρειάζεται να διενεργεί αξιολόγηση κινδύνου σε κάθε μετάδοση δεδομένων, υπό την προϋπόθεση ότι ο μετριασμός εφαρμόζεται και τεκμηριώνεται.
Πειστήρια: Ο οργανισμός πρέπει να διαθέτει τεκμηριωμένη προσέγγιση για τη διενέργεια εκτιμήσεων κινδύνου.
Αξιολόγηση: Η προσέγγιση εκτίμησης κινδύνου θα επανεξεταστεί ως προς την αντικειμενικότητα και την ικανότητά της να εφαρμόζεται με συνέπεια όταν χρησιμοποιούνται υποκειμενικά μέτρα.

Υπο-Στοιχείο: ΙΙ.Δ.2. Ανταπόκριση στους κινδύνους
Στόχος: Να τοποθετηθούν οι κίνδυνοι παραβίασης της ιδιωτικότητας εντός της αποδεκτής οργανωτικής ανοχής.
Περιγραφή: Εάν οι κίνδυνοι παραβίασης της ιδιωτικότητας υπερβαίνουν την ανοχή του οργανισμού, ο οργανισμός έχει δύο επιλογές: να μειώσει τους κινδύνους παραβίασης της

ιδιωτικότητας ή να αυξήσει την ανοχή του στον κίνδυνο παραβίασης της ιδιωτικότητας (προτιμάται το πρώτο). Ο συνηθέστερος τρόπος για τη μείωση του κινδύνου παραβίασης της ιδιωτικότητας είναι η εισαγωγή τεχνικών ή διοικητικών αντιμέτρων που αλλάζουν το πλαίσιο της ανάλυσης. Ωστόσο, δεν θα έχουν όλες οι αλλαγές στο πλαίσιο τη μορφή αντιμέτρων. Για παράδειγμα, η απόφαση να μην παρέχεται μια υπηρεσία σε ανηλίκους θα ήταν ένα παράδειγμα αλλαγής πλαισίου που θα αύξανε την πιθανότητα να χρησιμοποιείται η υπηρεσία σας από άτομα που μπορεί να είναι πιο ώριμα και ικανά να κατανοήσουν τους κινδύνους που ενέχει η χρήση της υπηρεσίας. Όταν χρησιμοποιούνται αντίμετρα για τον μετριασμό των κινδύνων, θα πρέπει να σχεδιάζονται, να αναπτύσσονται ή να αναπτύσσονται, ανάλογα με την περίπτωση, ώστε να μειώνουν επαρκώς τους κινδύνους. Η αξιολόγηση του υπολειπόμενου κινδύνου θα καταδεικνύει αυτή τη μείωση.
Οδηγίες εφαρμογής: Ο οργανισμός πρέπει να έχει μια προσέγγιση για την επανεξέταση των αλλαγών στο πλαίσιο (όπως η επιλογή αντιμέτρου) για τον μετριασμό των κινδύνων παραβίασης της ιδιωτικότητας. Ενώ οι αλλαγές πλαισίου δεν χρειάζεται να είναι απολύτως αντικειμενικές, ο οργανισμός θα πρέπει να είναι σε θέση να αιτιολογήσει γιατί έγιναν οι αλλαγές και γιατί δεν επιλέχθηκαν άλλοι. Αυτό είναι ακόμη πιο σημαντικό όταν δεν έγιναν αλλαγές στο πλαίσιο και η ανοχή οργανωτικού κινδύνου επεκτάθηκε ώστε να ληφθούν υπόψη οι εντοπισμένοι κίνδυνοι παραβίασης της ιδιωτικότητας. Κατά την επιλογή τεχνικών ή οργανωτικών ελέγχων, μπορεί να αξιοποιηθεί ένα πλαίσιο, όπως το Hoepman Privacy Design Strategies and Tactics ή το σύνολο ελέγχων NIST, ώστε να διασφαλιστεί ότι ο οργανισμός διαθέτει ένα ολοκληρωμένο σύνολο ελέγχων.
Πειστήρια: Ο οργανισμός πρέπει να παρέχει τεκμηριωμένη προσέγγιση για τον εντοπισμό αντιμέτρων για τον μετριασμό των κινδύνων παραβίασης της ιδιωτικότητας. Η επιλογή των αντιμέτρων πρέπει να περιλαμβάνει αιτιολόγηση των λόγων για τους οποίους επιλέχθηκαν ορισμένοι αντίμετρα και όχι άλλα. Ο οργανισμός θα πρέπει να τεκμηριώνει τα επιλεγμένα αντίμετρα και τα μέτρα μετριασμού και να παρακολουθεί το σκεπτικό της επιλογής όταν λαμβάνονται αποφάσεις συμβιβασμού.
Αξιολόγηση: Η προτεινόμενη προσέγγιση πρέπει να είναι σε θέση να μετριάσει όλους τους παράγοντες κινδύνου ως μέρος του μοντέλου κινδύνου παραβίασης της ιδιωτικότητας.

