



The byRisk project is funded by the Citizens, Equality, Rights and Values Programme (CERV) of the European Union under grant agreement No. 101193352.



“Κατανόηση Κινδύνων Ιδιωτικότητας”



Πριν ξεκινήσουμε μερικά διαχειριστικά θέματα...

- Κατά τη διάρκεια της παρουσίασης τα μικρόφωνα σας θα είναι απενεργοποιημένα για να αποφύγουμε πιθανούς θορύβους. Παρ' όλα αυτά σε τακτά χρονικά διαστήματα ο ομιλητής θα δίνει τη δυνατότητα να κάνετε ερωτήσεις ανοίγοντας το μικρόφωνο σας.
- Μετά το τέλος του σεμιναρίου θα λάβετε ένα email με ένα σύνδεσμο (link) για ένα πολύ σύντομο (ανώνυμο) ερωτηματολόγιο αξιολόγησης.
- Οι διαφάνειες καθώς και ο τρόπος πρόσβασης στο εργαλείο που θα σας παρουσιάσουμε θα είναι (σύντομα) διαθέσιμα μέσω του web site της Αρχής καθώς και του web site του έργου (<https://byrisk-project.eu/>).
- Οι βεβαιώσεις παρακολούθησης θα σας αποσταλούν με email τις επόμενες μέρες.

A. *Τί είναι η προστασία των δεδομένων;*

Η προστασία των προσωπικών δεδομένων αφορά την νόμιμη και ορθή χρήση των πληροφοριών που αφορούν συγκεκριμένα πρόσωπα.

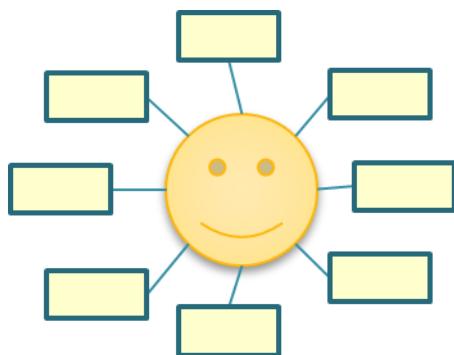
Στενά συνυφασμένα με το **θεμελιώδες δικαίωμα της ιδιωτικότητας** – αλλά δεν ταυτίζονται.

Ουσιαστικά πρόκειται για την οικοδόμηση εμπιστοσύνης ανάμεσα στους ανθρώπους και τους οργανισμούς. Πρόκειται για τη δίκαιη και διαφανή αντιμετώπιση των ανθρώπων, αναγνωρίζοντας το δικαίωμά τους να έχουν τον έλεγχο της ταυτότητάς τους και της συναναστροφής τους με άλλους και την επίτευξη ισορροπίας με τα ευρύτερα συμφέροντα της κοινωνίας. Επίσης, αφορά την απομάκρυνση μη απαραίτητων εμποδίων στο εμπόριο και τη συνεργασία. Υπάρχει εν μέρει εξαιτίας διεθνών συμφωνιών για κοινά πρότυπα τα οποία επιτρέπουν την ελεύθερη ροή των δεδομένων μεταξύ των συνόρων.

Η προστασία των δεδομένων είναι απαραίτητη για την καινοτομία. Οι καλές πρακτικές προστασίας δεδομένων είναι απαραίτητες για τη διασφάλιση της εμπιστοσύνης, και της υποστήριξης καινοτόμων τρόπων χρήσης των δεδομένων στον δημόσιο και ιδιωτικό τομέα.

Το ελληνικό καθεστώς προστασίας δεδομένων είναι καθορισμένο στον νόμο 4624/2019 και τον GDPR.

Προσωπικά Δεδομένα

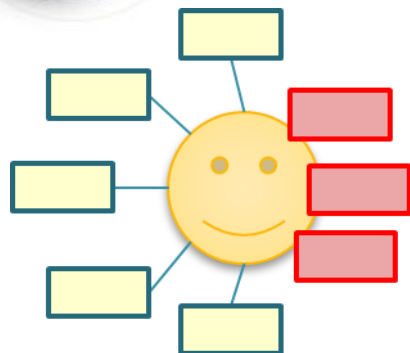


Π.χ. προσωπικά δεδομένα: όνομα και επώνυμο, αριθμός ταυτότητας, διεύθυνση κατοικίας, ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com, αναγνωριστικός αριθμός κάρτας, δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο), διεύθυνση δικτύου συσκευής χρήστη (IP address), ένα cookie ID, διαφημιστικό αναγνωριστικό του τηλεφώνου, δεδομένα που κατέχονται από ένα νοσοκομείο ή γιατρό, τα οποία μπορούν να είναι ένα σύμβολο για τη μοναδική αναγνώριση ενός ανθρώπου.

Π.χ. όχι προσωπικά δεδομένα: ο αριθμός εγγραφής μιας εταιρίας, μία διεύθυνση email όπως πληροφορίες@εταιρία.com, ανωνυμοποιημένα δεδομένα.

Προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία σχετικά με ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Ένα ταυτοποιήσιμο φυσικό πρόσωπο είναι όποιος μπορεί να ταυτοποιηθεί άμεσα ή έμμεσα, ιδίως με αναφορά σε αναγνωριστικά όπως όνομα, αριθμός ταυτότητας, δεδομένα τοποθεσίας, διαδικτυακά αναγνωριστικά ή από έναν ή περισσότερους παράγοντες συγκεκριμένα στη φυσική, ψυχολογική, γενετική, νοητική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα ενός φυσικού προσώπου.

Ειδικές Κατηγορίες Δεδομένων



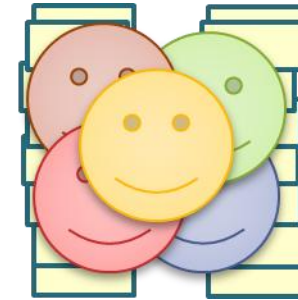
Τα δεδομένα αυτά αποκαλύπτουν: φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, ή συμμετοχή σε συνδικαλιστική οργάνωση και η επεξεργασία γενετικών και βιομετρικών δεδομένων με σκοπό τη μοναδική ταυτοποίηση του φυσικού προσώπου, δεδομένα που αφορούν την υγεία ή δεδομένα σχετικά με τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό ενός φυσικού προσώπου.

- «**γενετικά δεδομένα**»: Είναι δεδομένα σχετικά με κληρονομικά ή επίκτητα γενετικά χαρακτηριστικά ενός φυσικού προσώπου τα οποία έχουν μοναδικές πληροφορίες σχετικά με τη φυσιολογία ή την υγεία αυτού του φυσικού προσώπου και προκύπτουν από την ανάλυση βιολογικών δειγμάτων του.
- «**βιομετρικά δεδομένα**»: Είναι δεδομένα που προκύπτουν από συγκεκριμένη επεξεργασία σχετικά με φυσικά, ψυχολογικά και συμπεριφορικά χαρακτηριστικά ενός φυσικού προσώπου το οποίο επιτρέπει ή επιβεβαιώνει τη μοναδική ταυτοποίηση του
 - Π.χ. Εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα
- «**δεδομένα υγείας**»: Είναι δεδομένα σχετικά με τη φυσική ή ψυχολογική υγεία ενός φυσικού προσώπου
- Ξεχωριστή «ειδική» κατηγορία: **ποινικές καταδίκες και αδικήματα.**

Τί σημαίνει η 'επεξεργασία' ;

Σχεδόν τα πάντα που κάνετε με τα δεδομένα θεωρείται επεξεργασία!

- συλλογή,
- καταχώριση,
- οργάνωση,
- διάρθρωση,
- αποθήκευση,
- προσαρμογή ή μεταβολή,
- ανάκτηση,
- διαβούλευση,
- χρήση,
- γνωστοποίηση μέσω διαβίβασης ,
- διάδοση ή διάθεση με άλλο τρόπο,
- συσχέτιση ή συνδυασμός,
- περιορισμός,
- διαγραφή ή καταστροφή



Υποκείμενο των Δεδομένων



‘προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία σχετικά με **ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ...**’

Αυτός είναι ο τεχνικός όρος για ένα φυσικό πρόσωπο τον οποίο αφορούν τα συγκεκριμένα δεδομένα

Για παράδειγμα, όταν σερφάρουμε στο Διαδίκτυο, όταν αγοράζουμε κάτι, όταν χρησιμοποιούμε μία έξυπνη εφαρμογή κτλ. ουσιαστικά «διαθέτουμε» προσωπικά μας δεδομένα και, άρα, είμαστε υποκείμενα των δεδομένων για την εκάστοτε επεξεργασία

Τί είναι **identifiers** και **related** παράγοντες;

Ένα φυσικό πρόσωπο είναι ‘ταυτοποιημένο’ ή ‘ταυτοποιήσιμο’ εάν μπορείτε να το διακρίνετε από άλλα φυσικά πρόσωπα.

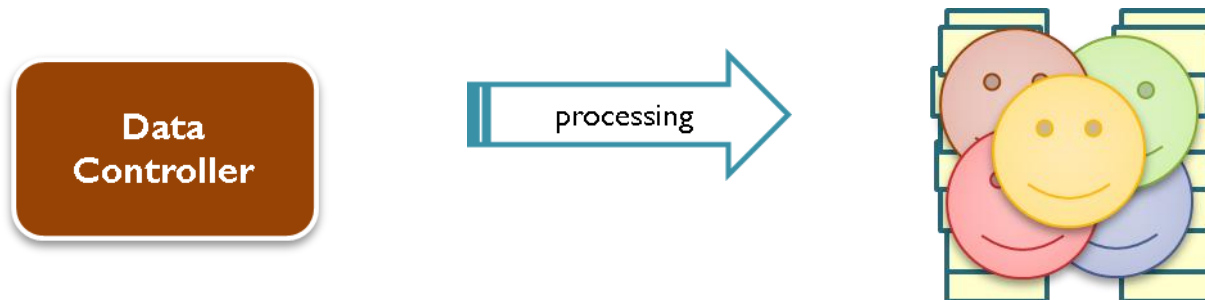
Το **όνομα** είναι ίσως το πιο κοινό μέσο αναγνώρισης κάποιου.

Ωστόσο, το εάν κάποιο identifier μπορεί να αναγνωρίσει ένα φυσικό πρόσωπο εξαρτάται από το πλαίσιο.

Ένας συνδυασμός από identifiers ίσως χρειαστούν για την αναγνώριση ενός φυσικού προσώπου.

***** Ο GDPR παρέχει μία μη – εξαντλητική λίστα από identifiers, περιλαμβανόμενων του: ονόματος, αριθμού ταυτοποίησης, δεδομένων τοποθεσίας και διαδικτυακών αναγνωριστικών. Τα διαδικτυακά αναγνωριστικά περιλαμβάνουν IP διευθύνσεις και αναγνωριστικά cookies τα οποία ίσως είναι προσωπικά δεδομένα. Και άλλοι παράγοντες μπορούν να ταυτοποιήσουν ένα φυσικό πρόσωπο.**

Υπεύθυνος Επεξεργασίας



Είναι οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που μόνα ή από κοινού με άλλα καθορίζουν **τους σκοπούς και τα μέσα** της επεξεργασίας δεδομένων προσωπικού χαρακτήρα

ΠΡΟΣΟΧΗ!: όπου οι σκοποί και τα μέσα της επεξεργασίας αυτής καθορίζονται από νόμο της Ένωσης ή του Κράτους μέλους , ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το νόμο αυτό.

