



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”

Driven by risk: Fostering data protection risk assessment for SMEs and raising risk awareness among the general public (byRisk)

(<https://byrisk-project.eu/>)





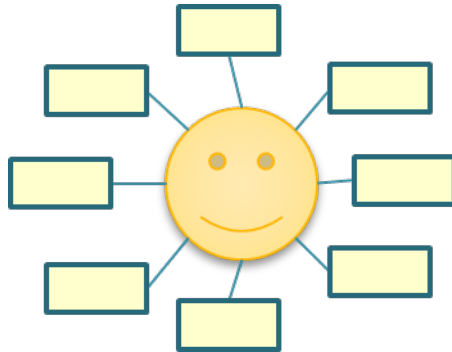
Πριν ξεκινήσουμε μερικά διαχειριστικά θέματα...



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

- 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.

Προσωπικά Δεδομένα

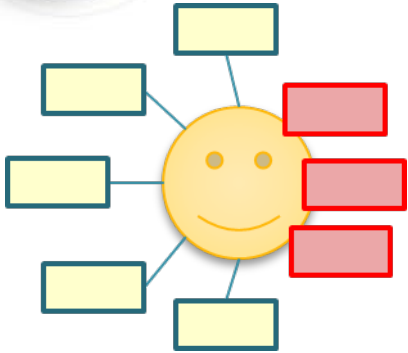


Π.χ. προσωπικά δεδομένα: όνομα και επώνυμο, αριθμός ταυτότητας, διεύθυνση κατοικίας, ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com, αναγνωριστικός αριθμός κάρτας, δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο), διεύθυνση δικτύου συσκευής χρήστη (IP address), 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.

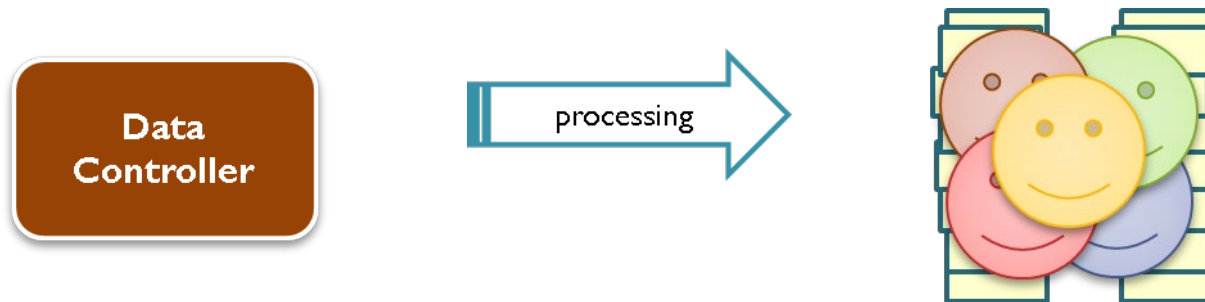
Ωστόσο, το εάν κάποιο identifier μπορεί να αναγνωρίσει ένα φυσικό πρόσωπο εξαρτάται από το πλαίσιο.

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’;



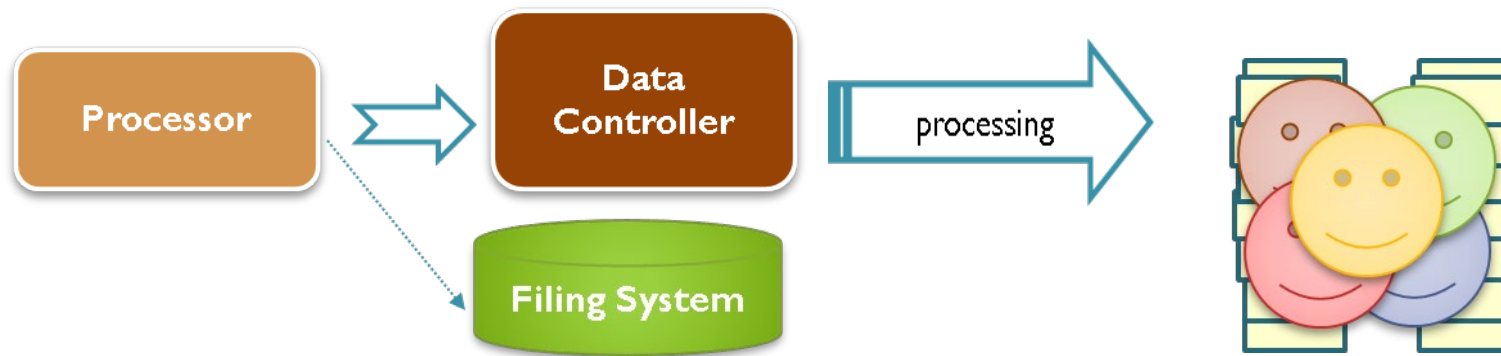
Ο υπεύθυνος επεξεργασίας είναι αυτός ο οποίος **αποφασίζει πώς και γιατί να συλλεχθούν και να χρησιμοποιηθούν τα δεδομένα**. Αυτό συνήθως είναι ένας οργανισμός , αλλά μπορεί να είναι και ένα φυσικό πρόσωπο (π.χ. ένας έμπορος, ένας γιατρός, ένας δικηγόρος κλπ.).

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.

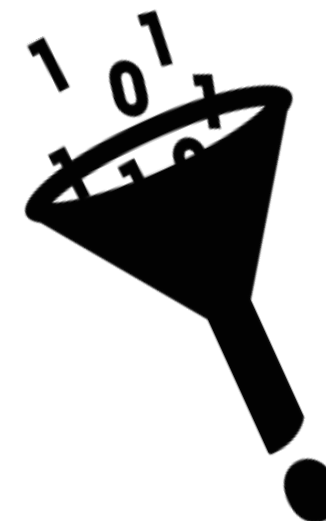
iii. Ελαχιστοποίηση των Δεδομένων

‘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.

‘Υφίστανται 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.

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 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.

Πως οι Μεθοδολογίες «Καθορίζουν» τον κίνδυνο (Ρίσκο)

Οι υπάρχουσες μεθοδολογίες για την ιδιωτικότητα και το ρίσκο υιοθετούν τη δική τους ερμηνεία για το ρίσκο η οποία καλύπτει τις συγκεκριμένες ανάγκες τους χωρίς να προσαρμόζονται σε συγκεκριμένες επιχειρησιακές ανάγκες και σενάρια. Συγκεκριμένα:

- Διάφορες προσεγγίσεις που αφορούν την εκτίμηση ρίσκου εστιάζουν στον καθορισμό του ρίσκου με βάση την «παραβίαση κανονισμών του GDPR» χωρίς να αξιολογούν τις πραγματικές συνέπειες της παραβίασης.
- Διάφορα πλαίσια αξιολόγησης ρίσκου δείχνουν μεγαλύτερη έμφαση στα ρίσκα που αφορούν την ασφάλεια των πληροφοριών σε σχέση με άλλες αρχές προστασίας δεδομένων (όπως ελαχιστοποίηση δεδομένων, νομιμότητα, δικαιώματα των υποκειμένων των δεδομένων).