Στοιχείο: ΙΙ.Ε. Επαλήθευση του πλαισίου και των απαιτήσεων του συστήματος-στόχου
Φάση: Ανάπτυξη και Εγκατάσταση
Στόχος: Να διασφαλιστεί ότι οι παραδοχές του συστήματος-στόχου είναι σωστές και ότι το σύστημα-στόχος λειτουργεί όπως αναμένεται στο προβλεπόμενο περιβάλλον.
Περιγραφή: Χρησιμοποιώντας υποθέσεις σχετικά με το πλαίσιο, τις απαιτήσεις και τα αντίμετρα, που προσδιορίστηκαν στη φάση της Αρχικής Ιδέας και χρησιμοποιήθηκαν στη διαδικασία σχεδιασμού, ο οργανισμός πρέπει να επανεξετάσει κατά πόσον αυτές οι υποθέσεις, οι απαιτήσεις και τα αντίμετρα ήταν ανακριβείς, ελλιπείς ή αναποτελεσματικοί.
Οδηγίες εφαρμογής: Οι διαδικασίες του οργανισμού θα πρέπει να περιλαμβάνουν βήματα για την επανεξέταση των παραδοχών σχετικά με το πλαίσιο του συστήματος-στόχου, τις απαιτήσεις και τους ελέγχους μετά την αξιολόγηση. Για παράδειγμα, η υπόθεση ότι σε ένα σύστημα θα συμπεριληφθούν μόνο δεδομένα πελατών μπορεί να αποδειχθεί λανθασμένη όταν οι πελάτες αρχίσουν να ανεβάζουν φωτογραφίες συγγενών τους, γεγονός που καθιστά αναγκαία τη διενέργεια αξιολόγησης των κινδύνων προστασίας της ιδιωτικής ζωής για μη πελάτες.
Πειστήρια: Βλέπε Γενικές Απαιτήσεις Πειστηρίων για Όλα τα Στοιχεία του Κύκλου Ζωής
Αξιολόγηση: Βλέπε Γενική Αξιολόγηση για όλα τα Στοιχεία του Κύκλου Ζωής

Στοιχείο: ΙΙ.Ζ. Παρακολούθηση του πλαισίου
Φάση: Εγκατάσταση
Στόχος: Να διασφαλιστεί ότι το πλαίσιο μετά την εγκατάσταση δεν θα αλλοιώσει την εκτίμηση κινδύνου και τις αποφάσεις που ελήφθησαν, απαιτώντας επαναξιολόγηση.
Περιγραφή: Θα πρέπει να παρακολουθούνται, τουλάχιστον οι: • διαφορές μεταξύ προσδοκώμενης και πραγματικής χρήσης • αλλαγές στο σύστημα-στόχο • αλλαγές στον οργανισμό • αλλαγές στο επιχειρηματικό περιβάλλον • αλλαγές στις εσωτερικές επιχειρηματικές λειτουργίες • αλλαγές στη νομοθεσία, τις πολιτικές, τις οδηγίες, τους κανονισμούς, τα πρότυπα και τους κοινωνικούς κανόνες Ι. Σύστημα-στόχος: Ο οργανισμός προσδιορίζει και τεκμηριώνει το πλαίσιο για την παρακολούθηση αλλαγών στο σύστημα-στόχο.

Α. Ο οργανισμός πρέπει να διαθέτει πολιτικές και διαδικασίες για την επαλήθευση της εφαρμογής όλων των απαιτήσεων ιδιωτικότητας.
Β. Ο οργανισμός πρέπει να διαθέτει διαδικασίες για την τακτική αξιολόγηση των αντιμέτρων ασφάλειας και προστασίας της ιδιωτικότητας του συστήματος-στόχου, ώστε να επιβεβαιώνεται ότι τα αντίμετρα συνεχίζουν να λειτουργούν αποτελεσματικά. Ο οργανισμός αποκαθιστά τυχόν μη συμμορφούμενα αντίμετρα ιδιωτικότητας ή ευπάθειες.

ΙΙ. Οργανισμός: Ο οργανισμός προσδιορίζει και τεκμηριώνει το πλαίσιο για την παρακολούθηση των αλλαγών στον οργανισμό που μπορεί να μεταβάλλουν την αξιολόγηση κινδύνου του συστήματος-στόχου. Συγκεκριμένα:

Α. Ο οργανισμός πρέπει να διαθέτει διαδικασίες για την παρακολούθηση της επιχειρηματικής στρατηγικής του, του πλαισίου διαχείρισης της ιδιωτικής ζωής και των προτεραιοτήτων διαχείρισης κινδύνων.
Β. Ο οργανισμός πρέπει να διαθέτει διαδικασίες για την παρακολούθηση των δραστηριοτήτων συγχώνευσης και εξαγοράς ή επέκτασης προϊόντων και υπηρεσιών σε άλλη χώρα ή περιοχή.