Τί είναι ονομαστικά ένας ‘υπεύθυνος επεξεργασίας’;



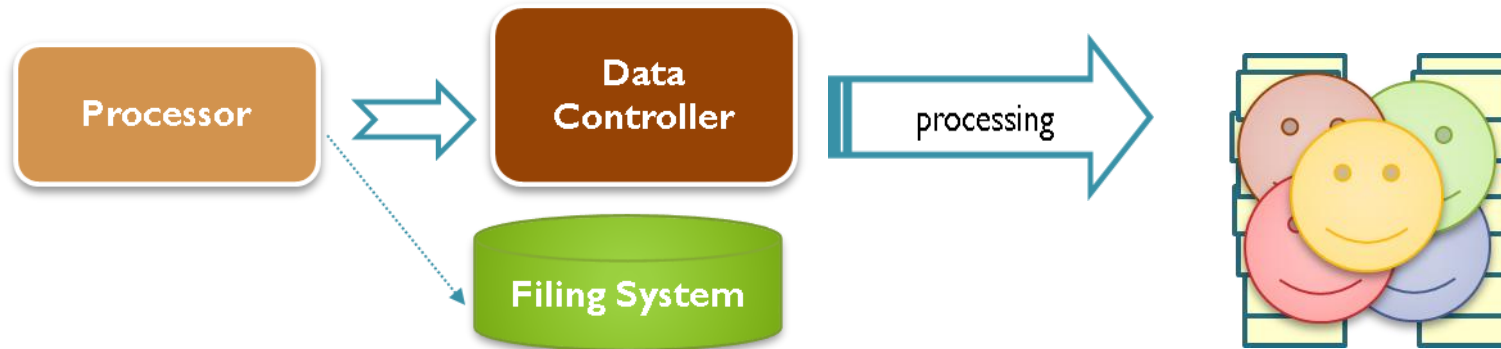
Ο υπεύθυνος επεξεργασίας είναι αυτός ο οποίος **αποφασίζει πώς και γιατί να συλλεχθούν και να χρησιμοποιηθούν τα δεδομένα**. Αυτό συνήθως είναι ένας οργανισμός, αλλά μπορεί να είναι και ένα φυσικό πρόσωπο (π.χ. ένας έμπορος, ένας γιατρός, ένας δικηγόρος κλπ.).

Για παράδειγμα: οι πάροχοι των ιστοσελίδων που επισκεπτόμαστε, τα (ηλεκτρονικά) καταστήματα από τα οποία αγοράζουμε, οι πάροχοι των εφαρμογών που χρησιμοποιούμε κτλ. είναι υπεύθυνοι επεξεργασίας.

Εάν είστε ένας υπάλληλος που εκπροσωπείτε έναν εργοδότη, τότε ο εργοδότης είναι ο υπεύθυνος επεξεργασίας.

Ο υπεύθυνος επεξεργασίας πρέπει να βεβαιωθεί ότι η επεξεργασία των δεδομένων είναι σύμφωνη με τους νόμους προστασίας δεδομένων.

Ο Εκτελών την Επεξεργασία



“ ένα φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας ο οποίος επεξεργάζεται τα προσωπικά δεδομένα εκ μέρους του υπεύθυνου επεξεργασίας”... και σύμφωνα με τις οδηγίες του.

*****ΔΕΝ είναι υπάλληλος!!!**

***Ο Εκτελών την επεξεργασία έχει μερικές νομικές υποχρεώσεις αλλά είναι περιορισμένες σε σχέση με του υπευθύνου επεξεργασίας

- ✓ Μία συνηθισμένη περίπτωση εκτελούντος την επεξεργασία είναι οι «υπεργολάβοι» που επεξεργάζονται προσωπικά δεδομένα.
- ✓ Στον δημόσιο τομέα, οι εκτελούντες την επεξεργασία είναι συνήθως άλλες δημόσιες αρχές π.χ. Taxisnet, G-Cloud, IDIKA.

Β. Αρχές Προστασίας Δεδομένων



Νομιμότητα, Αντικειμενικότητα και Διαφάνεια

Υποβάλλονται σε σύννομη, θεμιτή και διαφανή επεξεργασία σε σχέση με το υποκείμενο των δεδομένων

Περιορισμός του Σκοπού

Συλλέχτηκαν για συγκεκριμένους, ρητούς και νόμιμους λόγους και δεν θα υποστούν περαιτέρω επεξεργασία με τρόπους μη συμβατούς με αυτούς τους σκοπούς

Ελαχιστοποίηση των Δεδομένων

Επαρκής, σχετική και περιορισμένη η συλλογή των δεδομένων σε ότι είναι απαραίτητο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

Ακρίβεια

Ακριβή και όπου είναι απαραίτητο, να επικαιροποιούνται

Περιορισμός της Περιόδου Αποθήκευσης

Κρατούνται σε μορφή η οποία δεν επιτρέπει την αναγνώριση των υποκειμένων των δεδομένων περισσότερο από όσο είναι απαραίτητο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

Ακεραιότητα και Εμπιστευτικότητα

Υφίστανται επεξεργασία κατά τρόπο που διασφαλίζει την απαραίτητη ασφάλεια των προσωπικών δεδομένων χρησιμοποιώντας κατάλληλα τεχνικά και οργανωτικά μέτρα.

Λογοδοσία!

Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με τις προαναφερθείσες αρχές.

ι. Νομιμότητα, Αντικειμενικότητα και Διαφάνεια

‘Υποβάλλονται σε σύννομη, θεμιτή και διαφανή επεξεργασία σε σχέση με το υποκείμενο των δεδομένων’

Θεμιτή σημαίνει διαφανή διαδικασία, ειδικά όταν σχετίζεται με τα υποκείμενα των δεδομένων. Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει τα υποκείμενα των δεδομένων πριν την έναρξη της επεξεργασίας, τουλάχιστον για τον σκοπό της, το όνομα και την διεύθυνση του.

Τα υποκείμενα των δεδομένων έχουν δικαίωμα πρόσβασης στα δεδομένα τους σε κάθε περίπτωση.

Πέρα από τα προφανή, αυτή η αρχή στοχεύει στην οικοδόμηση εμπιστοσύνης ανάμεσα στον υπεύθυνο επεξεργασίας και τα υποκείμενα των δεδομένων!

ii. Περιορισμός του Σκοπού

‘Συλλέχτηκαν για συγκεκριμένους, ρητούς και νόμιμους λόγους και δεν θα υποστούν περαιτέρω επεξεργασία με τρόπους μη συμβατούς με αυτούς τους σκοπούς’

- περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνα ή στατιστικούς σκοπούς σύμφωνα με το άρθρο 89(1) δε θεωρούνται μη συμβατοί με τους αρχικούς σκοπούς

Ο σκοπός της επεξεργασίας πρέπει να είναι σαφώς καθορισμένος *πριν* την έναρξη της επεξεργασίας.

Η νομιμότητα της επεξεργασίας είναι στενά συνδεδεμένη με τον σκοπό της.

Επεξεργασία χωρίς ξεκάθαρους σκοπούς είναι παράνομη!

Περαιτέρω χρήση των δεδομένων για νέο σκοπό χρειάζεται νέα νομική βάση, εάν ο σκοπός δεν είναι συμβατός με τον αρχικό.

- *π.χ.: μεταφορά σε τρίτους είναι ένας νέος σκοπός και νέα νομική βάση είναι απαραίτητη!*

Η περαιτέρω χρήση για σκοπούς συμβατούς με τον αρχικό είναι νόμιμη και δεν χρειάζεται νέα νομική βάση.

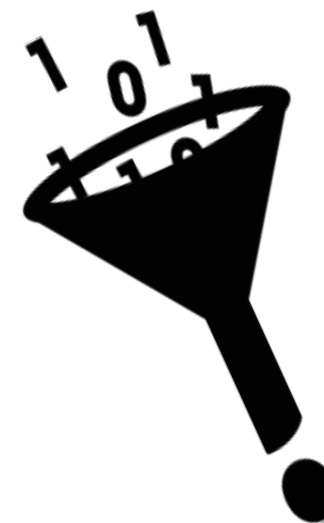
iii. Ελαχιστοποίηση των Δεδομένων

‘Επαρκής, σχετική και περιορισμένη η συλλογή των δεδομένων σε ότι είναι απαραίτητο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία’

Οι κατηγορίες δεδομένων που επιλέγονται για την επεξεργασία πρέπει να είναι σχετικές και απαραίτητες για την ικανοποίηση του σκοπού της επεξεργασίας.

Ο υπεύθυνος επεξεργασίας πρέπει να περιορίζει αυστηρά τη συλλογή των δεδομένων σε αυτά που είναι άμεσα συνδεδεμένα με τον συγκεκριμένο σκοπό επεξεργασίας.

Ιδιωτικότητα – προσιτές λύσεις θα πρέπει να επιλέγονται με τη χρήση νέων τεχνολογιών π.χ. μη χρήση προσωπικών στοιχείων, ψευδωνυμοποίηση.



iv. Ακρίβεια

*‘Ακριβή και όπου είναι απαραίτητο, να επικαιροποιούνται’
Πρέπει να γίνεται κάθε προσπάθεια ώστε να διασφαλιστεί ότι τα προσωπικά δεδομένα που είναι ανακριβή, διαγράφονται ή διορθώνονται χωρίς καθυστέρηση.*

Ο υπεύθυνος επεξεργασίας δεν πρέπει να χρησιμοποιεί δεδομένα χωρίς να παίρνει μέτρα για να διασφαλίσει ότι είναι ακριβή και ενημερωμένα.

Υπάρχουν περιπτώσεις όπου τα δεδομένα πρέπει να ενημερωθούν έτσι ώστε να αποφευχθεί βλάβη στα υποκείμενα των δεδομένων

Π.χ. Προκειμένου τα τραπεζικά ιδρύματα να ελέγχουν την φερεγγυότητα των πελατών τους, τα δεδομένα στα οποία θα βασίζονται πρέπει να είναι ακριβή και επικαιροποιημένα.



ν. Περιορισμός της Περιόδου Αποθήκευσης

‘Κρατούνται σε μορφή η οποία δεν επιτρέπει την αναγνώριση των υποκειμένων των δεδομένων περισσότερο από όσο είναι απαραίτητο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία’

***τα προσωπικά δεδομένα ίσως αποθηκευτούν για μεγαλύτερες χρονικές περιόδους στον βαθμό που αυτά θα υποστούν επεξεργασία για να επιτευχθούν σκοποί προς το δημόσιο συμφέρον, σκοποί για επιστημονική ή ιστορική έρευνα ή στατιστικοί σκοποί και υπάρχουν μέτρα ασφαλείας για τη διασφάλιση της προστασίας των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων.

Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται πέρα από τον σκοπό και για τη διάρκεια αποθήκευσης των προσωπικών τους δεδομένων.

Όταν αυτή η περίοδος τελειώσει, η επεξεργασία ίσως συνεχιστεί για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικών.

***Στον δημόσιο τομέα αυτή η περίοδος είναι καθορισμένη από τον νόμο.



νι. Ακεραιότητα και Εμπιστευτικότητα



The byRisk project is funded by the Citizens, Equality, Rights and Values Programme (CERV) of the European Union under grant agreement No. 101193352.

Ύφίστανται επεξεργασία κατά τρόπο που διασφαλίζει την απαραίτητη ασφάλεια των προσωπικών δεδομένων, περιλαμβάνοντας την προστασία ενάντια σε **μη εξουσιοδοτημένη** ή **παράνομη** επεξεργασία και ενάντια σε **τυχαία απώλεια, καταστροφή ή φθορά χρησιμοποιώντας κατάλληλα τεχνικά και οργανωτικά μέτρα!**

Ο υπεύθυνος επεξεργασίας έχει ως υποχρέωση να παίρνει τα κατάλληλα μέτρα ενάντια σε μη εξουσιοδοτημένη επεξεργασία.

Το επιτρεπτό επίπεδο ασφάλειας καθορίζεται από:

- Την τελευταία λέξη της τεχνολογίας όσον αφορά τα μέτρα ασφάλειας

- Το κόστος εφαρμογής των μέτρων αυτών και

- Το επίπεδο 'ευαισθησίας' των δεδομένων που επεξεργάζονται.

Η προσθήκη δικλίδων ασφαλείας είναι ένα γενικό καθήκον όλων όσων ασχολούνται με την επεξεργασία (υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία) για τη διασφάλιση ιδιωτικότητας.

vii. Λογοδοσία



Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με τις προαναφερθείσες αρχές.

Σύμφωνα με την ΟΕ του άρθρου 29, στον πυρήνα της λογοδοσίας βρίσκεται η υποχρέωση του υπεύθυνου επεξεργασίας να:

Διασφαλίζει την επιβολή μέτρων για την προστασία των δεδομένων.

Να έχει τα απαραίτητα έγγραφα για να αποδεικνύει και να επιδεικνύει τη συμμόρφωση με τον ΓΚΠΔ στην ΑΠΔΠΧ και προς τα υποκείμενα των δεδομένων.