Η έννοια του Αντίκτυπου

Ο αντίκτυπος μπορεί να κατηγοριοποιηθεί σε:

- Ασήμαντος αντίκτυπος
- Περιορισμένος αντίκτυπος
- Σημαντικός αντίκτυπος
- Μέγιστος αντίκτυπος

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



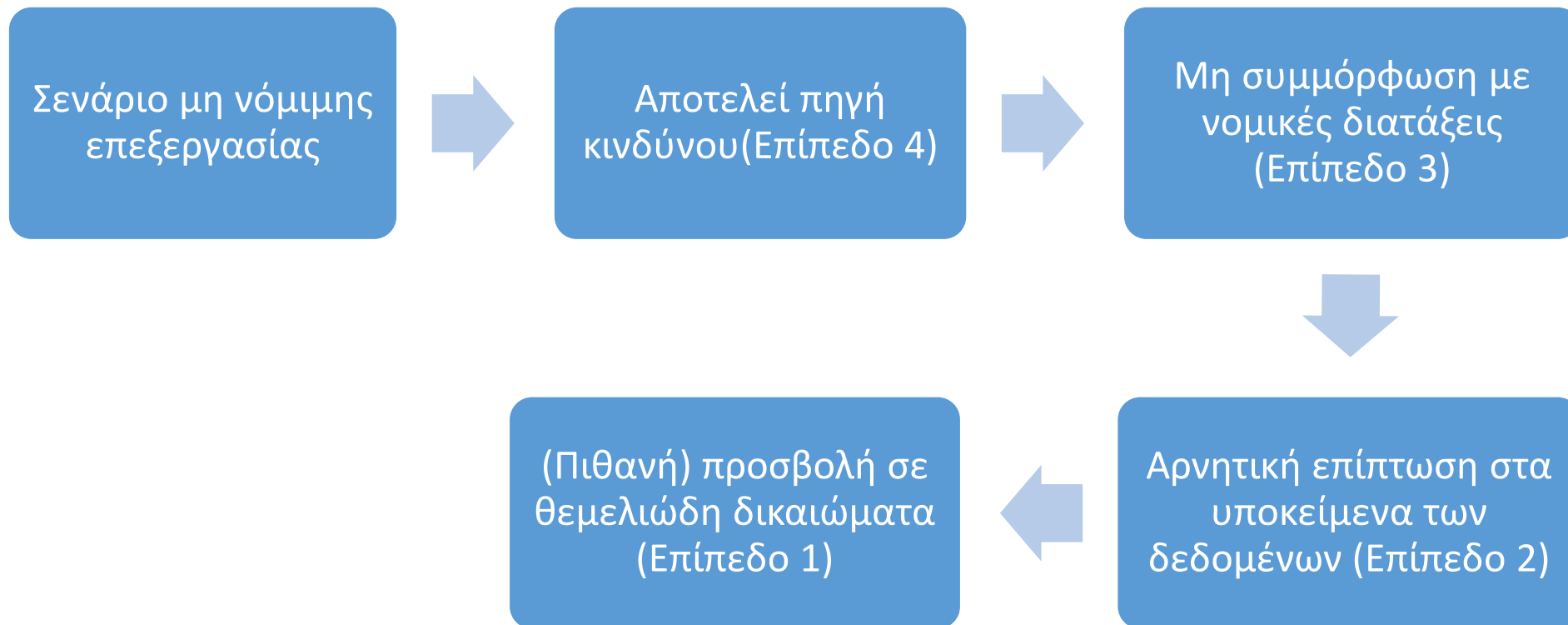
Επίπεδο 3: Μη συμμόρφωση με το κανονιστικό πλαίσιο



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)



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

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)



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

- 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 (1/41)

- 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 40 γενικές πηγές κινδύνων οι οποίες καλύπτουν όλες τις πιθανές περιπτώσεις με βάση τα δεδομένα που αναφέρθηκαν στα προηγούμενα επίπεδα.

Επίπεδο 4: Πηγές Κινδύνων (2/41)

Πηγές Κινδύνων:

1. Έλλειψη πληροφόρησης σχετικά με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
 - Χρήση βιβλιοθηκών λογισμικού τρίτων παρόχων που συλλέγουν δεδομένα «σιωπηλά».
 - «Κρυφές» μεταβιβάσεις δεδομένων μέσω API.
 - Χρήση ιχνηλατών τρίτων παρόχων και/ή cookies, τα οποία δεν είναι απαραίτητα για την παροχή της υπηρεσίας, χωρίς ενημέρωση.
 - Ο ιστότοπος δεν διαθέτει πολιτική προστασίας δεδομένων.
 - ...

Επίπεδο 4: Πηγές Κινδύνων (3/41)

2. Ασαφή, πολύ γενικά ή πολύ σύνθετα κείμενα ενημερώσεων

- Χρήση εργαλείων αυτόματης δημιουργίας πολιτικών απορρήτου χωρίς προσαρμογή.
- Χρήση δηλώσεων όπως «ενδέχεται να χρησιμοποιήσουμε τα δεδομένα σας για να βελτιώσουμε τις υπηρεσίες μας».
- Η πολιτική απορρήτου περιγράφει τα δεδομένα που συλλέγονται, τους σκοπούς επεξεργασίας τους και έναν κατάλογο νομικών βάσεων χωρίς ωστόσο να διευκρινίζει ποια δεδομένα αντιστοιχούν σε ποιο σκοπό ή/και ποιος σκοπός σε ποια νομική βάση.
- ...

Επίπεδο 4: Πηγές Κινδύνων (4/41)

3. Χρήση αδιαφανών μοντέλων TN που δεν παρέχουν πληροφορίες σχετικά με τον τρόπο με τον οποίο οι είσοδοι μετατρέπονται σε εξόδους *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*
- Ανάπτυξη σύνθετων μοντέλων (π.χ. βαθιά νευρωνικά δίκτυα, μέθοδοι συνόλων/ensemble methods) χωρίς τη χρήση εργαλείων όπως, ενδεικτικά, τα αντιπαραδειγματικά σενάρια (counterfactuals) ή η εφαρμογή ανάλυσης σημαντικότητας χαρακτηριστικών (feature importance analysis).
 - Χρήση στοιχείων/συστατικών TN κλειστού κώδικα ή προερχόμενων από τρίτους παρόχους, χωρίς πρόσβαση στην εσωτερική λογική λειτουργίας τους.
 - Ανεπαρκής τεκμηρίωση σχετικά με τον σχεδιασμό μοντέλων, τις διαδικασίες εκπαίδευσης και τις παραδοχές στις οποίες αυτό βασίζεται.