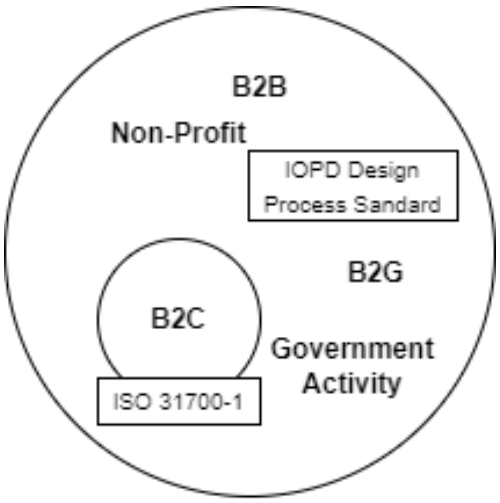
ΙΙΙ. Επιχειρηματικό περιβάλλον: Ο οργανισμός προσδιορίζει και τεκμηριώνει το πλαίσιο για την παρακολούθηση των αλλαγών στις επιχειρηματικές διαδικασίες, τις διαδικασίες πληροφοριών και τα περιβάλλοντα και τις υποδομές συστημάτων που ενδέχεται να μεταβάλλουν τις απαιτήσεις της ιδιωτικότητας και επιβεβαιώνει ότι τα επιλεγμένα αντίμετρα ιδιωτικότητας εξακολουθούν να είναι αποτελεσματικά.

Α. Ο οργανισμός πρέπει να διαθέτει διαδικασίες για την ανάδειξη νέων ή μεταβαλλόμενων απειλών ιδιωτικότητας σε προϊόντα και υπηρεσίες. Αξιολογείται η αποτελεσματικότητα των αντιμέτρων ιδιωτικότητας έναντι νέων και αναθεωρημένων απειλών και λαμβάνονται τα κατάλληλα μέτρα για τη μείωση των αυξημένων κινδύνων.
Β. Ο οργανισμός πρέπει να διαθέτει διαδικασίες για την τακτική διενέργεια αξιολογήσεων ευπαθειών ιδιωτικότητας (privacy vulnerability assessments) για προϊόντα και υπηρεσίες. Αξιολογείται η έκθεση του οργανισμού σε ευπάθειες ιδιωτικότητας και λαμβάνονται τα κατάλληλα μέτρα για την αντιμετώπιση τυχόν συναφών κινδύνων.
Γ. Ο οργανισμός πρέπει να διαθέτει διαδικασίες για τις περιπτώσεις αλλαγής του περιβάλλοντος ή της υποδομής του συστήματος (π.χ. on-site έναντι cloud). Τα προϊόντα και οι υπηρεσίες πρέπει να επανεξετάζονται και να δοκιμάζονται ώστε να διασφαλίζεται ότι δεν υπάρχει αντίκτυπος στην ιδιωτικότητα.
Δ. Ο οργανισμός πρέπει να διαθέτει διαδικασίες για την ανάθεση προϊόντων, υπηρεσιών ή διαδικασιών σε τρίτους, ώστε να αξιολογεί τους κινδύνους παραβίασης

της ιδιωτικότητας και να διασφαλίζει ότι τα επιλεγμένα αντίμετρα ιδιωτικότητας εξακολουθούν να είναι αποτελεσματικά. Ε. Ο οργανισμός πρέπει να έχει θεσπίσει διαδικασίες για την ταχεία, αποτελεσματική και ομαλή αντιμετώπιση περιστατικών ιδιωτικότητας (privacy incidents). Ζ. Ο οργανισμός πρέπει να διαθέτει διαδικασίες για την παρακολούθηση όλων των νόμων και κανονισμών που σχετίζονται με την ιδιωτικότητα και να προσδιορίζει ρητά και να τεκμηριώνει τη μέθοδο συμμόρφωσής του με τους εν λόγω νόμους και κανονισμούς.
Οδηγίες εφαρμογής: Ο οργανισμός πρέπει να ορίζει και να εφαρμόζει τεκμηριωμένες πολιτικές και διαδικασίες για τη συστηματική παρακολούθηση των αλλαγών όταν υπάρχει αλλαγή στο υπάρχον σύστημα, τον οργανισμό ή το επιχειρηματικό περιβάλλον ή/και τις εσωτερικές επιχειρηματικές λειτουργίες, ώστε να διασφαλίζεται η μέτρηση, η ανάλυση και ο μετριασμός των κινδύνων παραβίασης της ιδιωτικότητας. Ο οργανισμός πρέπει να διατηρεί τεκμηρίωση που να χρησιμεύει ως απόδειξη της συμμόρφωσης, συμπεριλαμβανομένων των σχεδίων αποκατάστασης για τη διόρθωση των ελλείψεων που διαπιστώνονται κατά την παρακολούθηση. Ο οργανισμός θα πρέπει να εξετάσει τις διαφορές μεταξύ των υποθέσεων και της χρήσης ("fly as you test"). Οι παραδοχές ελέγχουν ότι όλες οι απαιτήσεις μεταφράζονται επιτυχώς σε απαιτήσεις, επαληθεύονται και λειτουργούν όπως αναμένεται. Η χρήση δοκιμάζει τη συμπεριφορά νέων σεναρίων, απροσδόκητων συνθηκών ή δημιουργικών λειτουργιών που επιτρέπει ο σχεδιασμός του προϊόντος ή της υπηρεσίας. Ο οργανισμός πρέπει να διαθέτει τεκμηριωμένες πολιτικές, διαδικασίες ή/και διεργασίες για την καταγραφή των αποτελεσμάτων των δοκιμών για τις παραδοχές και τη χρήση, καθώς και τον μετριασμό με βάση το όφελος έναντι του κινδύνου.
Πειστήρια: Βλέπε Γενικές Απαιτήσεις Πειστηρίων για Όλα τα Στοιχεία του Κύκλου Ζωής
Αξιολόγηση: Βλέπε Γενική Αξιολόγηση για όλα τα Στοιχεία του Κύκλου Ζωής