Ο υπεύθυνος επεξεργασίας πρέπει *ανά πάσα στιγμή* να μπορεί να επιδεικνύει στα υποκείμενα των δεδομένων, σε δημόσιες και σε εποπτικές αρχές, τη συμμόρφωση με τους νόμους προστασίας δεδομένων.

Κ. Νομικές Βάσεις

Πότε η επεξεργασία είναι νόμιμη;

α. συγκατάθεση

Το υποκείμενο των δεδομένων έχει δώσει συγκατάθεση για την επεξεργασία των προσωπικών του/ της δεδομένων για έναν ή περισσότερους σκοπούς.

Προσοχή στον ορισμό της συγκατάθεσης!

β. Εκτέλεση και σύναψη σύμβασης

Η επεξεργασία είναι απαραίτητη:

- η εκτέλεση της σύμβασης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέλος, ή
- για να ληφθούν μέτρα μετά από αίτημα του υποκειμένου των δεδομένων πριν τη σύναψη της σύμβασης.

γ. Νομική υποχρέωση

Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπεύθυνου επεξεργασίας

Πέρα από τον δημόσιο τομέα υπάρχουν περιπτώσεις όπου υπεύθυνοι επεξεργασίας είναι υποχρεωμένοι από το νόμο να επεξεργαστούν δεδομένα. π.χ. γιατροί και νοσοκομεία, εργοδότες, εταιρίες (δεδομένα πελατών για φορολογικούς σκοπούς)

Σ. Νομικές Βάσεις

Πότε η επεξεργασία είναι νόμιμη;

δ. Ζωτικό συμφέρον

Η επεξεργασία είναι απαραίτητη για τα **ζωτικά συμφέροντα** του υποκειμένου των δεδομένων ή κάποιου άλλου φυσικού προσώπου.

ε. Δημόσιο συμφέρον

Η επεξεργασία είναι απαραίτητη για την εκτέλεση μίας εργασίας που πραγματοποιείται:

Για το **δημόσιο συμφέρον** ή

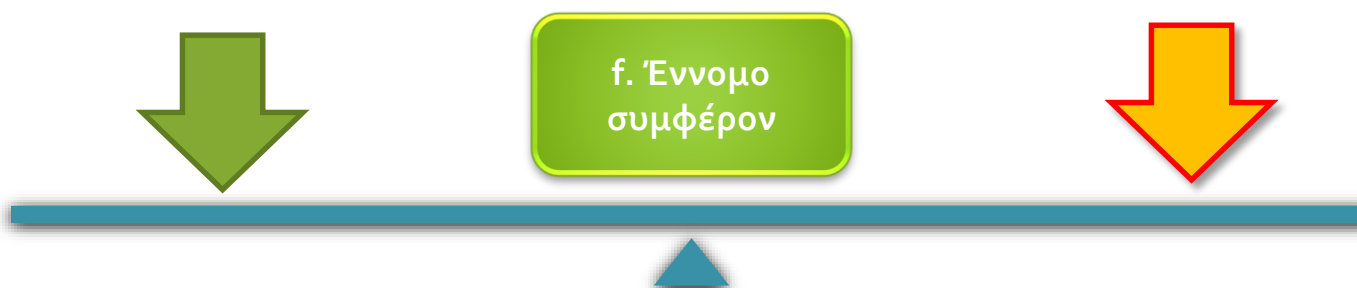
Κατά την άσκηση **δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.**

Κ. Νομικές Βάσεις

Πότε η επεξεργασία είναι νόμιμη;

Η επεξεργασία είναι απαραίτητη:
για τους σκοπούς των **έννομων συμφερόντων** που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος

εκτός εάν έναντι των συμφερόντων αυτών **υπερισχύει το συμφέρον** ή τα **θεμελιώδη δικαιώματα** και οι **ελευθερίες** του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, **ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.**



- ✓ Χρησιμοποιείται συνήθως στον ιδιωτικό τομέα (π.χ. για χρηματοοικονομικούς σκοπούς)
- ✓ Όπου η συγκατάθεση δεν αποτελεί νομική βάση (π.χ. βίντεο παρακολούθηση)

Προσοχή!

Δεν μπορεί να εφαρμοστεί σε επεξεργασία που πραγματοποιείται από **δημόσιες αρχές** κατά την εκτέλεση των καθηκόντων τους.



Πότε και πώς η επεξεργασία **ειδικών κατηγοριών** είναι νόμιμη;



The byRisk project is funded by the Citizens, Equality, Rights and Values Programme (CERV) of the European Union under grant agreement No. 101193352.

Απαγόρευση!

Η επεξεργασία ειδικών κατηγοριών είναι απαγορευμένη.

Υπάρχουν όμως μερικές εξαιρέσεις στον GDPR!

- Επιτρέπεται για παράδειγμα όταν υπάρχει ρητή συγκατάθεση, λόγοι δημόσιου συμφέροντος, ανάγκες υγείας.
- Απαιτείται αυξημένο επίπεδο προστασίας και ασφάλειας κατά την επεξεργασία τους.
- Στόχος είναι η προστασία των πολιτών από διακρίσεις και καταχρηστική χρήση των πιο ευαίσθητων πληροφοριών τους.

D. Τα δικαιώματα των Υποκειμένων των Δεδομένων

- Διαφανής Επικοινωνία, Ενημέρωση και Άσκηση Δικαιωμάτων(άρθ. 12).
- (1) Το Δικαίωμα στην Ενημέρωση (άρθ. 13, 14).
- (2) Το Δικαίωμα στην Πρόσβαση (άρθ. 15).
- (3) Το Δικαίωμα στην Διόρθωση (άρθ. 16).
- (4) Το Δικαίωμα της Διαγραφής / δικαίωμα να «ξεχαστείς» (άρθ. 17).
- (5) Το Δικαίωμα στον Περιορισμό της Επεξεργασίας (άρθ. 18).
- (6) Το Δικαίωμα στην Φορητότητα των Δεδομένων (άρθ. 20)
- (7) Το Δικαίωμα στη Εναντίωση (άρθ. 21).
- (8) Το Δικαίωμα στην μη Αυτοματοποιημένη Λήψη Αποφάσεων περιλαμβανόμενων και της δημιουργίας προφίλ (άρθ. 22).



Ενημέρωση και επικοινωνία πρέπει να παρέχεται στις ακόλουθες περιπτώσεις:

- Πριν / κατά τη διάρκεια της επεξεργασίας,
- Άσκηση των δικαιωμάτων και
- Παραβίαση των δεδομένων.
- Συνοπτική, διαφανής, κατανοητή και εύκολα προσβάσιμη μορφή.
- **Τρόπος ενημέρωσης:** γραπτώς ή με άλλα μέσα, μεταξύ άλλων με ηλεκτρονικά μέσα, όπου είναι εφικτό.
- **Προφορικά, όταν ζητείται από το υποκείμενο των δεδομένων:** υπό την προϋπόθεση ότι η ταυτότητά του υποκειμένου των δεδομένων έχει επικυρωθεί με άλλα μέσα.
- Η ενημέρωση θα πρέπει να παρέχεται **δωρεάν** (μία λογική αμοιβή μπορεί να χρεωθεί εάν το αίτημα είναι αβάσιμο ή υπερβολικό συγκεκριμένα εξαιτίας του επαναληπτικού χαρακτήρα).



- **Προθεσμία του υπεύθυνου επεξεργασίας να παράσχει πληροφορίες:**
 - Χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση μέσα σε **έναν (1) μήνα** από την παραλαβή του αιτήματος.
 - Επέκταση της περιόδου κατά **δύο (2) επιπλέον μήνες** λαμβάνοντας υπόψη την **πολυπλοκότητα** και τον **αριθμό** των αιτημάτων.
 - Τα υποκείμενα των δεδομένων πρέπει σε κάθε περίπτωση να είναι ενήμερα για κάθε χρονική επέκταση και για τους λόγους που αυτή απαιτείται, μέσα σε **ένα (1) μήνα**.
- **Καμία ενέργεια δεν έγινε από τον υπεύθυνο επεξεργασίας:**
 - Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει το υποκείμενο των δεδομένων **χωρίς καθυστέρηση** και **τουλάχιστον μέσα σε έναν (1) μήνα** από την παραλαβή του αιτήματος για:
 - Τους **λόγους** που δεν κάνει καμία ενέργεια και
 - Τη δυνατότητα υποβολής (εκ μέρους του υποκειμένου των δεδομένων) **παραπόνου** σε εποπτική αρχή καθώς και άσκησης ένδικων μέσων

Η έννοια του Κινδύνου

Υπάρχουν δύο κύριες έννοιες διαχείρισης του κινδύνου:

- Η υποκειμενική αντίληψη του κινδύνου.
- Η αντικειμενική / τεχνική αντίληψη του κινδύνου.



Αυτές οι ερμηνείες περιγράφουν διαφορετικούς τρόπους κατανόησης, αξιολόγησης και αντιμετώπισης πιθανών αντικτύπων από απροσδόκητα περιστατικά ασφάλειας.

Υποκειμενική / Τεχνική Ερμηνεία

- Η υποκειμενική ερμηνεία αναφέρεται σε πιθανό μελλοντικό συμβάν ασφάλειας το οποίο μπορεί να προκαλέσει επιβλαβείς συνέπειες (και συνεπώς αποτελεί πιθανό κίνδυνο).
- Η αντικειμενική / τεχνική ερμηνεία υιοθετεί μία διπλή έννοια, δηλαδή την πιθανότητα εμφάνισης ενός πιθανού συμβάντος ασφάλειας σε συνδυασμό με τον αντίκτυπο.
- Επομένως, η διαδικασία αναγνώρισης κινδύνων ακολουθεί τα ακόλουθα κριτήρια:
 - a) Το πιθανό μελλοντικό γεγονός,
 - b) Τον αντίκτυπο που μπορεί να προκαλέσει,
 - c) Πώς μπορεί το γεγονός να υλοποιηθεί.

Η έννοια του Αντίκτυπου

Ο αντίκτυπος μπορεί να κατηγοριοποιηθεί σε:

- Ασήμαντο αντίκτυπο
- Περιορισμένο αντίκτυπο
- Σημαντικό αντίκτυπο
- Μέγιστο αντίκτυπο

υποστηρίζοντας μία συστηματική ανάλυση πιθανών αρνητικών συνεπειών που μπορεί να επηρεάσουν φυσικά άτομα, τεχνολογικές υποδομές και επιχειρησιακές διαδικασίες.

Διαβαθμίσεις του Αντικτύπου

- **Ασήμαντου αντικτύπου:** Λανθασμένη αποστολή ενημερωτικού email χωρίς ευαίσθητα δεδομένα σε μικρό αριθμό παραληπτών, χωρίς κρυφή κοινοποίηση, που προκαλεί απλή ενόχληση χωρίς περαιτέρω συνέπειες.
- **Περιορισμένου αντικτύπου:** Διαρροή στοιχείων επικοινωνίας (όνομα, email) που οδηγεί σε ανεπιθύμητη επικοινωνία ή spam, χωρίς όμως οικονομική ή άλλη σοβαρή βλάβη.
- **Σημαντικού αντικτύπου:** Μη εξουσιοδοτημένη πρόσβαση σε οικονομικά δεδομένα (π.χ. στοιχεία κάρτας), που μπορεί να οδηγήσει σε οικονομική ζημία ή απάτη για το άτομο.
- **Μέγιστου αντικτύπου:** Διαρροή ευαίσθητων δεδομένων (π.χ. υγείας) που οδηγεί σε στιγματισμό, διακρίσεις ή σοβαρή κοινωνική/επαγγελματική βλάβη.

Θεμελιώδη Δικαιώματα

Τα θεμελιώδη δικαιώματα είναι βασικά οικουμενικά δικαιώματα και ελευθερίες που αποκτούνται απλά και μόνο λόγω της ύπαρξης κάθε ατόμου. Θεωρούνται έμφυτα, αναπαλλοτρίωτα, αδιαίρετα, αλληλεξαρτημένα και βασικά για την ανθρώπινη αξιοπρέπεια και αποτελούν τη βάση των δημοκρατικών κοινωνιών και νομικών συστημάτων.