Επίπεδο 4: Πηγές Κινδύνων (5/41)

4. Απουσία ερμηνευσιμότητας *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*

- Δεν υπάρχουν διεπαφές χρήστη ή μηχανισμοί ανατροφοδότησης για την επεξήγηση της λογικής λήψης απόφασης για το σύστημα TN.
- Ανεπαρκής τεκμηρίωση σχετικά με τον σχεδιασμό μοντέλων, τις διαδικασίες εκπαίδευσης και τις παραδοχές στις οποίες αυτό βασίζεται.
- Χρήση στοιχείων/συστατικών TN κλειστού κώδικα ή προερχόμενων από τρίτους παρόχους, χωρίς πρόσβαση στην εσωτερική λογική λειτουργίας τους

Επίπεδο 4: Πηγές Κινδύνων (6/41)

5. Χρήση των δεδομένων των πελατών/χρηστών για στοχευμένη διαφήμιση.
- Τα προσωπικά δεδομένα αναλύονται για να συναχθούν οι προτιμήσεις ή η συμπεριφορά των χρηστών (προφίλ) για διαφημιστικούς σκοπούς χωρίς έγκυρη συγκατάθεση.
 - Τα δεδομένα κοινοποιούνται σε διαφημιστικά δίκτυα, παρόχους υπηρεσιών ανάλυσης δεδομένων κ.λπ. χωρίς να λαμβάνεται έγκυρη συγκατάθεση.
 - Οι πολιτικές απορρήτου δεν αναφέρουν σαφώς ότι τα δεδομένα των χρηστών θα χρησιμοποιηθούν για διαφήμιση ή η χρήση αυτή είναι «κρυμμένη» σε αόριστες ή σύνθετες διατυπώσεις.
 - ...

Επίπεδο 4: Πηγές Κινδύνων (7/41)

6. Χρήση των δεδομένων των υπαλλήλων για αξιολόγηση χωρίς νομική βάση.

- Ανάπτυξη εργαλείων παρακολούθησης της παραγωγικότητας/των επιδόσεων που βασίζονται στην ΤΝ χωρίς νομική βάση *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα)*.
- Συλλογή υπερβολικών δεδομένων (π.χ. πλήρες ιστορικό περιήγησης) χωρίς νόμιμο σκοπό που να συνδέεται με υποχρεώσεις απασχόλησης.
- Χρήση εργαλείων ΤΝ για προσλήψεις χωρίς ενημέρωση και/ή χωρίς ανθρώπινη παρέμβαση *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα)*.
- ...

Επίπεδο 4: Πηγές Κινδύνων (8/41)

7. Κοινοποίηση δεδομένων σε τρίτους χωρίς εκ νέου προσδιορισμό του σκοπού και χωρίς νομική βάση (π.χ. μεσίτες δεδομένων (data brokers))
 - Χρήση βιβλιοθηκών λογισμικού από τρίτους παρόχους που συλλέγουν δεδομένα «σιωπηλά».
 - «Κρυφές» μεταβιβάσεις δεδομένων μέσω API.
 - Οι δραστηριότητες των εκτελούντων την επεξεργασία δεν υπόκεινται σε εποπτεία και έλεγχο.
 - Μη πλήρεις ή ασαφείς συμφωνίες επεξεργασίας δεδομένων (Data Protection Agreements) σχετικά με το τι μπορεί να κάνει ο εκτελών την επεξεργασία.
 - ...

Επίπεδο 4: Πηγές Κινδύνων (9/41)

8. Μη ανανέωση της συγκατάθεσης για τον νέο σκοπό (για τον οποίο απαιτείται νέα συγκατάθεση)
- Θεώρηση ότι η ευρεία ή γενική συγκατάθεση που ελήφθη αρχικά είναι επαρκής για κάθε νέα δραστηριότητα επεξεργασίας.
 - Δεν εφαρμόζεται ορθή διαδικασία για τον έλεγχο του κατά πόσον μια αλλαγή στον σκοπό της επεξεργασίας απαιτεί εκ νέου συγκατάθεση.
 - Οι όροι συγκατάθεσης ενημερώνονται στην πολιτική απορρήτου, αλλά οι υπάρχοντες χρήστες δεν καλούνται εκ νέου να παράσχουν νέα συγκατάθεση για τις αλλαγές.

Επίπεδο 4: Πηγές Κινδύνων (10/41)

9. Τα δεδομένα που συλλέχθηκαν αρχικά για έναν σκοπό επαναχρησιμοποιούνται για την ανάπτυξη ή την ανάλυση μοντέλων ΤΝ χωρίς πρόσθετη συγκατάθεση ή χωρίς άλλη νομική βάση *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα)*.
- Κοινοποίηση δεδομένων χρηστών σε άλλους οργανισμούς για ανάπτυξη τεχνητής νοημοσύνης.
 - Χρήση «παλαιών» δεδομένων για εκπαίδευση ΤΝ μοντέλου, τα οποία είχαν χρησιμοποιηθεί για διαφορετική περίπτωση.
 - Συνεχής συλλογή δεδομένων προσωπικού χαρακτήρα από διάφορες πηγές, για την τροφοδότηση του συστήματος ΤΝ, χωρίς νομική βάση.

Επίπεδο 4: Πηγές Κινδύνων (11/41)

10. Ένα μοντέλο ΤΝ που έχει εκπαιδευτεί για ένα πλαίσιο επαναχρησιμοποιείται σε άλλο *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).*

- Οι ικανότητες του συστήματος ΤΝ επεκτείνονται πέραν του αρχικού πεδίου εφαρμογής του.
- Ένας ψηφιακός βοηθός ΤΝ (AI chatbot) που έχει εκπαιδευτεί σε ερωτήματα γενικής εξυπηρέτησης πελατών επαναχρησιμοποιείται για άλλους σκοπούς (π.χ. για την ανάλυση συναισθημάτων του χρήστη).

Επίπεδο 4: Πηγές Κινδύνων (12/41)

11. Η διάρκεια της αποθήκευσης των δεδομένων δεν είναι καθορισμένη.

- Δεν υπάρχει χρονοδιάγραμμα/πολιτική για την περίοδο αποθήκευσης δεδομένων για διαφορετικούς τύπους δεδομένων προσωπικού χαρακτήρα.
- Αποτυχία ενσωμάτωσης πολιτικών διατήρησης με συστήματα δημιουργίας αντιγράφων ασφαλείας και αρχειοθέτησης δεδομένων.
- Το μοντέλο TN δεν μπορεί να επανεκπαιδευτεί ή να τροποποιηθεί μετά τη διαγραφή δεδομένων (Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).

Επίπεδο 4: Πηγές Κινδύνων (13/41)

12. Η διάρκεια της αποθήκευσης των δεδομένων δεν είναι τεκμηριωμένη.

- Εφαρμόζεται ενιαία περίοδος διατήρησης δεδομένων σε όλους τους τύπους δεδομένων (ο υπεύθυνος επεξεργασίας δεδομένων δεν επιβάλλει χρονοδιάγραμμα διατήρησης δεδομένων για διαφορετικούς τύπους δεδομένων προσωπικού χαρακτήρα).
- Οι μηχανισμοί διαγραφής δεδομένων δεν εφαρμόζονται σωστά λόγω σφαλμάτων συστήματος/λογισμικού.
- Μη δικαιολογημένη αποθήκευση δεδομένων από τους εκτελούντες την επεξεργασία.
- ...

Επίπεδο 4: Πηγές Κινδύνων (14/41)

13. Έλλειψη σχεδιασμού συλλογής δεδομένων για συγκεκριμένο σκοπό.

- Τα API ή οι εφαρμογές δεν έχουν σχεδιαστεί με σαφείς περιορισμούς ελαχιστοποίησης δεδομένων για κάθε σκοπό.
- Οι «έξυπνες» εφαρμογές έχουν πρόσβαση σε περισσότερα δεδομένα από όσα πραγματικά χρειάζονται.
- Συγκέντρωση δεδομένων από πολλαπλές πηγές συνδυαστικά, με αποτέλεσμα συλλογή περισσότερων δεδομένων από όσα απαιτούνται για τον σκοπό (δηλαδή υπερβαίνουν τον αρχικό σκοπό).
- Αυτόματη καταγραφή της δραστηριότητας του χρήστη χωρίς την κατάλληλη ελαχιστοποίηση των δεδομένων.
- ...