3. Σύγκριση των Προτύπων

Υπάρχει μεγάλη δραστηριότητα στην τυποποίηση των απαιτήσεων ιδιωτικότητας ήδη από τον σχεδιασμό. Νωρίτερα φέτος, τόσο το Institute of Operational Privacy Design (IOPD) όσο και ο Διεθνής Οργανισμός Τυποποίησης (ISO) κυκλοφόρησαν πρότυπα. Ο IOPD κυκλοφόρησε το Πρότυπο Διαδικασίας Σχεδιασμού [57] και το ISO κυκλοφόρησε το ISO-31700-1 [1]. Όπως υποδηλώνει το όνομα του προτύπου IOPD, καλύπτει τα απαραίτητα στοιχεία για την ενσωμάτωση των θεωρήσεων της ιδιωτικότητας στη "διαδικασία" σχεδιασμού ενός οργανισμού, είτε πρόκειται για το σχεδιασμό ενός προϊόντος, μιας υπηρεσίας ή μιας επιχειρηματικής διαδικασίας. Το Πρότυπο ISO θέτει το οργανωτικό πλαίσιο για την ιδιωτικότητα ως επικάλυψη του κύκλου ζωής ανάπτυξης λογισμικού (Software Development Life Cycle - SDLC), χωρίς να περιορίζεται σε κάποιο συγκεκριμένο στάδιο. Αυτό το κεφάλαιο, και αφού έχουν εξετασθεί σε βάθος τα δύο πρότυπα, συγκρίνει και αντιπαραβάλλει τα δύο πρότυπα. Θα εξεταστούν μερικοί βασικοί τομείς. Αρχικά, το πρότυπο IOPD είναι ένα πρότυπο συμμόρφωσης, πράγμα που σημαίνει ότι ένας οργανισμός μπορεί να πιστοποιηθεί ότι ακολουθεί το πρότυπο. Για κάθε στοιχείο, το πρότυπο παρέχει πειστήρια (evidence) και κριτήρια αξιολόγησης (evaluation criteria). Από την άλλη, το πρότυπο ISO δεν αναπτύχθηκε ως πρότυπο συμμόρφωσης. Οι απαιτήσεις είναι υψηλού επιπέδου (high-level), παρέχοντας έτσι υπερβολική υποκειμενικότητα σε οποιαδήποτε αξιολόγηση.
Ένα άλλο σημείο διάκρισης, είναι ότι το Πρότυπο ISO επικεντρώνεται ειδικά στους καταναλωτές και στο μοντέλο Business to Consumer (B2C), ενώ το Πρότυπο IOPD είναι ευρύ και επιτρέπει την εξέταση των κινδύνων για όλα τα άτομα που επηρεάζονται από τα συστήματα όλων των τύπων οργανισμών, συμπεριλαμβανομένων, μεταξύ άλλων, εκείνων που λειτουργούν σε πλαίσια B2C, Business to Business (B2B), κυβέρνησης, εργασιακού περιβάλλοντος και μη κερδοσκοπικών οργανισμών. Οι επιχειρήσεις που επικεντρώνονται στην καταναλωτική αγορά θα μπορούσαν επομένως να εφαρμόσουν και τα δύο πρότυπα, αλλά όσοι δεν έχουν εντολές για καταναλωτές θα πρέπει να χρησιμοποιήσουν το πρότυπο IOPD.



Εικόνα 2 - Που απευθύνεται το κάθε πρότυπο

Ενώ και τα δύο πρότυπα χρησιμοποιούν τον όρο "απαιτήσεις" και τη σημασία της ενσωμάτωσης της ιδιωτικότητας σε αυτά, ο όρος χρησιμοποιείται διαφορετικά σε κάθε πρότυπο. Η κατανόηση αυτής της διάκρισης είναι σημαντική. Η σωστή χρήση του όρου "απαιτήσεις" είναι ένας από τους τρόπους με τους οποίους τα δύο αυτά πρότυπα μπορούν να συνεργαστούν. Το πρότυπο ISO περιλαμβάνει 27 υψηλού επιπέδου τεχνικές και επιχειρηματικές ειδικές απαιτήσεις που σχετίζονται με την ιδιωτικότητα για τον οργανισμό που επιθυμεί να εφαρμόσει το πρότυπο. Οι περισσότερες από τις απαιτήσεις ξεκινούν με το "Ο οργανισμός θα πρέπει να [...]". Ένα παράδειγμα είναι:

"*Ο οργανισμός θα πρέπει να προσδιορίζει τις ανάγκες των καταναλωτών σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα από προϊόντα που έχουν σχεδιαστεί και αναπτυχθεί για τους καταναλωτές*".