- Στοχεύουν στην προστασία τόσο των ατομικών όσο και των ομαδικών ελευθεριών.
- Οι τύποι τους εκτείνονται σε: Πολιτικούς, οικονομικούς, κοινωνικούς, πολιτιστικούς και ψηφιακούς τομείς.
- Στην ΕΕ τα θεμελιώδη δικαιώματα καλύπτονται από τον Χάρτη των Θεμελιωδών Δικαιωμάτων ενισχύοντας εθνικά νομικά συστήματα.

Χάρτης των Θεμελιωδών Δικαιωμάτων

Ο Χάρτης περιέχει 54 άρθρα ομαδοποιημένα σε 6 κύριες κατηγορίες:

- I. Αξιοπρέπεια, η οποία προστατεύει την έμφυτη αξιοπρέπεια του κάθε ατόμου (και εκ τούτου συνιστά τη βάση των θεμελιωδών δικαιωμάτων) και συνεπώς τη φυσική και ηθική ακεραιότητα.
- II. Ελευθερίες, οι οποίες εστιάζουν στις ατομικές ελευθερίες και στην προσωπική αυτονομία (το δικαίωμα να προστατεύεις την προσωπική και οικογενειακή ζωή σου καθώς και το δικαίωμα στην προστασία προσωπικών δεδομένων).
- III. Ισότητα, η οποία εστιάζει στην ίση μεταχείριση και προστασία ενάντια στις διακρίσεις.
- IV. Αλληλεγγύη, η οποία καλύπτει κοινωνικά και εργατικά δικαιώματα.
- V. Δικαιώματα των πολιτών, τα οποία εστιάζουν στη δημοκρατική συμμετοχή και την διοικητική διαφάνεια.
- VI. Δικαιοσύνη, η οποία διασφαλίζει την πρόσβαση σε δίκαιες νομικές διαδικασίες.

Ταξινόμηση Κινδύνων (byRisk)

Το έργο byRisk ανέπτυξε μία νέα ταξινόμηση κινδύνων η οποία συσχετίζει σε μεγάλο βαθμό τον **Κίνδυνο** με τον **Αντίκτυπο**.

Αυτή η νέα ταξινόμηση προωθεί ένα δομημένο πλαίσιο για την κατηγοριοποίηση και ανάλυση κινδύνων αναφορικά με τις σχετικές συνέπειες για κάθε φυσικό πρόσωπο.

Αυτή η ταξινόμηση αποτελείται από τέσσερα διακριτά επίπεδα:

- Επίπεδο 1: Παραβίαση των Θεμελιωδών Δικαιωμάτων.
- Επίπεδο 2: Επιπτώσεις για φυσικά πρόσωπα.
- Επίπεδο 3: Μη συμμόρφωση με το κανονιστικό πλαίσιο.
- Επίπεδο 4: Πηγές Κινδύνων.

Ταξινόμηση Κινδύνων (byRisk)

Επίπεδο 1: Παραβίαση των Θεμελιωδών Δικαιωμάτων



Επίπεδο 2: Επιπτώσεις για φυσικά πρόσωπα



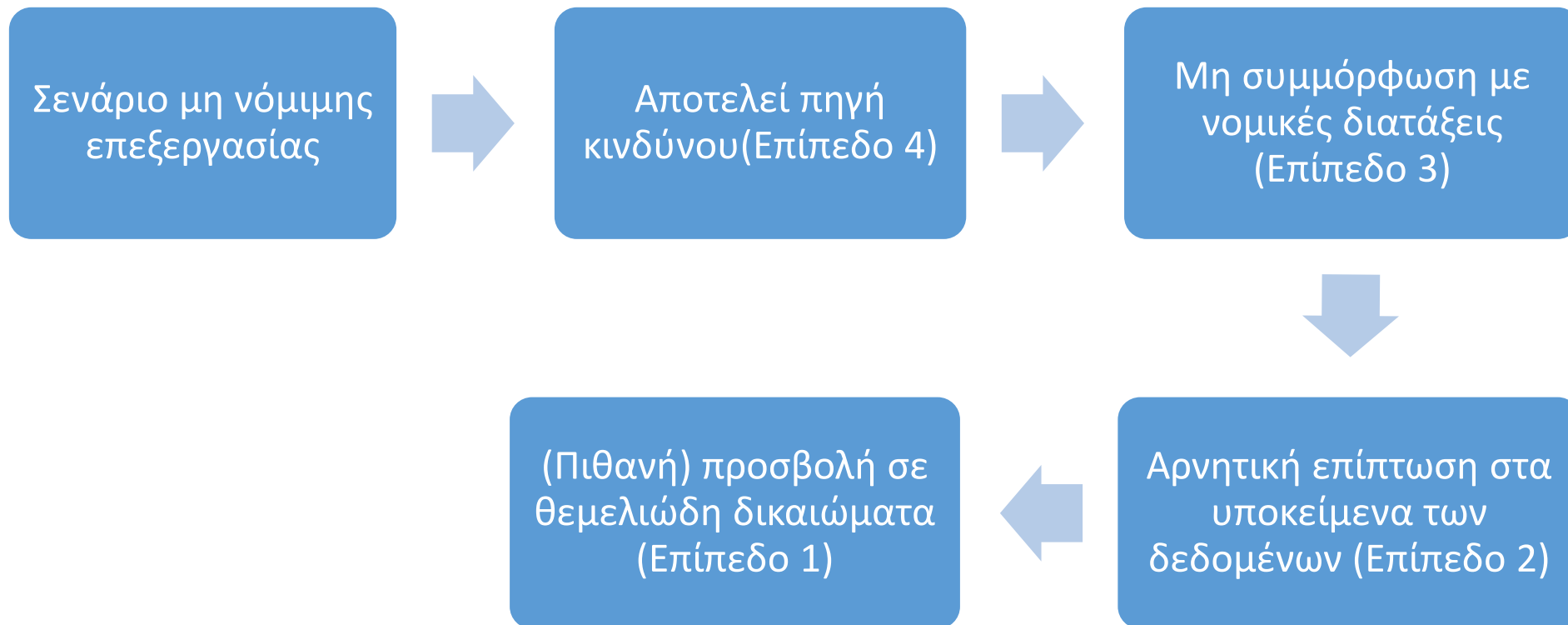
Επίπεδο 3: Μη συμμόρφωση με το κανονιστικό πλαίσιο



Επίπεδο 4: Πηγές Κινδύνων

Έργο byRisk

Εστιάζει στις αρνητικές επιπτώσεις που μπορεί να επέλθουν για τα υποκείμενα των δεδομένων από μη νόμιμη επεξεργασία δεδομένων τους.





Επίπεδο 1: Παραβίαση των Θεμελιωδών Δικαιωμάτων (1/2)

- Η μη νόμιμη επεξεργασία προσωπικών δεδομένων μπορεί να πλήξει διάφορα θεμελιώδη δικαιώματα (πέραν των δικαιωμάτων της προστασίας δεδομένων και ιδιωτικότητας)
- Το έργο byRisk δίνει έμφαση σε αυτά τα δικαιώματα
- Αυτά τα δικαιώματα ίσως παραβιαστούν αν ενεργοποιηθούν συγκεκριμένες πηγές κινδύνων, σε σχέση με την επεξεργασία προσωπικών δεδομένων

Επίπεδο 1: Παραβίαση των Θεμελιωδών Δικαιωμάτων (2/2)

Θεμελιώδη Δικαιώματα τα οποία μπορεί να παραβιαστούν:

1. Δικαίωμα στην Ανθρώπινη Αξιοπρέπεια.
2. Δικαίωμα στην Ιδιωτικότητα και στην Προστασία Δεδομένων.
3. Ελευθερία Έκφρασης και Πληροφορίας.
4. Ελευθερία του Συνέρχεσθαι και του Συνεταιρίζεσθαι.
5. Δικαίωμα στην Ιδιοκτησία.
6. Δικαίωμα στη μη Διάκριση και την Ισότητα (περιλαμβάνει ανθρώπους με αναπηρίες).
7. Δικαίωμα του Παιδιού.
8. Δικαίωμα στην Υγεία.
9. Οικονομικά και Κοινωνικά Δικαιώματα (δηλαδή εργασία, στέγαση, εκπαίδευση).

Επίπεδο 2: Επιπτώσεις για φυσικά πρόσωπα (1/4)

- Αντιστοιχεί σε πιθανές αρνητικές επιπτώσεις ή συνέπειες από την παραβίαση θεμελιωδών δικαιωμάτων.
- Τύποι επιπτώσεων:
 - Φυσικές
 - Οικονομικές
 - Υπόληψης
 - Διακρίσεις
 - Ψυχολογικές
 - Αυτονομίας
- Εστιάζει στις επιπτώσεις οι οποίες τυπικά αναμένεται να εμφανιστούν μέσω της επεξεργασίας προσωπικών δεδομένων από μικρομεσαίες επιχειρήσεις.

Επίπεδο 2: Επιπτώσεις για φυσικά πρόσωπα(2/4)

Πιθανές επιπτώσεις για φυσικά πρόσωπα:

1. Σωματική βλάβη.
2. Ψυχολογική επίπτωση – Άγχος.
3. (Διαδικτυακός) – εκφοβισμός.
4. Απώλεια αυτονομίας, χειραγώγηση και επιρροή (περιλαμβάνεται και η παραπληροφόρηση).
5. Αποθαρρυντική επίδραση (chilling effect).
6. Παραβίαση της ιδιωτικότητας (πέρα από τις προσδοκίες του χρήστη).
7. Αίσθηση απώλειας ελέγχου των προσωπικών δεδομένων.
8. Αρνητική επίπτωση σε φήμη/κύρος.
9. Διακρίσεις.
10. Άρνηση δικαιωμάτων / υπηρεσιών.
11. Οικονομική ζημία.

Επίπεδο 2: Επιπτώσεις για φυσικά πρόσωπα(3/4)

Οι προαναφερθείσες επιπτώσεις μπορούν να κατηγοριοποιηθούν σε τέσσερις κατηγορίες:

- Σωματικές και Ψυχολογικές Επιπτώσεις

1. Σωματική βλάβη.
2. Ψυχολογική επίπτωση – Άγχος.
3. (Διαδικτυακός) – εκφοβισμός.

- Επιπτώσεις Αυτονομίας

4. Απώλεια αυτονομίας, χειραγώγηση και επιρροή (περιλαμβάνεται και η παραπληροφόρηση).
5. Αποθαρρυντική επίδραση (chilling effect).
6. Παραβίαση της ιδιωτικότητας (πέρα από τις προσδοκίες του χρήστη).
7. Αίσθηση απώλειας ελέγχου των προσωπικών δεδομένων.

Επίπεδο 2: Επιπτώσεις για φυσικά πρόσωπα(4/4)

- Κοινωνικές Επιπτώσεις και Διακρίσεις
 8. Αρνητική επίπτωση σε φήμη/κύρος.
 9. Διακρίσεις.
 10. Άρνηση δικαιωμάτων / υπηρεσιών.
- Οικονομικές Επιπτώσεις
 11. Οικονομική ζημία.

Οι επιπτώσεις του Επιπέδου 2 και τα θεμελιώδη δικαιώματα του Επιπέδου 1 είναι συσχετισμένα, αλλά η ακριβής αντιστοίχιση τους εξαρτάται από το περιβάλλον της επεξεργασίας των προσωπικών δεδομένων.

Επίπεδο 3: Μη Συμμόρφωση με το Κανονιστικό Πλαίσιο(1/2)



- Περιγράφει γενικά νομικά ζητήματα τα οποία μπορούν να εμφανιστούν όταν ένας συγκεκριμένος κίνδυνος συμβεί.
- Βοηθά στο να αναγνωρίσουμε εάν συγκεκριμένες πηγές κινδύνου (Επίπεδο 4) οι οποίες μπορούν να προκαλέσουν επιπτώσεις σε φυσικά πρόσωπα όπως περιγράφονται στο Επίπεδο 2 είναι πραγματικά συσχετισμένες με τη μη συμμόρφωση με συγκεκριμένες νομικές διατάξεις.
- Βασίζεται στον GDPR.