Επίπεδο 4: Πηγές Κινδύνων (15/41)

14. Συλλογή δεδομένων χωρίς ειδική συγκατάθεση ή δυνατότητα εξαίρεσης.

- Προαιρετικές δηλώσεις για επεξεργασία δεδομένων τίθενται ως υποχρεωτικές στις συμβάσεις.
- Ζητείται μία συγκατάθεση για περισσότερους από έναν διαφορετικούς σκοπούς.
- Δεν υπάρχουν (εύκολα) μέσα για να αντιταχθούν οι χρήστες στην επεξεργασία.

Επίπεδο 4: Πηγές Κινδύνων (16/41)

15. Συλλογή προσωπικών πληροφοριών ταυτοποίησης χωρίς να είναι απαραίτητες.

- Χρήση εργαλείων αναγνώρισης προσώπου χωρίς νομική βάση.
- Μη σωστή εφαρμογή εργαλείων τρίτων παρόχων (π.χ. εξαγωγή στατιστικών στοιχείων, CRM, «ζωντανή» συνομιλία), διαμορφωμένα για τη συλλογή προσωπικών αναγνωρίσιμων πληροφοριών χωρίς να είναι απαραίτητα.
- Οι πραγματικές ανάγκες σε δεδομένα δεν είναι σαφώς καθορισμένες (π.χ. προγραμματιστές ή ιδιοκτήτες προϊόντων συμπεριλαμβάνουν πεδία πληροφοριών προσωπικής ταυτοποίησης για κάθε περίπτωση που «μπορεί να χρειαστούν»).

Επίπεδο 4: Πηγές Κινδύνων (17/41)

16. Επανα-ταυτοποίηση χρήστη χωρίς να είναι απαραίτητο για τον επιδιωκόμενο σκοπό

- Εκμετάλλευση ασθενούς ψευδωνυμοποίησης (π.χ. η οποία έγινε με απλό hash χωρίς κλειδί) με στόχο την αντιστροφή της ψευδωνυμοποίησης.
- Σύνδεση ανωνυμοποιημένων / ψευδωνυμοποιημένων συνόλων δεδομένων με άλλα σύνολα δεδομένων για την αποκάλυψη ταυτότητας.
- Μη ανώνυμα δεδομένα χαρακτηρίζονται λανθασμένα ως ανώνυμα (π.χ. δημοσίευση «πλούσιων» συνόλων δεδομένων με πολλά ψευδο-αναγνωριστικά (quasi-identifiers)).
- Το σύνολο δεδομένων εκπαίδευσης ΤΝ μοντέλου δεν είναι σωστά ανωνυμοποιημένο / ψευδωνυμοποιημένο (Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).
- ...

Επίπεδο 4: Πηγές Κινδύνων (18/41)

17. Μη δικαιολογημένη παρακολούθηση της τοποθεσίας ή της διαδικτυακής συμπεριφοράς.

- Χρήση ιχνηλατών τρίτων παρόχων και/ή cookies, τα οποία δεν είναι απαραίτητα για την παροχή της υπηρεσίας, χωρίς ενημέρωση.
- Χρήση τεχνολογιών παρακολούθησης (π.χ. cookies) για την παρακολούθηση χωρίς την έγκυρη συγκατάθεση του χρήστη μετά από ενημέρωσή του.
- Χρήση δεδομένων GPS χωρίς να είναι απαραίτητα για τον επιδιωκόμενο σκοπό επεξεργασίας.
- ...

Επίπεδο 4: Πηγές Κινδύνων (19/41)

18. Έλλειψη κατάλληλου σχεδιασμού για συλλογή δεδομένων για χρήση για εκπαίδευση TN μοντέλου *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*

- Χρήση προσωπικών δεδομένων για εκπαίδευση χωρίς φιλτράρισμα μη σχετικών χαρακτηριστικών.
- Συνεχής συλλογή δεδομένων προσωπικού χαρακτήρα από διάφορες πηγές, για την τροφοδότηση του συστήματος TN για εκπαίδευση, χωρίς νομική βάση.
- Δεδομένα που εισάγουν οι χρήστες χρησιμοποιούνται και για εκπαίδευση του μοντέλου, χωρίς κατάλληλη νομική βάση.
- ...

Επίπεδο 4: Πηγές Κινδύνων (20/41)

19. 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).*

- Συσχέτιση διαφορετικών συνόλων δεδομένων για τη συναγωγή προσωπικών πληροφοριών.
- Τα συστήματα TN συνάγουν δεδομένα σχετικά με τους χρήστες με βάση τις αγορές / συναλλαγές τους χωρίς νομική βάση.
- Χρήση συστημάτων αναγνώρισης προσώπου χωρίς νομική βάση.
- ...

Επίπεδο 4: Πηγές Κινδύνων (21/41)

20. Απομνημόνευση Προσωπικών Δεδομένων από το TN μοντέλο (Model memorization) *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*

- Συμπερίληψη σπάνιων/μοναδικών αρχείων στο σύνολο δεδομένων εκπαίδευσης.
- Το σύνολο δεδομένων εκπαίδευσης δεν είναι σωστά ανωνυμοποιημένο / ψευδωνυμοποιημένο.
- Εσφαλμένες προδιαγραφές μοντέλου λόγω υπερπροσαρμογής (overfitting).
- ...

Επίπεδο 4: Πηγές Κινδύνων (22/41)

21. Δημοσίευση δεδομένων στο διαδίκτυο χωρίς νομική βάση.

- Ένας εργαζόμενος δημοσιεύει κατά λάθος προσωπικά δεδομένα (π.χ. εκ παραδρομής ή εν αγνοία του).
- Ένα τεχνικό ζήτημα/πρόβλημα καθιστά τα δεδομένα διαθέσιμα στο κοινό (π.χ. διαθέσιμα μέσω URL).
- Τα δεδομένα δημοσιεύονται σκόπιμα στο διαδίκτυο από έναν κακόβουλο χρήστη (δηλαδή έναν εισβολέα).

Επίπεδο 4: Πηγές Κινδύνων (23/41)

22. Διαμοιρασμός δεδομένων με τρίτους χωρίς νομική βάση.

- Εκ παραδρομής αποστολή αλληλογραφίας με προσωπικά δεδομένα (ή με άλλα μέσα) σε λάθος παραλήπτες.
- Ανταλλαγή δεδομένων μέσω διαφόρων διαύλων επικοινωνίας (π.χ. μέσα κοινωνικής δικτύωσης, εφαρμογές βιντεοδιάσκεψης), χωρίς νομική βάση.
- Δεν λαμβάνονται μέτρα για την απόκρυψη των προσώπων σε βίντεο κλειστού κυκλώματος τηλεόρασης όταν απαιτείται.

Επίπεδο 4: Πηγές Κινδύνων (24/41)

23. Παραβίαση Δεδομένων λόγω συμβάντος κυβερνοασφάλειας.