Το πρότυπο συνεχίζει παρέχοντας λεπτομερή επεξήγηση και την αντίστοιχη οδηγία. Ορισμένες από τις επιχειρηματικές απαιτήσεις του προτύπου ISO απαιτούν στην πραγματικότητα συγκεκριμένες απαιτήσεις σε επίπεδο συστήματος. "Ο οργανισμός θα πρέπει να σχεδιάζει ρυθμίσεις απορρήτου και μέτρα διαχείρισης απορρήτου που μπορούν να διαμορφωθούν από τον καταναλωτή, λαμβάνοντας υπόψη τις δυνατότητες των καταναλωτών και τις πιθανές ειδικές ανάγκες τους". Αυτό περιγράφει μια επιχειρησιακή απαίτηση (ένα μέρος της διαδικασίας σχεδιασμού) για να συμπεριλάβει ένα χαρακτηριστικό (μια απαίτηση συστήματος του προϊόντος ή της υπηρεσίας που σχεδιάζεται). Αυτή η τελευταία χρήση της λέξης “απαίτηση” συνάδει με τη χρήση του όρου στο πρότυπο IOPD, δηλαδή για την περιγραφή των λειτουργικών και μη λειτουργικών απαιτήσεων του συστήματος (προϊόν, υπηρεσία ή επιχειρησιακή διαδικασία) που σχεδιάζεται. Επειδή το Πρότυπο IOPD αναφέρει ότι ένας οργανισμός πρέπει να θεσπίζει απαιτήσεις, αλλά δεν ορίζει τι είναι αυτές, ένας οργανισμός θα μπορούσε να χρησιμοποιήσει ορισμένες από τις απαιτήσεις του Προτύπου ISO, δηλαδή εκείνες, όπως η παραπάνω, που απαιτούν απαιτήσεις συστήματος. Αυτό μπορεί να προκαλέσει σύγχυση, γι’ αυτό και είναι σημαντικό να διευκρινιστεί η διάκριση αυτή.

Αξίζει να σημειωθεί ότι αυτό που το πρότυπο ISO αποκαλεί απαίτηση (ένα απαραίτητο στοιχείο για να ακολουθήσει ο οργανισμός το πρότυπο), το πρότυπο IOPD το αποκαλεί στοιχείο (Component – ένα "απαραίτητο" συστατικό που πρέπει να έχει η διαδικασία σχεδιασμού του οργανισμού).

Η λογοδοσία (accountability) αποτελεί χαρακτηριστικό γνώρισμα της καλής επιχειρηματικής διακυβέρνησης και βασική πτυχή των επιτυχημένων προγραμμάτων ιδιωτικότητας. Και τα δύο πρότυπα απαιτούν λογοδοσία, αν και την προσεγγίζουν ελαφρώς διαφορετικά. Το πρότυπο ISO απαιτεί ένα υπεύθυνο πρόσωπο για την επισκόπηση του κύκλου ζωής του προϊόντος (4.5.1 Απαίτηση) και για κάθε λειτουργία στο σχεδιασμό ή τη λειτουργία των αντιμέτρων ιδιωτικότητας (4.6.1 Απαίτηση). Το Πρότυπο IOPD υιοθετεί μια λίγο πιο ολιστική και οργανωτική προσέγγιση και απαιτεί την λογοδοσία ως προϋπόθεση στο επίπεδο διακυβέρνησης, δηλώνοντας ότι πρέπει να υπάρχει "*ιδιοκτησία (ownership) ή λογοδοσία για κάθε ένα από τα σημεία της διαδικασίας σχεδιασμού*". Αυτό αναδεικνύει τις διαφορές και επισημαίνει τη συμβατότητα των δύο. Το πρότυπο IOPD προϋποθέτει καλή διακυβέρνηση ως προϋπόθεση, ενώ το πρότυπο ISO περιλαμβάνει πιο λεπτομερή οργανωτικά χαρακτηριστικά ως μέρος του συνόλου των απαιτήσεών του. Παρόμοια με τον τρόπο με τον οποίο συγκεκριμένες απαιτήσεις σε επίπεδο συστήματος από το πρότυπο ISO μπορούν να χρησιμοποιηθούν για όσους εφαρμόζουν το πρότυπο IOPD, οι σχετικές οργανωτικές απαιτήσεις θα μπορούσαν να χρησιμοποιηθούν ως πειστήρια της εκπλήρωσης του προτύπου IOPD για τη διακυβέρνηση.