Επίπεδο 3: Μη συμμόρφωση με το κανονιστικό πλαίσιο (2/2)

1. Έλλειψη διαφάνειας.
2. Παρέκκλιση σκοπού / Έλλειψη περιορισμού του σκοπού.
3. Παράνομη ή υπερβολική διατήρηση δεδομένων.
4. Συλλογή υπέρμετρου όγκου προσωπικών δεδομένων.
5. Απώλεια εμπιστευτικότητας / ακεραιότητας / ακρίβειας.
6. Έλλειψη ενήμερης συγκατάθεσης.
7. Τα δικαιώματα των χρηστών δεν ικανοποιούνται (επαρκώς).
8. Παράνομη δημιουργία προφίλ και / ή αυτοματοποιημένη λήψη αποφάσεων.
9. Έλλειψη ακρίβειας / ανθεκτικότητας / αμεροληψίας συστημάτων τεχνητής νοημοσύνης *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα)*

Επίπεδο 4: Πηγές Κινδύνων (1/4)

- Αντιστοιχεί σε πιθανές καταστάσεις που μπορούν να προκαλέσουν βλάβες σε φυσικά πρόσωπα.
- Εστιάζει σε συγκεκριμένες πηγές κινδύνου οι οποίες εάν υφίστανται μέσα σε ένα πλαίσιο επεξεργασίας δεδομένων θα έχουν ως αποτέλεσμα τη μη συμμόρφωση με το νομικό πλαίσιο.
- Περιλαμβάνει 21 γενικές πηγές κινδύνων οι οποίες καλύπτουν όλες τις πιθανές περιπτώσεις με βάση τα δεδομένα που αναφέρθηκαν στα προηγούμενα επίπεδα.

Πηγές Κινδύνων:

1. Έλλειψη πληροφόρησης σχετικά με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα
2. Ασαφή, πολύ γενικά ή πολύ σύνθετα κείμενα ενημερώσεων.
3. Χρήση των δεδομένων μου για στοχευμένη διαφήμιση.
4. Χρήση των δεδομένων των εργαζομένων για αξιολόγηση χωρίς νομική βάση.
5. Ένα μοντέλο ΤΝ που έχει εκπαιδευτεί για ένα πλαίσιο επαναχρησιμοποιείται σε άλλο *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα)*.
6. Η διάρκεια αποθήκευσης των δεδομένων δεν καθορίζεται καθόλου.
7. Η διάρκεια της αποθήκευσης των δεδομένων δεν δικαιολογείται.
8. Έλλειψη σχεδιασμού συλλογής δεδομένων για συγκεκριμένο σκοπό

9. Συλλογή δεδομένων χωρίς ειδική συγκατάθεση ή δυνατότητα εξαίρεσης.
10. Συλλογή προσωπικών πληροφοριών ταυτοποίησης χωρίς να είναι απαραίτητες.
11. Εξαγωγή συμπερασμάτων για (ενδεχομένως ευαίσθητες) προσωπικές πληροφορίες από το σύστημα TN (π.χ. η περιήγηση μπορεί να έχει ως αποτέλεσμα τη συναγωγή ευαίσθητων πληροφοριών, όπως η θρησκεία κ.λπ.)
(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).
12. Τα δεδομένα δημοσιεύονται στο Διαδίκτυο χωρίς νομική βάση.
13. Τα δεδομένα διαμοιράζονται με άλλα άτομα, χωρίς νομική βάση
14. Παραβίαση δεδομένων λόγω συμβάντος κυβερνοασφάλειας.
15. Κρυφή παρακολούθηση στο χώρο εργασίας (επικοινωνίες, αρχεία καταγραφής, PCs...,)
16. Δεν υπάρχει μηχανισμός για την εξασφάλιση της συγκατάθεσης των χρηστών
(αν και απαιτείται συγκατάθεση)

Επίπεδο 4: Πηγές Κινδύνων (4/4)



17. Παραπλανητικά μοτίβα στη συλλογή της συγκατάθεσης.
18. Τεχνικές αστοχίες όσον αφορά την ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων.
19. Μη (ορθή) ενημέρωση των υποκειμένων των δεδομένων σχετικά με τα δικαιώματά τους.
20. Μη ορθή χρήση αλγορίθμων για κατάρτιση προφίλ/αυτοματοποιημένη λήψη αποφάσεων.
21. Συστηματική παρακολούθηση των δραστηριοτήτων των εργαζομένων.

Κανονιστικά Ζητήματα Συσχετισμένα με τις Πηγές Κινδύνων

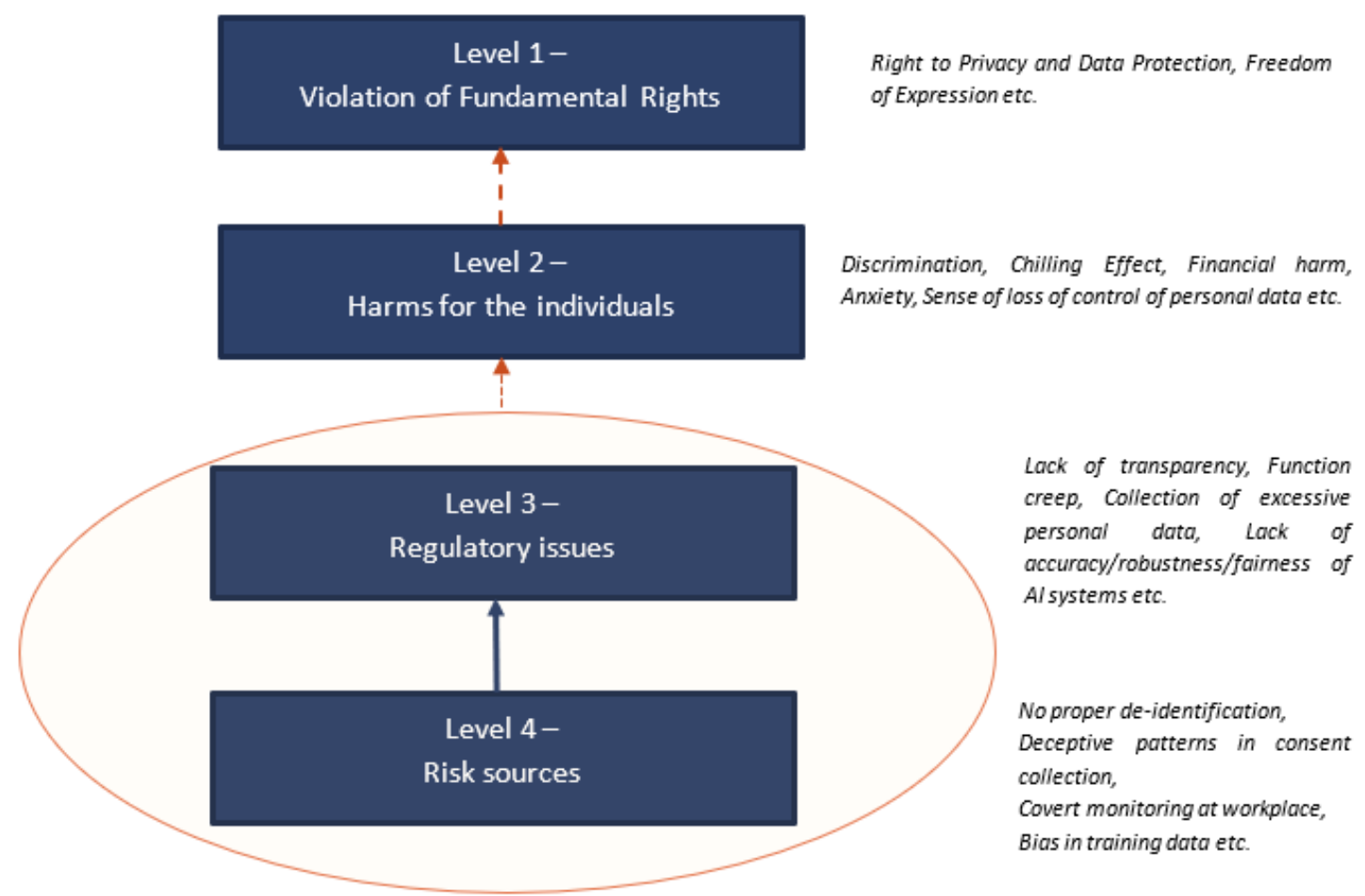
1. Έλλειψη διαφάνειας

- SR-1 Έλλειψη πληροφόρησης σχετικά με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- SR-2 Ασαφή, πολύ γενικά ή πολύ σύνθετα κείμενα ενημερώσεων
-

Παρέκκλιση σκοπού/έλλειψη περιορισμού σκοπού

- SR-5 Χρήση των δεδομένων μου για στοχευμένη διαφήμιση.
- SR-6 Χρήση των δεδομένων των εργαζομένων για αξιολόγηση χωρίς νομική βάση.
- ...

Συνοψίζοντας την Ταξινόμηση



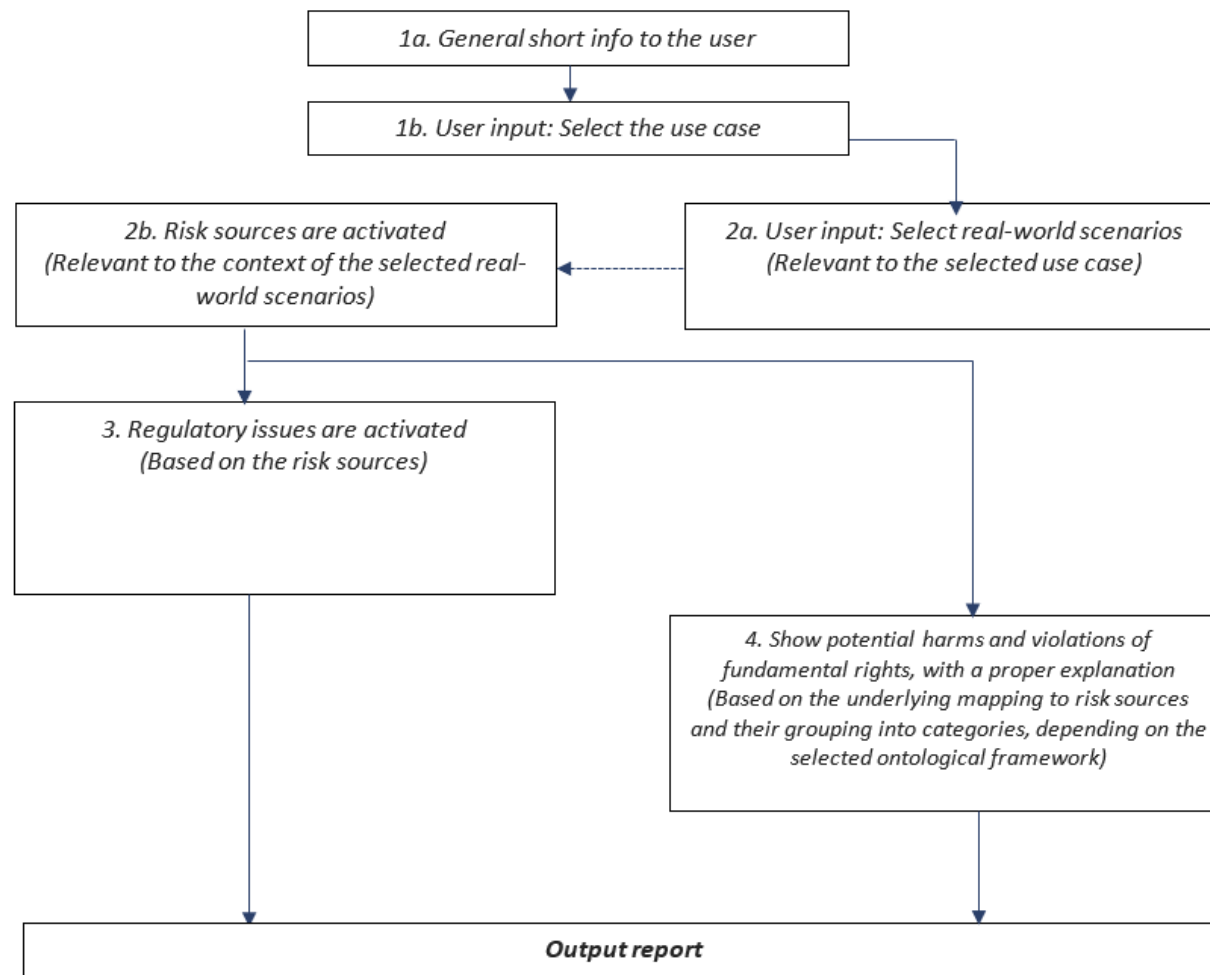
Εργαλείο Ευαισθητοποίησης Σχετικά με τον Κίνδυνο



Σε συνδυασμό με την ταξινόμηση που παρουσιάστηκε στις προηγούμενες διαφάνειες, το έργο byRisk ανέπτυξε ένα εργαλείο ευαισθητοποίησης σχετικά με τον Κίνδυνο το οποίο:

- Παρέχει μία σαφή και έγκυρη καταγραφή των διαφορετικών κινδύνων στα δικαιώματα και τις ελευθερίες του ευρέος κοινού.
- Αναδεικνύει τυπικές μεθόδους αντιμετώπισης αυτών των κινδύνων και παρουσιάζει τις πιθανές επιπτώσεις οι οποίες μπορούν να προκληθούν από κάθε έναν από τους προαναφερθέντες κινδύνους.