- Διαρροή δεδομένων λόγω εκμετάλλευσης μη κατάλληλα διαμορφωμένου πρωτοκόλλου δικτύου και/ή εφαρμογής (π.χ. εσφαλμένα διαμορφωμένο TLS που επιτρέπει παρωχημένες κρυπτογραφικές σουίτες, εσφαλμένα διαμορφωμένος διακομιστής εφαρμογής/βάσης δεδομένων που επιτρέπει επιθέσεις τύπου «SQL injection» κ.λπ.).
- Εξαγωγή δεδομένων εισόδου χρηστών λόγω μη ασφαλών APIs ή τελικών σημείων (endpoints).
- Μη εξουσιοδοτημένοι χρήστες απέκτησαν πρόσβαση λόγω απουσίας ισχυρού μηχανισμού ελέγχου ταυτότητας (π.χ. μη χρήση ελέγχου ταυτότητας δύο παραγόντων (2FA) σε περίπτωση που απαιτείται).
- ...

Επίπεδο 4: Πηγές Κινδύνων (25/41)

24. Παραβίαση δεδομένων εξαιτίας ενός ανθρώπινου παράγοντα (πέραν της περίπτωσης δημοσίευσης/διαμοιρασμού δεδομένων).

- Ένας υπάλληλος ανταποκρίνεται σε ηλεκτρονικό παραπλανητικό (Phishing) μήνυμα.
- Εργαζόμενος εσκεμμένα αποσπά, διαρρέει ή διαχειρίζεται με λάθος τρόπο προσωπικά δεδομένα.
- Απώλεια ή κλοπή εγγράφων σε έντυπη μορφή που περιέχουν δεδομένα προσωπικού χαρακτήρα.
- ...

Επίπεδο 4: Πηγές Κινδύνων (26/41)

25. Παραβίαση δεδομένων λόγω οργανωτικών ζητημάτων.

- Μη ανώνυμα δεδομένα χαρακτηρίζονται λανθασμένα ως ανώνυμα (π.χ. δημοσίευση «πλούσιων» συνόλων δεδομένων με πολλά ψευδο-αναγνωριστικά (quasi-identifiers)).
- Μη ορθή καταστροφή δεδομένων ή επαναχρησιμοποίηση υλικού (hardware) (π.χ. σκληροί δίσκοι/φορητοί υπολογιστές με προσωπικά δεδομένα επαναχρησιμοποιούνται χωρίς διαγραφή/καθαρισμό των δεδομένων) .
- Οι εκτελούντες την επεξεργασία δεδομένων (π.χ. πάροχοι υπηρεσιών μισθοδοσίας, ανάλυσης δεδομένων, υπολογιστικού νέφους) υφίστανται παραβίαση, εκθέτοντας τα κοινόχρηστα προσωπικά δεδομένα.
- ...

Επίπεδο 4: Πηγές Κινδύνων (27/41)

26. Κρυφή παρακολούθηση στο χώρο εργασίας (επικοινωνίες, αρχεία καταγραφής, υπολογιστές κ.α.)

- Κρυφή παρακολούθηση της θέσης του χρήστη (π.χ. χρήση δεδομένων GPS για σκοπό που δεν είναι γνωστός στον χρήστη).
- Κρυφή παρακολούθηση των δραστηριοτήτων του εργαζομένου (π.χ. διαδικτυακή περιήγηση του εργαζομένου).
- Αδικοιολόγητος έλεγχος των μεταδεδομένων τηλεφωνικών κλήσεων των εργαζομένων.
- Αδικοιολόγητος έλεγχος των μεταδεδομένων των ηλεκτρονικών μηνυμάτων των εργαζομένων.
- ...

Επίπεδο 4: Πηγές Κινδύνων (28/41)

27. Δεν υπάρχει μηχανισμός για την εξασφάλιση της συγκατάθεσης των χρηστών (αν και απαιτείται συγκατάθεση)

- Χρήση ιχνηλατών τρίτων παρόχων και/ή cookies τα οποία δεν είναι απαραίτητα για την παροχή της υπηρεσίας χωρίς ενημέρωση.
- Χρήση ιχνηλατών τρίτων παρόχων και/ή μη απαραίτητων cookies με προ-επιλεγμένο το πλαίσιο συγκατάθεσης (opt-out).
- Απαίτηση μίας ενιαίας συγκατάθεσης για περισσότερους από έναν διαφορετικούς σκοπούς (π.χ. ομαδοποιημένη συγκατάθεση).
- Κατάρτιση προφίλ ή λήψη αυτοματοποιημένων αποφάσεων χωρίς μηχανισμό λήψης συγκατάθεσης (σε περιπτώσεις που αυτή είναι η μόνη νομική βάση).
- ...

Επίπεδο 4: Πηγές Κινδύνων (29/41)

28. Παραπλανητικά μοτίβα στη συλλογή της συγκατάθεσης.

- Παραπλανητικές πληροφορίες σχετικά με το αν ο χρήστης είναι ελεύθερος να συναινέσει ή όχι.
- Η «αναγκαστική» συγκατάθεση —δηλαδή εκπτώσεις, πόντοι επιβράβευσης κτλ. - παρέχονται μόνο εάν ο χρήστης συμφωνεί να υποβάλει πρόσθετα δεδομένα προσωπικού χαρακτήρα που δεν σχετίζονται με την υπηρεσία.
- Οι διεπαφές με το χρήστη όσον αφορά τη συγκατάθεση έχουν σχεδιαστεί με διατύπωση όπως «Ενίσχυση της εμπειρίας σας», ώστε οι χρήστες να προτρέπονται στο να συμφωνούν με την υπερβολική συλλογή δεδομένων.
- ...

Επίπεδο 4: Πηγές Κινδύνων (30/41)

29. Τεχνικές αστοχίες όσον αφορά την ενεργοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων

- Τα δεδομένα που ζητούνται από τα υποκείμενα των δεδομένων δεν εξάγονται λόγω τεχνικών αδυναμιών.
- Τα δεδομένα είναι κατανεμημένα σε διάφορα συστήματα ή αρχεία καταγραφής με τρόπους που εμποδίζουν την αποτελεσματική ικανοποίησης των αιτημάτων.
- Έλλειψη κατάλληλου χειρισμού αυθεντικοποίησης χρηστών όταν υποβάλουν αιτήματα (άρνηση νόμιμων αιτημάτων).
- Τα δεδομένα δεν μπορούν να εντοπιστούν ή να αφαιρεθούν μεταξύ των συστημάτων λόγω τεχνικών δυσκολιών.
- ...

Επίπεδο 4: Πηγές Κινδύνων (31/41)

30. Μη (ορθή) ενημέρωση των υποκειμένων των δεδομένων σχετικά με τα δικαιώματά τους.

- Ο ιστότοπος δεν διαθέτει πολιτική προστασίας δεδομένων.
- Τα έντυπα που καλούνται να συμπληρώσουν τα υποκείμενα των δεδομένων δεν περιέχουν καμία αναφορά στα δικαιώματα που έχουν.
- Οι χρήστες δεν ενημερώνονται όταν αλλάζουν οι πολιτικές.
- Οι όροι της σύμβασης με το υποκείμενο των δεδομένων δεν είναι πλήρεις.
- ...

Επίπεδο 4: Πηγές Κινδύνων (32/41)

31. Συστημικές και οργανωτικές αποτυχίες στη διασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων .

- Χρήση στοιχείων/συστατικών ΤΝ κλειστού κώδικα ή προερχόμενων από τρίτους παρόχους, χωρίς πρόσβαση στην εσωτερική λογική λειτουργίας τους *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα)*.
- Τα αιτήματα απαντώνται με αδικαιολόγητη καθυστέρηση.
- Οι εκτελούντες την επεξεργασία δεν συμβάλλουν στην ικανοποίηση των αιτημάτων των χρηστών (π.χ. διαγραφή).
- Τα υποκείμενα των δεδομένων καλούνται να ακολουθήσουν μια πολύπλοκη διαδικασία για την άσκηση των δικαιωμάτων τους.
- ...

Επίπεδο 4: Πηγές Κινδύνων (33/41)

32. Μη ορθή χρήση αλγορίθμων για την κατάρτιση προφίλ/ αυτοματοποιημένη λήψη αποφάσεων.

- Χρήση αλγορίθμων που ενδέχεται να παράγουν εσφαλμένα αποτελέσματα (π.χ. μεροληπτικοί αλγόριθμοι που επιτρέπουν διακρίσεις).
- Οι χρήστες δεν έχουν σαφή ή προσβάσιμο τρόπο να αντιταχθούν στην κατάρτιση προφίλ ή να ζητήσουν ανθρώπινη επανεξέταση μιας απόφασης.
- Δεν υπάρχει μηχανισμός για την λήψη συγκατάθεσης για κατάρτιση προφίλ ή λήψη αυτοματοποιημένων αποφάσεων (σε περιπτώσεις που αυτή είναι η μόνη νομική βάση).
- ...

Επίπεδο 4: Πηγές Κινδύνων (34/41)

33. Κατάρτιση προφίλ για σκοπούς μάρκετινγκ/ ανάλυσης δεδομένων χωρίς νομική βάση.

- Τα δεδομένα που συλλέχθηκαν αρχικά για την παροχή υπηρεσιών χρησιμοποιούνται αργότερα από το σύστημα για στοχευμένη διαφήμιση ή ανάλυση δεδομένων χωρίς να επικαιροποιείται η νομική βάση ή να ενημερώνονται οι χρήστες.
- Χρήση βιβλιοθηκών τρίτων παρόχων που συλλέγουν δεδομένα για δικούς τους σκοπούς, τα οποία χρησιμοποιούνται από συστήματα.
- ...

Επίπεδο 4: Πηγές Κινδύνων (35/41)

34. Συστηματική παρακολούθηση των δραστηριοτήτων των υπαλλήλων.

- Συλλογή υπερβολικών δεδομένων (π.χ. πλήρες ιστορικό περιήγησης) χωρίς νόμιμο σκοπό που να συνδέεται με υποχρεώσεις απασχόλησης.
- Αδικοιολόγητος έλεγχος των μεταδεδομένων τηλεφωνικών κλήσεων των εργαζομένων.
- Αδικοιολόγητος έλεγχος των μεταδεδομένων των ηλεκτρονικών μηνυμάτων των εργαζομένων.
- Κρυφή παρακολούθηση της θέσης του χρήστη (π.χ. χρήση δεδομένων GPS για σκοπό που δεν είναι γνωστός στον χρήστη).
- ...

Επίπεδο 4: Πηγές Κινδύνων (36/41)

35. Κατάχρηση συστημάτων αναγνώρισης (π.χ. προσώπου, πινακίδες αυτοκίνητου κλπ.) *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*

- Ανάπτυξη συστημάτων αναγνώρισης (σε δημόσιους χώρους) χωρίς νομική βάση.
- Κρυφή χρήση συστημάτων αναγνώρισης.
- Χρήση συστήματος ταυτοποίησης για σκοπούς αναγνώρισης προσώπου βάσει δεδομένων που είναι δημοσίως διαθέσιμα (π.χ. στο διαδίκτυο) χωρίς νομική βάση.
- Ενσωμάτωση/διασύνδεση συστημάτων αναγνώρισης με άλλα συστήματα, όπως π.χ. συστήματα CCTV χωρίς νομική βάση.

Επίπεδο 4: Πηγές Κινδύνων (37/41)

36. Χρήση δεδομένων εκπαίδευσης χαμηλής ποιότητας (όχι ακριβή, εκτός πεδίου εφαρμογής κ.λπ.) *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*

- Επαναχρησιμοποίηση συνόλων δεδομένων για εκπαίδευση από διαφορετικούς τομείς/πλαίσια.
- Τα σύνολα δεδομένων που χρησιμοποιούνται για την εκπαίδευση δεν είναι αντιπροσωπευτικά.
- Μη ορθή επισήμανση στα δεδομένα που χρησιμοποιούνται για την εκπαίδευση.
- «Μόλυνση» δεδομένων, δηλ. ακούσια συμπερίληψη ακατάλληλων ή παραπλανητικών δεδομένων κατά τη διάρκεια των φάσεων εκπαίδευσης, επικύρωσης ή δοκιμής
-

Επίπεδο 4: Πηγές Κινδύνων (38/41)

37. Μεροληψία στα δεδομένα εκπαίδευσης *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).*

- Μεροληψία που εισάγεται στην προεπεξεργασία (pre-processing) δεδομένων.
- Μεροληψία στην επισήμανση (labeling) δεδομένων εκπαίδευσης (λόγω, π.χ., ανθρώπινου σφάλματος).
- Χρήση συνθετικών δεδομένων για εκπαίδευση που δεν αντικατοπτρίζουν την πραγματικότητα.
- ...

Επίπεδο 4: Πηγές Κινδύνων (39/41)

38. Μεροληψία του μοντέλου TN *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*

- Εσφαλμένη προδιαγραφή του μοντέλου λόγω υπερπροσαρμογής (overfitting).
- Εσφαλμένη προδιαγραφή του μοντέλου λόγω υποπροσαρμογής (underfitting).
- Ανισορροπία κλάσεων (class imbalance) λόγω σφαλμάτων στο μοντέλο (π.χ. απουσία στάθμισης ή εξισορρόπησης κατά την εκπαίδευση).
- Μεροληψία που προκύπτει από ενισχυτική μάθηση (reinforcement learning).
- ...

Επίπεδο 4: Πηγές Κινδύνων (40/41)

39. Η είσοδος στα συστήματα ΤΝ επηρεάζεται από κακόβουλες επιθέσεις (adversarial attacks)* *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).*

- Έκθεση σε επιθέσεις «Jailbreaking» (δηλαδή χειραγώγηση ή εκμετάλλευση ενός συστήματος ΤΝ ώστε να εκτελεί ενέργειες ή να παράγει περιεχόμενο που έχει σχεδιαστεί ρητά να αποφεύγει, όπως π.χ. η διάδοση τοξικού περιεχομένου), λόγω έλλειψης κατάλληλων προστατευτικών μέτρων.
- Κακόβουλη «δηλητηρίαση» δεδομένων (data poisoning) (π.χ. για την ενσωμάτωση εκμεταλλεύσιμων κερκόπορτων) λόγω έλλειψης σχετικών προστατευτικών μέτρων.
- Επιθέσεις έγχυσης προτροπών (prompt injection), για LLM, λόγω έλλειψης σχετικών προστατευτικών μέτρων.
- ...