Και τα δύο πρότυπα λαμβάνουν υπόψη τον κίνδυνο παραβίασης ιδιωτικότητας, αλλά, όπως και πριν, τον προσεγγίζουν ελαφρώς διαφορετικά. Το Πρότυπο IOPD επικεντρώνεται στον κίνδυνο και στην αποφυγή ή τον μετριασμό των κινδύνων για τα άτομα. Το πρότυπο IOPD ενσωματώνει αυτή την έννοια στο πρότυπο απαιτώντας ένα καθορισμένο μοντέλο κινδύνου από την αρχή, το οποίο επιτρέπει στον οργανισμό να αξιολογεί με συνέπεια τον κίνδυνο σε όλα τα διαφορετικά συστήματα. Το μοντέλο κινδύνου πρέπει να προσδιορίζει τις απειλές, τις ευπάθειες, τις δυσμενείς συνέπειες για τους ανθρώπους και τα ποσοτικά ή ποιοτικά μέσα μέτρησης της πιθανότητας και της σοβαρότητας αυτών των συνεπειών. Η μέτρηση είναι καθοριστικής σημασίας, διότι οι οργανισμοί πρέπει επίσης να καθορίσουν την ανοχή τους σε κινδύνους και τη διάθεσή τους να συγκρίνουν εάν ο κίνδυνος υπερβαίνει την ανοχή αυτή. Αν και το πρότυπο ISO απαιτεί τη διοίκηση του κινδύνου παραβίασης ιδιωτικότητας, συμπεριλαμβανομένης της διενέργειας αξιολογήσεων κινδύνου, η εν λόγω απαίτηση είναι ασαφής και σχετίζεται με τον ορισμό της ("επίδραση της αβεβαιότητας στην ιδιωτικότητα"). Σε αντίθεση με τις παραπάνω συζητήσεις, το πρότυπο IOPD μπορεί να υποστηρίξει το πρότυπο ISO παρέχοντας μια συγκεκριμένη προσέγγιση, απαιτώντας πρώτα ένα μοντέλο κινδύνου, στη συνέχεια μια αξιολόγηση κινδύνου (πλαισίωση παραγόντων από το μοντέλο, ανάδειξη ζητημάτων, αξιολόγηση του κινδύνου) και, τέλος, αντιμετώπιση του κινδύνου μέσω του σχεδιασμού του συστήματος.

Η διαφορά των δύο προτύπων αντικατοπτρίζει το πού χρησιμοποιούνται κυρίως στον κύκλο ζωής ανάπτυξης λογισμικού (SDLC). Το πρότυπο ISO εμφανίζεται κυρίως κατά τη διάρκεια της συλλογής απαιτήσεων και των φάσεων σχεδιασμού. Ενώ το πρότυπο IOPD αποτελεί μια επικάλυψη σε όλες τις φάσεις του κύκλου ζωής: συλλογή απαιτήσεων, σχεδιασμός, κατασκευή, επαλήθευση και παραγωγή.

Αν και ακολουθούν διαφορετικές προσεγγίσεις, τα δύο πρότυπα είναι συμπληρωματικά ως προς τη φύση τους και στοιχεία από το καθένα μπορούν να χρησιμοποιηθούν για την υποστήριξη του άλλου [58].

Παρακάτω παρουσιάζονται διάφορα στοιχεία και κριτήρια σύγκρισης μεταξύ των δύο προτύπων σε μορφή πίνακα:

	ISO 31700-1 (ISO)	Design Process Standard (IOPD)	Notes
Ημερομηνία Υιοθέτησης του Προτύπου	08 Φεβρουαρίου 2023	01 Ιανουαρίου 2023	-
Στόχος	Οργανωτικές λειτουργίες, συμπεριλαμβανομένου του κύκλου ζωής προϊόντος/υπηρεσίας	Κύκλος ζωής προϊόντος/υπηρεσίας	Τα πρότυπα ISO και IOPD είναι συμπληρωματικά σχετικά με αυτό, με στοιχεία του προτύπου ISO να είναι χρήσιμα ως πειστήρια στοιχεία για την τήρηση του προτύπου IOPD.
Πρότυπο συμμόρφωσης	Όχι	Ναι	Το Πρότυπο IOPD προορίζεται για τις εταιρείες προς πιστοποίηση και το Πρότυπο ISO δεν περιλαμβάνει πειστήρια και κριτήρια αξιολόγησης.
Άτομο ενδιαφέροντος	Καταναλωτές	Καταναλωτές, εργαζόμενοι, υποψήφιοι πελάτες, παρευρισκόμενοι,	Το Πρότυπο IOPD αφορά ένα ευρύτερο σύνολο ατόμων σε

		υποκείμενα των δεδομένων και οποιοδήποτε άλλο άτομο τίθεται σε κίνδυνο μέσω του προϊόντος/υπηρεσίας.	κίνδυνο (at-risk individuals).
Εφαρμοσιμότητα	Business to Consumer (B2C)	Business to Consumer, Government, Non-Profit, and others	Το Πρότυπο IOPD είναι ευρύτερο στις ισχύουσες αγορές.
Πεδίο Εφαρμογής	Καταναλωτικά αγαθά και υπηρεσίες που επεξεργάζονται ΔΠΧ	Όλα τα προϊόντα, οι υπηρεσίες και οι επιχειρηματικές διαδικασίες που επηρεάζουν την ιδιωτικότητα ενός ατόμου	Το Πρότυπο IOPD έχει ευρύτερο πεδίο εφαρμογής.
Μοντέλο ιδιωτικότητας	Επεξεργασία ΔΠΧ	Περιλαμβάνει πληροφοριακή, σωματική, προσωπική αυτονομία και ιδιωτικότητα φυσικού χώρου	Το πρότυπο ISO περιορίζεται μόνο στην επεξεργασία ΔΠΧ
Λογοδοσία	Φυσικό πρόσωπο που λογοδοτεί	Λογοδοσία μέσω διακυβέρνησης	Τα πρότυπα ISO και IOPD είναι συμπληρωματικά σε αυτό, με το πρότυπο ISO που χρησιμοποιείται ως πειστήριο για την τήρηση του προτύπου IOPD.
Κίνδυνος	Απαιτεί διαχείριση κινδύνου	Καθορίζει μια προσέγγιση διαχείρισης κινδύνου	Τα δύο πρότυπα είναι συμπληρωματικά σε αυτό, με το Πρότυπο IOPD να χρησιμοποιείται ως