Ροή των Διαδικασιών

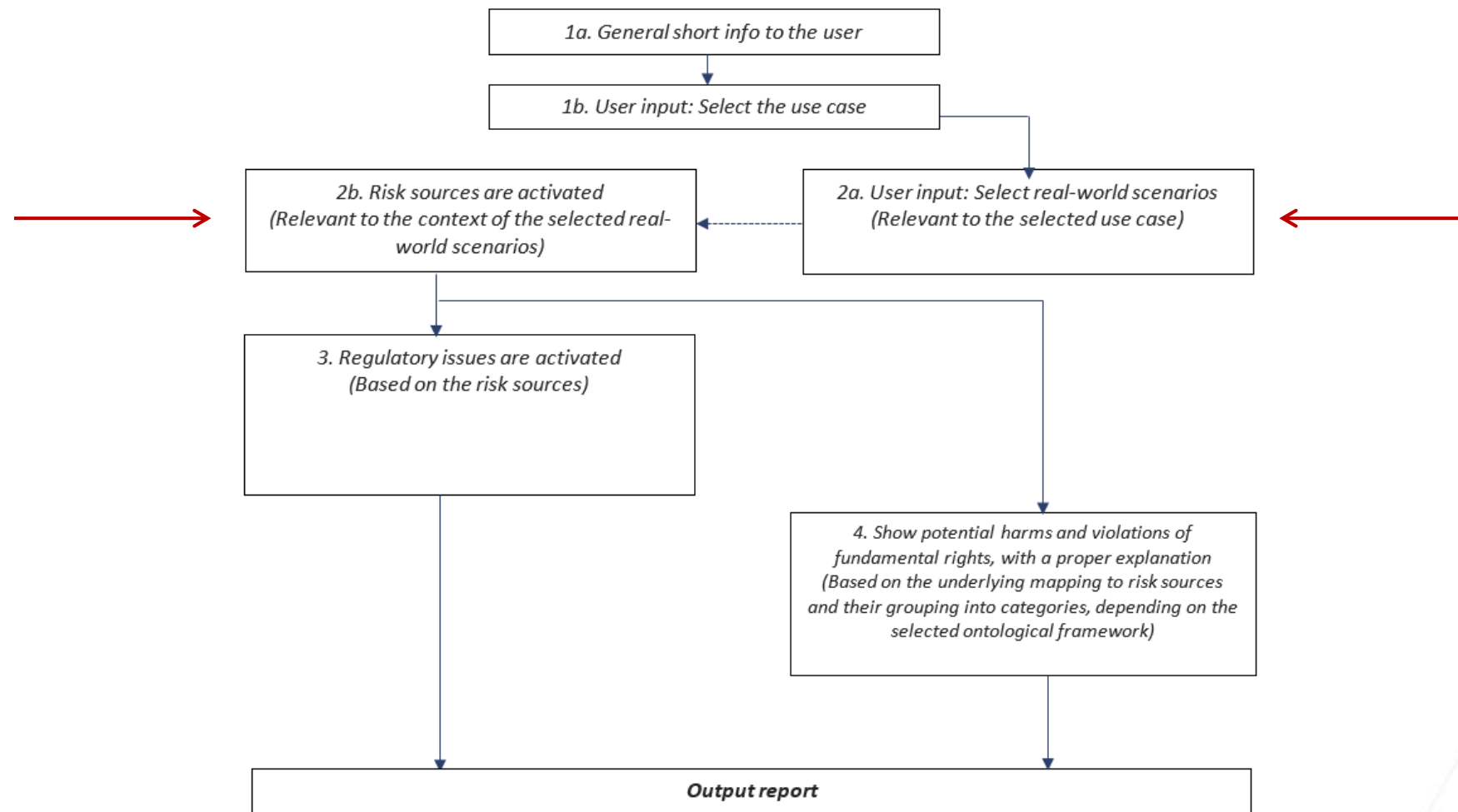


Πρακτικό Παράδειγμα

Use case: Επισκέπτομαι διάφορες ιστοσελίδες αναζητώντας πληροφορίες (δηλαδή περιήγηση στο διαδίκτυο).

- I. Θα ζητηθεί από το χρήστη να διαβάσει μία σύντομη εισαγωγική παράγραφο πριν χρησιμοποιήσει το εργαλείο. (Initial Phase 1a.)
- II. Ο χρήστης θα επιλέξει το «Επισκέπτομαι διάφορες ιστοσελίδες αναζητώντας πληροφορίες» όπως στο συγκεκριμένο παράδειγμα. (Phase 1b.)
- III. Ο χρήστης θα επιλέξει ένα ή περισσότερα πραγματικά σενάρια, βασισμένα στο επιλεγμένο παράδειγμα. Τα σενάρια θα παρουσιάζονται σε ομάδες βασισμένα στη συσχέτισή τους με τις πηγές κινδύνων (Phase 2a. – 2b.)

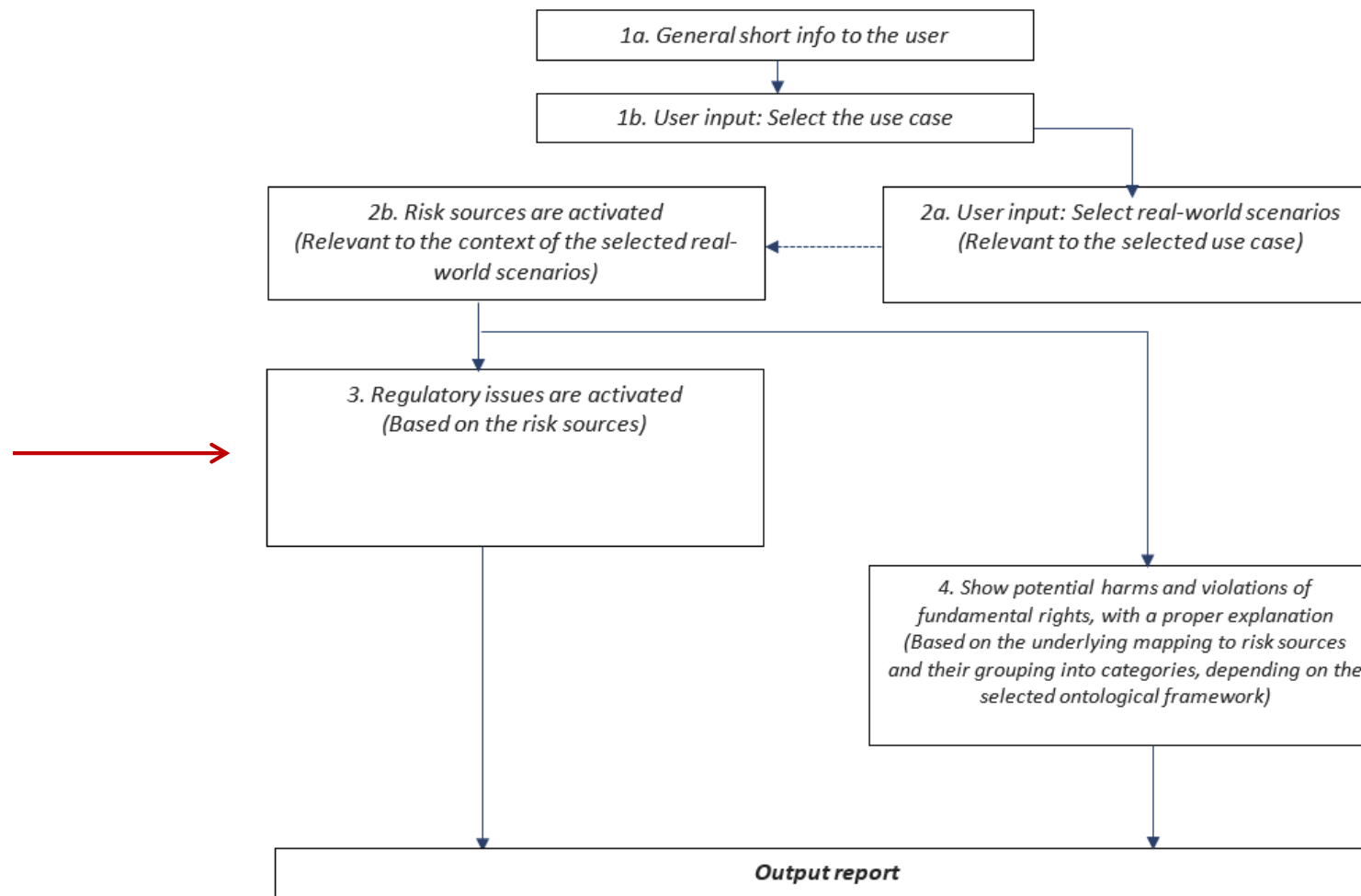
Ροή των Διαδικασιών



Οι συσχετίσεις μεταξύ των πηγών κινδύνων και των πραγματικών σεναρίων στη συγκεκριμένη περίπτωση χρήσης είναι:

1. SR-1. Έλλειψη πληροφόρησης σχετικά με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα
 - Ο ιστότοπος δεν διαθέτει πολιτική προστασίας δεδομένων.
 - Χρήση Χρήση ιχνηλατών τρίτων παρόχων και/ή cookies χωρίς ενημέρωση
 - Κρυφή παρακολούθηση της τοποθεσίας μου (π.χ. χρήση δεδομένων GPS για σκοπό που δεν γνωρίζω).
 - Τα δεδομένα μου συλλέγονται και συγκεντρώνονται από πολλαπλές πηγές χωρίς να το γνωρίζω.
 - Τα δεδομένα μου κοινοποιούνται σε τρίτους (συμπεριλαμβανομένων των παρόχων υπηρεσιών ανάλυσης δεδομένων ή οποιασδήποτε άλλης οντότητας) χωρίς να έχω πληροφορηθεί για αυτό.
 - Ο υπεύθυνος επεξεργασίας δεδομένων χρησιμοποιεί βιβλιοθήκες λογισμικού τρίτων παρόχων που συλλέγουν δεδομένα «σιωπηλά»

Ροή των Διαδικασιών



Πρακτικό Παράδειγμα

IV. Το εργαλείο θα αντιστοιχεί σημεία μη συμμόρφωσης με το κανονιστικό πλαίσιο που ενεργοποιούνται από τις επιλεγμένες πηγές κινδύνων (Phase 3)