Επίπεδο 4: Πηγές Κινδύνων (41/41)

40. Εσφαλμένη εκτίμηση ως προς τη συμβατότητα νέου σκοπού επεξεργασίας με τον αρχικό

- Τα δεδομένα κοινοποιούνται σε διαφημιστικά δίκτυα, παρόχους υπηρεσιών ανάλυσης δεδομένων κ.λπ. χωρίς να λαμβάνεται έγκυρη συγκατάθεση.
- Τα προσωπικά δεδομένα αναλύονται για να συναχθούν οι προτιμήσεις ή η συμπεριφορά των χρηστών (προφίλ) για διαφημιστικούς σκοπούς χωρίς έγκυρη συγκατάθεση.
- Θεώρηση ότι η ευρεία ή γενική συγκατάθεση που ελήφθη αρχικά είναι επαρκής για κάθε νέα δραστηριότητα επεξεργασίας.
- ...

Κανονιστικά Ζητήματα Συσχετισμένα με τις Πηγές Κινδύνων

Έλλειψη σαφούς
ενημέρωσης και
διαφάνειας

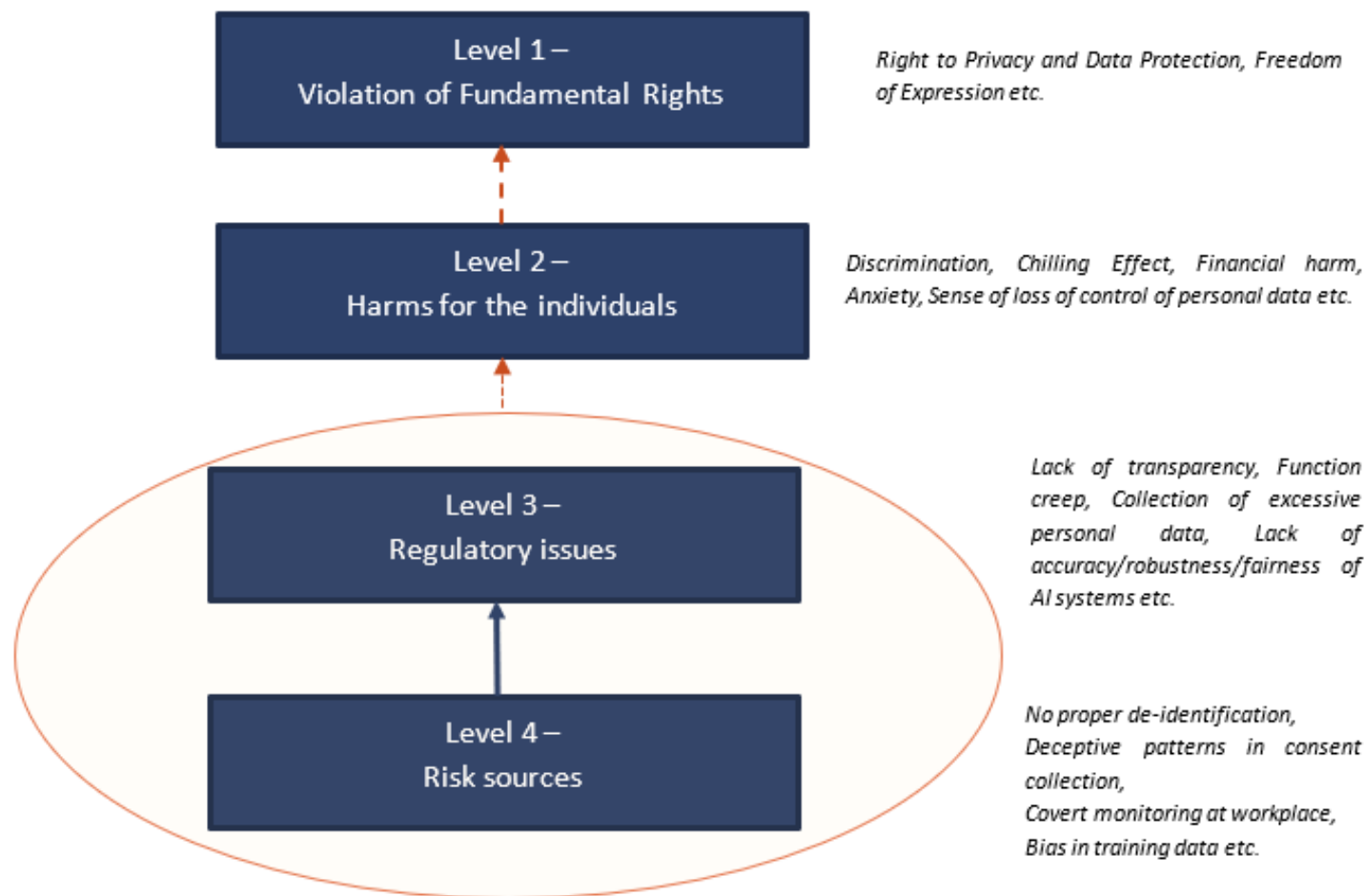
- SR-1 Έλλειψη πληροφόρησης σχετικά με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- SR-2 Ασαφή, πολύ γενικά ή πολύ σύνθετα κείμενα ενημερώσεων.
-

Έλλειψη συγκατάθεσης ή
άλλης νομικής βάσης

- SR-5 Χρήση των δεδομένων του πελάτη/χρήστη για στοχευμένη διαφήμιση.
- SR-6 Χρήση των δεδομένων των εργαζομένων για αξιολόγηση χωρίς νομική βάση.
- ...

Κατηγορίες	Συμπεριλαμβανόμενες πηγές κινδύνου
1. Έλλειψη σαφούς ενημέρωσης και διαφάνειας	SR-1, SR-2, SR-3, SR-4, SR-30
2. Έλλειψη συγκατάθεσης ή άλλης νομικής βάσης	SR-5, SR-6, SR-7, SR-8, SR-9, SR-10, SR-13, SR-14, SR-27, SR-28, SR-40
3. Υπερβολική ή/και μη αναγκαία συλλογή δεδομένων	SR-11, SR-12, SR-15, SR-16, SR-17
4. Προβλήματα χρήσης Τεχνητής Νοημοσύνης και σχετικών δεδομένων	SR-18, SR-19, SR-20, SR-35, SR-36, SR-37, SR-38, SR-39
5. Ασφάλεια δεδομένων και περιστατικά παραβίασης	SR-21, SR-22, SR-23, SR-24, SR-25
6. Παρακολούθηση ή/και δημιουργία προφίλ	SR-26, SR-32, SR-33, SR-34
7. Μη αποτελεσματική διασφάλιση των δικαιωμάτων των φυσικών προσώπων	SR-29, SR-31