			πειστήριο για την απαίτηση διαχείρισης κινδύνου του προτύπου ISO.

Βιβλιογραφία

[1] "ISO 31700-1:2023 - Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements." https://www.iso.org/standard/84977.html (accessed Dec. 29, 2023).

[2] D. P. and P. Commissioners and Data Protection and Privacy Commissioners, "International Conference on Data Protection and Privacy Commisioners (32nd October 2010) Resolution on Privacy by Design," *Icdppc*, pp. 1–2, 2010, Accessed: Dec. 28, 2023. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

[3] "EDPS Preliminary Opinion on Privacy by Design | European Data Protection Supervisor." https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en (accessed Dec. 28, 2023).

[4] "Privacy By Design, The 7 Foundational Principles," 2011, [Online]. Available: https://ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[5] "The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices," [Online]. Available: https://ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[6] "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default | European Data Protection Board." https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-42019-article-25-data-protection_en (accessed Dec. 28, 2023).

[7] "ISO 26000:2010 - Guidance on social responsibility." https://www.iso.org/standard/42546.html (accessed Dec. 28, 2023).

[8] "ISO/IEC 29151:2017 - Information technology — Security techniques — Code of practice for personally identifiable information protection." https://www.iso.org/standard/62726.html (accessed Dec. 28, 2023).

[9] "Data Protection and Privacy Legislation Worldwide | UNCTAD." https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed Dec. 28, 2023).

[10] "THE OECD PRIVACY FRAMEWORK 2013," 2013.

[11] "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da."

[12] “APEC Privacy Framework (2015) | APEC.” https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015) (accessed Dec. 28, 2023).

[13] “ISO/IEC 29100:2011 - Information technology — Security techniques — Privacy framework.” https://www.iso.org/standard/45123.html (accessed Dec. 28, 2023).

[14] “ISO/IEC 15944-8:2012 - Information technology — Business operational view — Part 8: Identification of privacy protection requirements as external constraints on business transactions.” https://www.iso.org/standard/51544.html (accessed Dec. 28, 2023).

[15] “Business and organizational privacy policy resources - CPA Canada.” https://www.cpacanada.ca/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/business-and-organizational-privacy-policy-resources (accessed Dec. 28, 2023).

[16] “ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.” https://www.iso.org/standard/71670.html (accessed Dec. 29, 2023).

[17] “NIST PRIVACY FRAMEWORK. A TOOL FOR IMPROVING PRIVACY THROUGH ENTRERPRISE RISK MANAGEMENT, VERSION 1.0 January 16, 2020.”

[18] “ISO/IEC 29184:2020 - Information technology — Online privacy notices and consent.” https://www.iso.org/standard/70331.html (accessed Dec. 28, 2023).

[19] “ISO/IEC 27555:2021 - Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion.” https://www.iso.org/standard/71673.html (accessed Dec. 29, 2023).

[20] “ISO 22458:2022 - Consumer vulnerability — Requirements and guidelines for the design and delivery of inclusive service.” https://www.iso.org/standard/73261.html (accessed Dec. 28, 2023).

[21] “ISO/IEC Guide 76:2020 - Development of service standards — Recommendations for addressing consumer issues.” https://www.iso.org/standard/73717.html (accessed Dec. 28, 2023).

[22] “IoT Devices Should Deal with Privacy Impacts for People with Disabilities - Future of Privacy Forum,” *https://fpf.org/*, doi: 10.0/OTBANNERSDK.JS.

[23] “ISO/IEC 27556:2022 - Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework.” https://www.iso.org/standard/71674.html (accessed Dec. 28, 2023).

[24] “Privacy Management Reference Model and Methodology (PMRM) Version 1.0.” https://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html (accessed Dec. 28, 2023).

[25] “ISO/TR 31700-2:2023 - Consumer protection — Privacy by design for consumer goods and services — Part 2: Use cases.” https://www.iso.org/standard/84978.html (accessed Dec. 28, 2023).

[26] “IEC 62559-2:2015 | IEC Webstore.” https://webstore.iec.ch/publication/22349 (accessed Dec. 28, 2023).

[27] “ISO 30401:2018 - Knowledge management systems — Requirements.” https://www.iso.org/standard/68683.html (accessed Dec. 28, 2023).