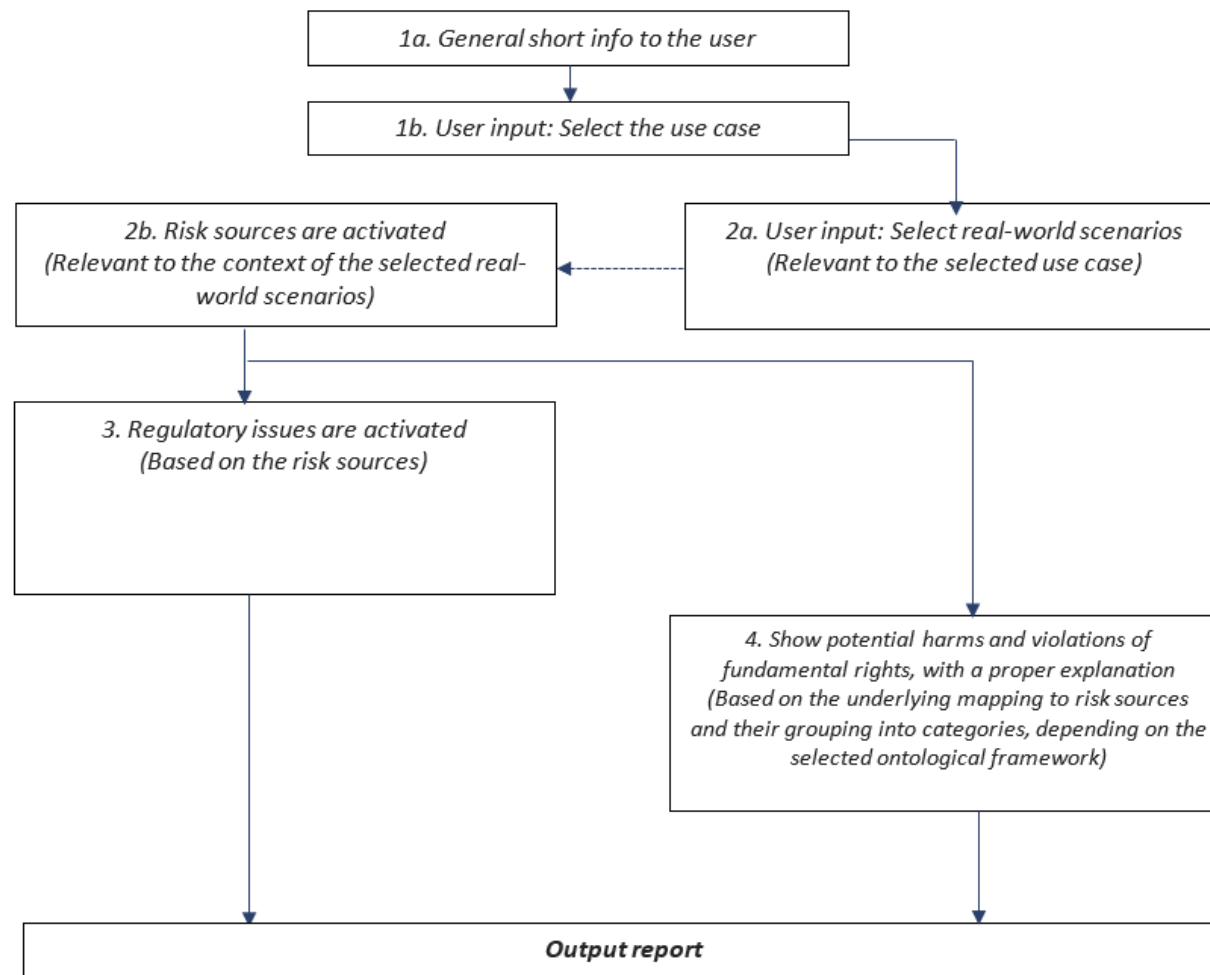
Για το συγκεκριμένο παράδειγμα τα πιθανά σημεία είναι τα ακόλουθα (βασισμένα στις πιθανές πηγές κινδύνων):

1. Έλλειψη διαφάνειας

- SR-1. Έλλειψη πληροφόρησης σχετικά με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- SR-2. Ασαφή, πολύ γενικά ή πολύ σύνθετα κείμενα ενημερώσεων.
- SR-30. Μη (ορθή) ενημέρωση των υποκειμένων των δεδομένων σχετικά με τα δικαιώματά τους.

...

Ροή των Διαδικασιών



Πρακτικό Παράδειγμα

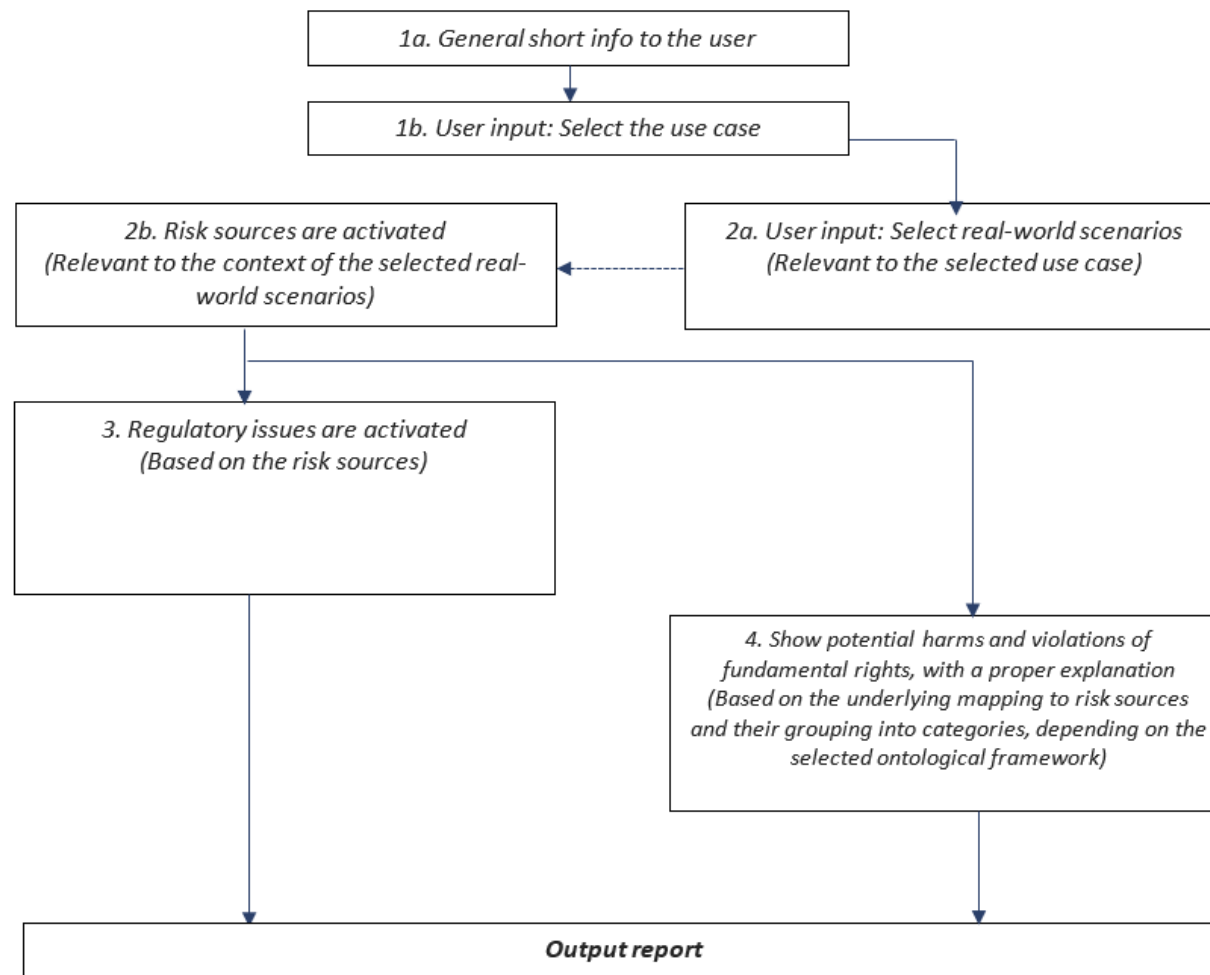
- V. Το εργαλείο θα δείχνει τις πιθανές επιπτώσεις και παραβιάσεις των θεμελιωδών δικαιωμάτων που είναι συσχετισμένα με τις πηγές κινδύνων της Φάσης 2b (Φάση 4). Το εργαλείο κατασκευάζει νέες ομάδες κινδύνων βασισμένες στις πηγές κινδύνων και τις συσχετίζει με τις πιθανές επιπτώσεις και παραβιάσεις δικαιωμάτων.

Οι νέες ομάδες είναι:

1. Έλλειψη Σαφούς Ενημέρωσης και Διαφάνειας
 - SR-1. Έλλειψη πληροφόρησης σχετικά με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
 - SR-2. Ασαφή, πολύ γενικά ή πολύ σύνθετα κείμενα ενημερώσεων.
 - SR-30. Μη (ορθή) ενημέρωση των υποκειμένων των δεδομένων σχετικά με τα δικαιώματά τους.
2. Έλλειψη συγκατάθεσης ή άλλης έγκυρης νομικής βάσης
 - SR-5. Χρήση των δεδομένων μου για στοχευμένη διαφήμιση.
 - SR-13. Έλλειψη σχεδιασμού συλλογής δεδομένων για συγκεκριμένο σκοπό.

...

Ροή των Διαδικασιών



Πρακτικό Παράδειγμα

Στο συγκεκριμένο παράδειγμα οι κατηγορίες πηγών κινδύνου είναι:

- Έλλειψη Σαφούς Ενημέρωσης και Διαφάνειας.
- Έλλειψη συγκατάθεσης ή άλλης έγκυρης νομικής βάσης .
- Παρακολούθηση ή/και Δημιουργία Προφίλ.

Πρακτικό Παράδειγμα

Με βάση τις ομάδες κινδύνων, οι συσχετίσεις με τις πιθανές επιπτώσεις είναι οι ακόλουθες:

1. Έλλειψη Σαφούς Ενημέρωσης και Διαφάνειας

- **Απώλεια αυτονομίας, χειραγώγηση και επιρροή (περιλαμβάνεται και η παραπληροφόρηση):** Όταν οι πρακτικές εξεργασίας δεδομένων είναι κρυμμένες ή αμφιλεγόμενες/πολύπλοκες, δεν μπορείτε να πάρετε ορθές αποφάσεις ή να συναινέσετε σωστά. Αυτό σας στερεί το δικαίωμα να κάνετε αυτόνομα μία ελεύθερη επιλογή και μπορεί να επιτρέψει την κρυφή χειραγώγηση και/ή επιρροή μέσω στοχευμένης διαφήμισης ή προκατειλημμένων αποτελεσμάτων αναζήτησης.
- **Αποθαρρυντική επίδραση (chilling effect):** Εάν υποψιαστείτε ότι οι αναζητήσεις σας παρακολουθούνται αλλά δεν μπορείτε να επιβεβαιώσετε πώς, τότε μπορεί να αυτολογοκριθείτε ή να αποφύγετε συγκεκριμένα θέματα.
- **Αίσθηση απώλειας ελέγχου των προσωπικών δεδομένων:** Όταν οι πρακτικές επεξεργασίας δεδομένων δεν είναι διαφανείς ή αμφιλεγόμενες ή όταν δεν γνωρίζετε τα δικαιώματά σας και/ή πώς να τα ασκήσετε, ή δεν μπορείτε να τα ασκήσετε, ίσως νιώσετε ότι δεν έχετε πια τον έλεγχο των δεδομένων σας - Ποιος τα συλλέγει, πώς χρησιμοποιούνται ή πώς να τα διαγράψετε.

Πρακτικό Παράδειγμα

- **Ψυχολογική επίπτωση – Άγχος:** Ακόμα και η απουσία μίας πολιτικής ιδιωτικότητας ή μίας αμφιλεγόμενης / πολύπλοκης πολιτικής μπορεί να προκαλέσει σύγχυση, αβεβαιότητα και έλλειψη εμπιστοσύνης. Ίσως αισθανθείτε αγχωμένοι π.χ. ποια δεδομένα συλλέγονται. Το ίδιο ισχύει όταν δε γνωρίζετε τα δικαιώματά σας – ή δεν καταλαβαίνετε πώς να τα ασκήσετε.
- **Άρνηση δικαιωμάτων / υπηρεσιών:** Εάν η διαδικασία δεν είναι διαφανής και/ή οι ιστοσελίδες δεν σας ενημερώνουν για τα δικαιώματά σας σωστά, τότε αυτό έμμεσα σημαίνει ότι δεν σας δίνεται η δυνατότητα να ασκήσετε τα δικαιώματά σας όπως ανάκληση συγκατάθεσης ή απαίτηση διαγραφής δεδομένων.
- **Ανεπιθύμητη παραβίαση της ιδιωτικότητας (πέρα από τις προσδοκίες του χρήστη):** Συνήθως αναμένετε πως έχετε κάποια δικαιώματα σχετικά με τα δεδομένα σας και γνωρίζετε ποιος επεξεργάζεται τα δεδομένα σας και για ποιο σκοπό. Εάν αυτό δεν είναι σαφές, νιώθετε ότι υπάρχει παραβίαση της ιδιωτικότητάς σας.