Συνοψίζοντας την Ταξινόμηση

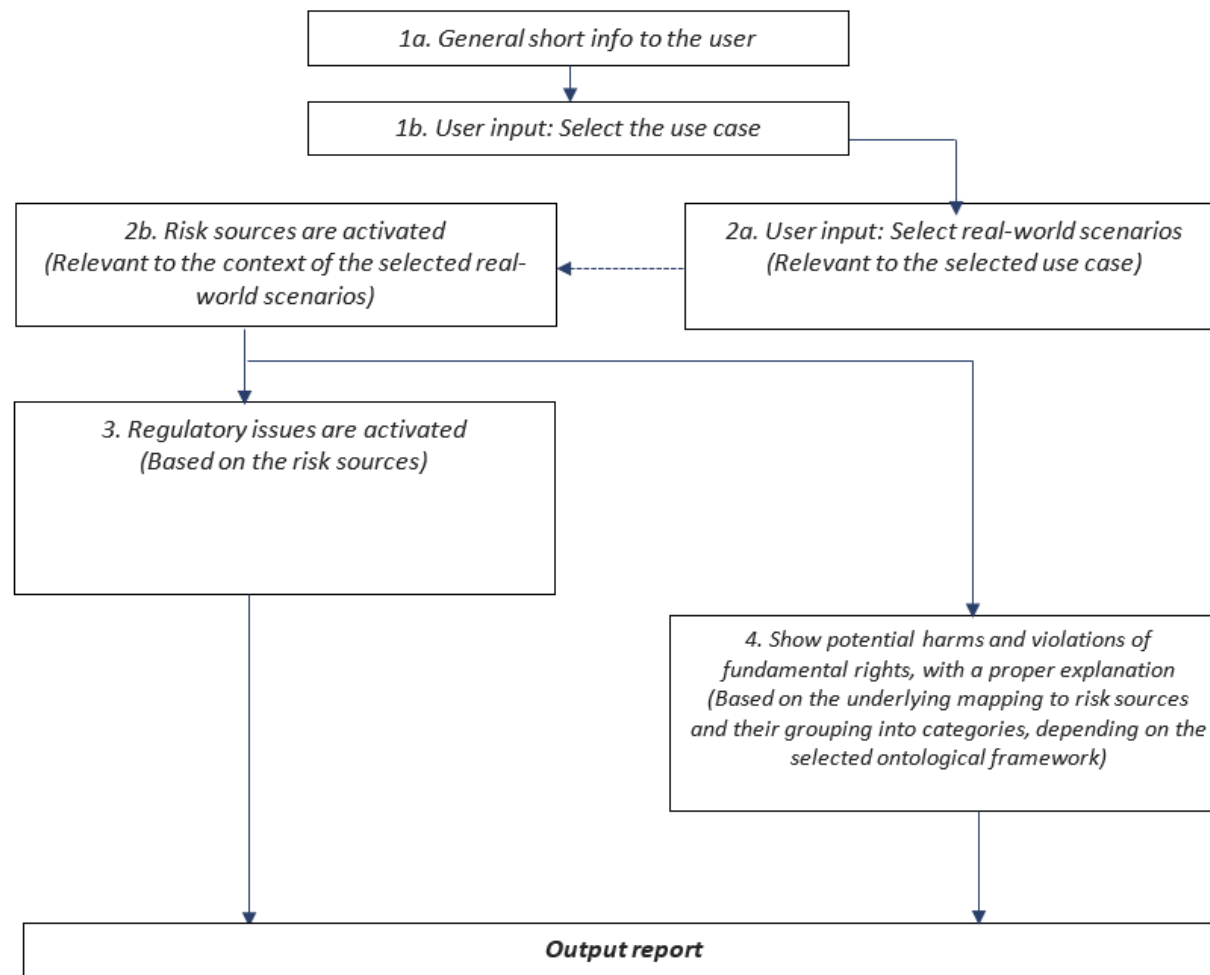


Εργαλείο Ευαισθητοποίησης Σχετικά με τον Κίνδυνο

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

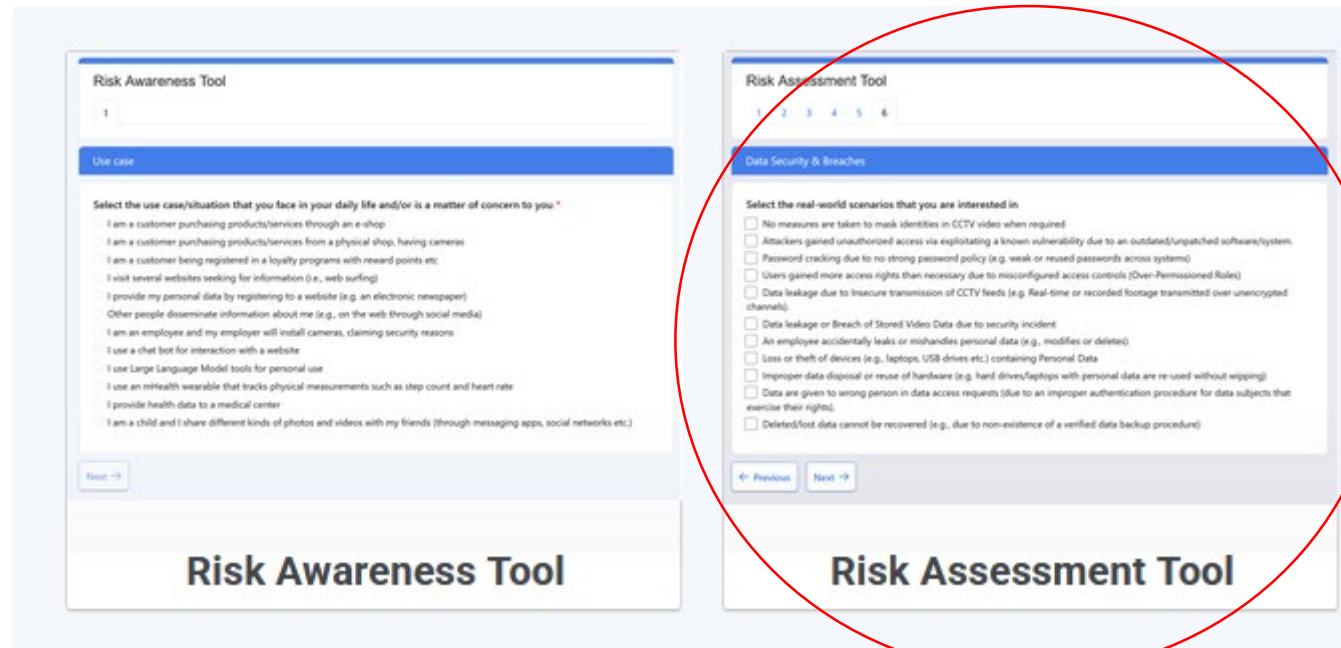
- Παρέχει μία σαφή και έγκυρη καταγραφή των διαφορετικών κινδύνων στα δικαιώματα και τις ελευθερίες του ευρέος κοινού.
- Παρουσιάζει τις πιθανές επιπτώσεις οι οποίες μπορούν να προκληθούν από κάθε έναν από τους προαναφερθέντες κινδύνους και, άρα, αναδεικνύεται και η σημασία τους.

Ροή των Διαδικασιών



Το εργαλείο byRisk στην πράξη

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



The screenshot displays two side-by-side web forms. The left form is titled 'Risk Awareness Tool' and contains a list of use cases for selection. The right form is titled 'Risk Assessment Tool' and contains a list of real-world scenarios for selection. The right form is circled in red.

Risk Awareness Tool

1

Use case

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

1 2 3 4 5 6

Data Security & Breaches

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 Roles)
- ☐ 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.....