[28] “ISO 9001:2015 - Quality management systems — Requirements.” https://www.iso.org/standard/62085.html (accessed Dec. 28, 2023).

[29] “ISO/IEC/IEEE 15288:2015 - Systems and software engineering — System life cycle processes.” https://www.iso.org/standard/63711.html (accessed Dec. 28, 2023).

[30] “OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC | OASIS.” https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se (accessed Dec. 28, 2023).

[31] “Van Der Nagle E., Arnold M., Nansen B., Gibbs M., Kohn T., Bellamy C. Death and the Internet: Consumer issues for planning and managing digital legacies. Australian Communications Consumer Action Network, Sydney, Second Edition, 2017.”

[32] “IEC/IEEE 82079-1:2019 - Preparation of information for use (instructions for use) of products — Part 1: Principles and general requirements.” https://www.iso.org/standard/71620.html (accessed Dec. 28, 2023).

[33] “ISO COPOLCO. 2016, Identification of current consumer issues in privacy and protection of personal data - Document N211/2016 Annex 1.”

[34] “ANEC Consumer Representatives Guidance ‘Domestic privacy and the privacy of digitally connected devices’ - ANEC: The European consumer voice in standardisation.” https://www.anec.eu/publications/other-publications/588-anec-consumer-representatives-guidance-domestic-privacy-and-the-privacy-of-digitally-connected-devices (accessed Dec. 28, 2023).

[35] “Securing consumer trust in the Internet of Things. Principles & recommendations 2017’ ANEC, BEUC, CI, ICRT.”

[36] “ISO/IEC 27035-2:2023 - Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response.” https://www.iso.org/standard/78974.html (accessed Dec. 28, 2023).

[37] “ISO/IEC 27035-1:2023 - Information technology — Information security incident management — Part 1: Principles and process.” https://www.iso.org/standard/78973.html (accessed Dec. 28, 2023).

[38] “ISO - ISO 31000 — Risk management.” https://www.iso.org/iso-31000-risk-

management.html (accessed Dec. 28, 2023).

[39] “ISO/IEC 27557:2022 - Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management.” https://www.iso.org/standard/71675.html (accessed Dec. 28, 2023).

[40] “Resources | NIST.” https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources (accessed Dec. 28, 2023).

[41] “Title: Privacy Risk Management for Federal Information Systems,” 2017, doi: 10.6028/NIST.IR.8062.

[42] “ISO/IEC 29134:2017 - Information technology — Security techniques — Guidelines for privacy impact assessment.” https://www.iso.org/standard/62289.html (accessed Dec. 28, 2023).

[43] R. M. Blank and P. D. Gallagher, “Guide for Conducting Risk Assessments,” Sep. 2012, doi: 10.6028/NIST.SP.800-30R1.

[44] “linddun.org | Privacy Engineering.” https://linddun.org/ (accessed Dec. 28, 2023).

[45] “SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC.” https://csrc.nist.gov/pubs/sp/800/30/r1/final (accessed Dec. 28, 2023).

[46] “ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes.” https://www.iso.org/standard/50053.html (accessed Dec. 28, 2023).

[47] J. Task Force, “NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations JOINT TASK FORCE,” doi: 10.6028/NIST.SP.800-53r5.

[48] “ISO/IEC 20000-1:2018 - Information technology — Service management — Part 1: Service management system requirements.” https://www.iso.org/standard/70636.html (accessed Dec. 29, 2023).

[49] “ISO 10377:2013 - Consumer product safety — Guidelines for suppliers.” https://www.iso.org/standard/45967.html (accessed Dec. 29, 2023).

[50] “ISO/IEC 20889:2018 - Privacy enhancing data de-identification terminology and classification of techniques.” https://www.iso.org/standard/69373.html (accessed Dec. 28, 2023).

[51] “ISO/IEC TS 27570:2021 - Privacy protection — Privacy guidelines for smart cities.” https://www.iso.org/standard/71678.html (accessed Dec. 28, 2023).

[52] “ISO COPOLCO 39th meeting - An outline description of the proposed new standard for privacy by design of consumer goods and services, April 2017 - Annex B of Document N283.”

[53] A. Cavoukian, “Operationalizing Privacy by Design: A Guide to Implementing Strong

Privacy Practices," 2012, Accessed: Dec. 29, 2023. [Online]. Available: www.privacybydesign.ca.

[54] "ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks." https://www.iso.org/standard/80585.html (accessed Dec. 29, 2023).

[55] "ISO/IEC 29180:2012 - Information technology — Telecommunications and information exchange between systems — Security framework for ubiquitous sensor networks." https://www.iso.org/standard/45259.html (accessed Dec. 29, 2023).

[56] A. R. Regenscheid, L. Feldman, and G. A. Witte, "NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization." 2015, Accessed: Dec. 29, 2023. [Online]. Available: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization.

[57] "Institute of Operational Privacy Design Design Process Standard."

[58] "Privacy by Design Standards: ISO v IOPD Compare and Contrast – Institute of Operational Privacy Design." https://instituteofprivacydesign.org/2023/05/08/privacy-by-design-standards-iso-v-iopd-compare-and-contrast/ (accessed Jan. 07, 2024).