Πρακτικό Παράδειγμα

2. Έλλειψη Συγκατάθεσης ή άλλης έγκυρης νομικής βάσης

- **Ψυχολογική επίπτωση – Άγχος:** Ίσως νιώσετε άβολα όταν συνειδητοποιήσετε ότι η διαδικτυακή συμπεριφορά σας παρακολουθείται συνεχώς για διαφημιστικούς λόγους ή ότι τα δεδομένα σας συλλέγονται ευρέως (και πιθανότατα ξαναχρησιμοποιούνται για άγνωστους και πολλαπλούς σκοπούς). Επιπλέον, κάποια παραπλανητικά μοτίβα ίσως είναι αρκετά έντονα σε σχέση με το τι συναισθήματα προκαλούν στον χρήστη (π.χ. «Θα χάσεις αυτήν την μοναδική προσφορά;»).
- **Απώλεια αυτονομίας, χειραγώγηση και επιρροή (περιλαμβάνεται και η παραπληροφόρηση):** Στοχευμένες διαφημίσεις μπορούν διακριτικά να επηρεάσουν αποφάσεις, συμπεριφορές ή απόψεις – μερικές φορές εκμεταλλευόμενες διάφορες ευπάθειες (π.χ. συναισθηματικές καταστάσεις, εθισμοί). Αυτό απευθείας υπονομεύει την αυτονομία σας και τη λήψη τεκμηριωμένων αποφάσεων. Επίσης, αυτό μπορεί να προκληθεί εξαιτίας της έλλειψης αναλυτικής συγκατάθεσης ή σε κάποιες περιπτώσεις πλήρους απουσίας συγκατάθεσης.

Πρακτικό Παράδειγμα

- **Ανεπιθύμητη παραβίαση της ιδιωτικότητας (πέρα από τις προσδοκίες του χρήστη):** Η λήψη προσωποποιημένων διαφημίσεων ίσως οδηγήσει σε μεγαλύτερη από όσο φαντάζεστε παραβίαση της ιδιωτικότητας (π.χ. εάν δεν τις θέλετε ή εάν δεν ξέρετε γιατί βλέπετε συγκεκριμένες διαφημίσεις). Γενικότερα, εάν δεδομένα που συλλέγονται για έναν σκοπό φαίνεται να μην είναι σχετικά με αυτόν τον σκοπό ή η συγκατάθεσή σας δεν είχε ληφθεί σωστά, τότε οι προσδοκίες σας σχετικά με την ιδιωτικότητα σας παραβιάζονται.
- **Αίσθηση απώλειας ελέγχου των προσωπικών δεδομένων:** Όταν τα δεδομένα συλλέγονται χωρίς συγκεκριμένο ή διαφανή σκοπό ή όταν υπάρχει απώλεια μηχανισμών επιλογής (π.χ. για στοχευμένη διαφήμιση) δε μπορείτε να ελέγξετε πώς ή γιατί χρησιμοποιούνται τα δεδομένα σας (ίσως νιώσετε «παγιδευμένοι» σε ένα σύστημα όπου συλλέγει δεδομένα ανεξαρτήτως της θέλησής σας).
- **Διακρίσεις:** Σε περιπτώσεις στοχευμένης διαφήμισης, τέτοια συστήματα ίσως καταλήξουν σε διακρίσεις π.χ. εμφάνιση διαφορετικών αγγελιών εργασίας, τιμές ή ευκαιρίες σε συγκεκριμένες δημογραφικές ομάδες.

Πρακτικό Παράδειγμα

3. Παρακολούθηση ή/και Δημιουργία Προφίλ

- **Απώλεια αυτονομίας, χειραγώγηση και επιρροή (περιλαμβάνεται και η παραπληροφόρηση):** Οι αλγόριθμοι δημιουργίας προφίλ μπορούν να χρησιμοποιηθούν για τη χειραγώγηση φυσικών προσώπων (π.χ. μέσω συμπεριφορικών διαφημίσεων, προτάσεις περιεχομένου, πολιτική μικροστόχευση). Οι χρήστες κατευθύνονται προς συγκεκριμένες επιλογές χωρίς να το αντιλαμβάνονται – μία απευθείας παραβίαση της αυτονομίας.
- **Ανεπιθύμητη παραβίαση της Ιδιωτικότητας (πέρα από τις προσδοκίες του χρήστη):** Η δημιουργία προφίλ χρησιμοποιεί συγκέντρωση και εξαγωγή δεδομένων που είναι πέρα από αυτό που εσείς περιμένετε ή συγκατατίθεστε.
- **Αίσθηση απώλειας ελέγχου των προσωπικών δεδομένων:** Εάν δε μπορείτε εύκολα να γνωρίζετε τι δεδομένα χρησιμοποιούνται, πώς λαμβάνονται αποφάσεις ή πως να αμφισβητήσετε τα αποτελέσματα, τότε δημιουργείτε μία δυνατή αίσθηση απώλειας ελέγχου.

Πρακτικό Παράδειγμα

- **Διακρίσεις:** Τέτοιοι αλγόριθμοι μπορούν να οδηγήσουν σε άνιση μεταχείριση– π.χ. επειδή έχει δημιουργηθεί ένα ανακριβές προφίλ για εσάς ίσως δείτε διαφορετικές τιμές σε σχέση με άλλους (με βάση το προφίλ σας).
- **Ψυχολογική επίπτωση – Άγχος:** Ίσως νιώσετε άβολα όταν συνειδητοποιήσετε ότι αυτοματοποιημένα συστήματα παρακολουθούν τη διαδικτυακή συμπεριφορά σας για τη δημιουργία προφίλ.

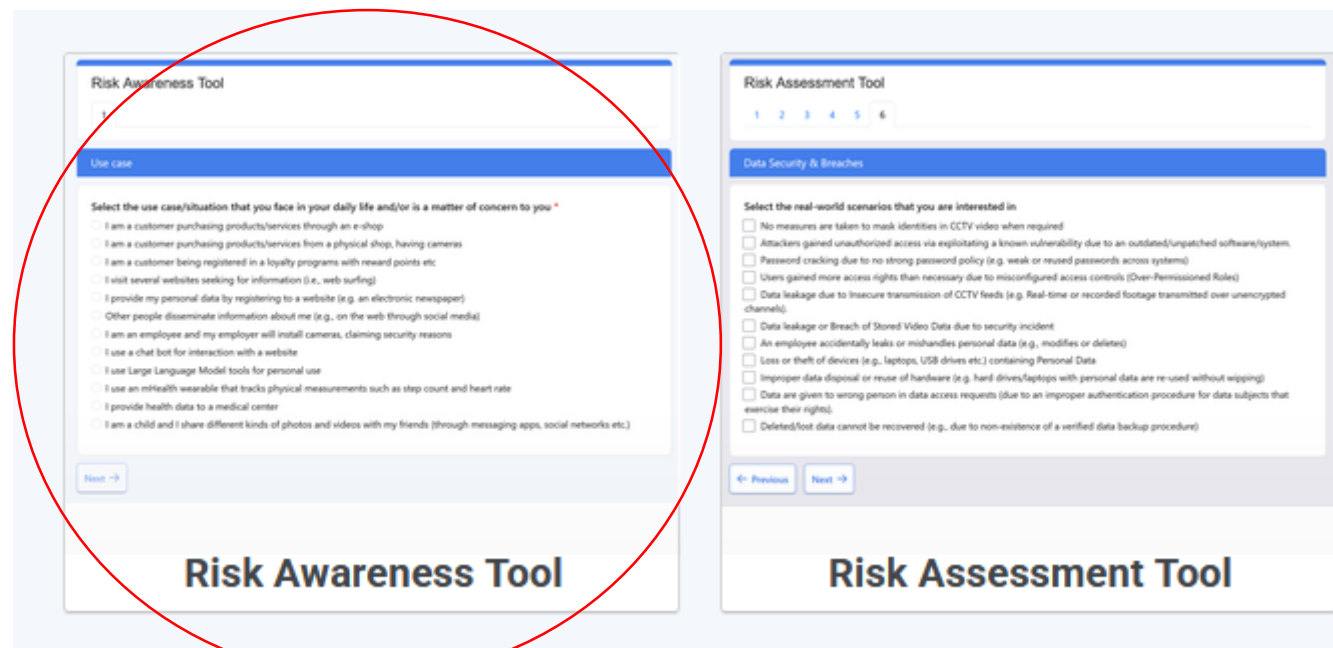
Πρακτικό Παράδειγμα

Οι πιθανές παραβιάσεις των θεμελιωδών δικαιωμάτων είναι οι ακόλουθες:

1. Δικαίωμα στην Ιδιωτικότητα και στην Προστασία Δεδομένων.
 - Αυτό καθιστά το βασικό δικαίωμα το οποίο ίσως παραβιαστεί – για παράδειγμα όταν αισθάνεστε αβοήθητοι σχετικά με το πώς τα δεδομένα σας χρησιμοποιούνται και από ποιον, όταν δεν μπορείτε εύκολα να ασκήσετε τα δικαιώματα της προστασίας των δεδομένων σας κλπ.
2. Δικαίωμα στη Μη Διάκριση και την Ισότητα
 - Προκαταλήψεις στους αλγόριθμους ή άνιση μεταχείριση (επιρροή και/ή χειραγώγηση) σε αποτελέσματα αναζήτησης, δημιουργία προφίλ, ή στοχευμένες διαφημίσεις, ίσως παραβιάσουν την ισότητα και το δικαίωμα στη μη διάκριση.
3. Ελευθερία Έκφρασης και Πληροφορίας.
 - Εάν αυτολογοκριθείτε ή αποφεύγετε διαδικτυακές αλληλεπιδράσεις από φόβο για τη δημιουργία προφίλ ή παρακολούθησης, τότε το δικαίωμά σας στην ελεύθερη έκφραση έχει περιοριστεί.

Το εργαλείο byRisk στην πράξη

- Επισκεφθείτε τη σελίδα <https://byrisk.dpa.gr/>



The screenshot displays two side-by-side panels of the byRisk tool. The left panel, titled 'Risk Awareness Tool', is circled in red and contains a 'Use case' section with a list of scenarios for selection. The right panel, titled 'Risk Assessment Tool', contains a 'Data Security & Breaches' section with a list of real-world scenarios for selection. Both panels have a 'Next' button at the bottom.

Risk Awareness Tool

Select the use case/situation that you face in your daily life and/or is a matter of concern to you *

- ☐ I am a customer purchasing products/services through an e-shop
- ☐ I am a customer purchasing products/services from a physical shop, having cameras
- ☐ I am a customer being registered in a loyalty programs with reward points etc
- ☐ I visit several websites seeking for information (i.e., web surfing)
- ☐ I provide my personal data by registering to a website (e.g. an electronic newspaper)
- ☐ Other people disseminate information about me (e.g., on the web through social media)
- ☐ I am an employee and my employer will install cameras, claiming security reasons
- ☐ I use a chat bot for interaction with a website
- ☐ I use Large Language Model tools for personal use
- ☐ I use an mHealth wearable that tracks physical measurements such as step count and heart rate
- ☐ I provide health data to a medical center
- ☐ I am a child and I share different kinds of photos and videos with my friends (through messaging apps, social networks etc.)

Next →

Risk Assessment Tool

Select the real-world scenarios that you are interested in

- ☐ No measures are taken to mask identities in CCTV video when required
- ☐ Attackers gained unauthorized access via exploiting a known vulnerability due to an outdated/unpatched software/system
- ☐ Password cracking due to no strong password policy (e.g. weak or reused passwords across systems)
- ☐ Users gained more access rights than necessary due to misconfigured access controls (Over-Permissioned Rules)
- ☐ Data leakage due to insecure transmission of CCTV feeds (e.g. Real-time or recorded footage transmitted over unencrypted channels)
- ☐ Data leakage or Breach of Stored Video Data due to security incident
- ☐ An employee accidentally leaks or mishandles personal data (e.g., modifies or deletes)
- ☐ Loss or theft of devices (e.g. laptops, USB drives etc.) containing Personal Data
- ☐ Improper data disposal or reuse of hardware (e.g. hard drives/laptops with personal data are re-used without wiping)
- ☐ Data are given to wrong person in data access requests (due to an improper authentication procedure for data subjects that exercise their rights)
- ☐ Deleted/lost data cannot be recovered (e.g., due to non-existence of a verified data backup procedure)

← Previous Next →

Σας ευχαριστώ για την Προσοχή σας.....