



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/>)





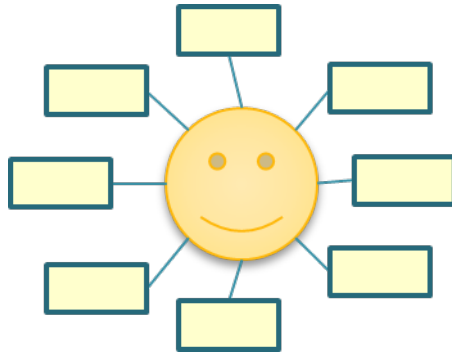
Πριν ξεκινήσουμε μερικά διαχειριστικά θέματα...



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 είναι 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

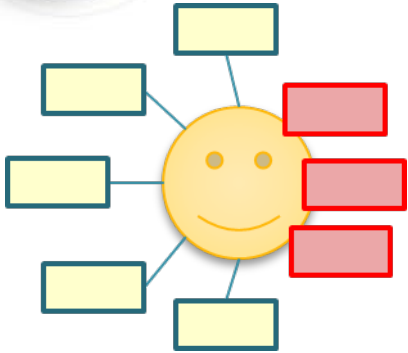


Π.χ. προσωπικά δεδομένα: όνομα και επώνυμο, αριθμός ταυτότητας, διεύθυνση κατοικίας, ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com, αναγνωριστικός αριθμός κάρτας, δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο), διεύθυνση δικτύου συσκευής χρήστη (IP address),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

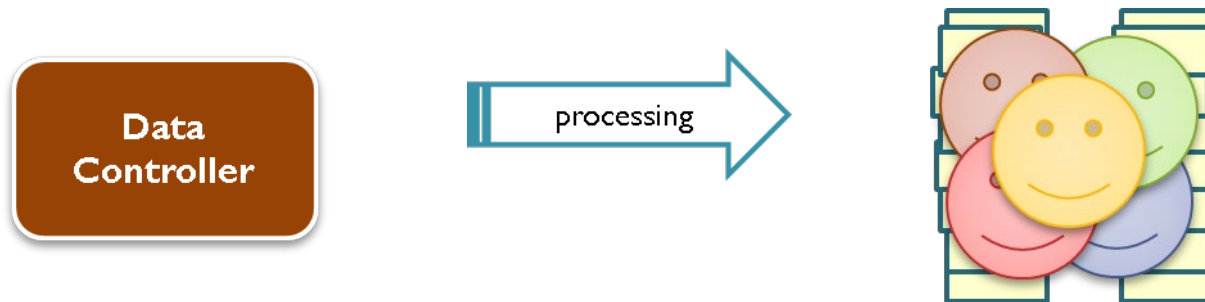
Ωστόσο, το εάν κάποιο identifier μπορεί να αναγνωρίσει ένα φυσικό πρόσωπο εξαρτάται από το πλαίσιο.

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’;



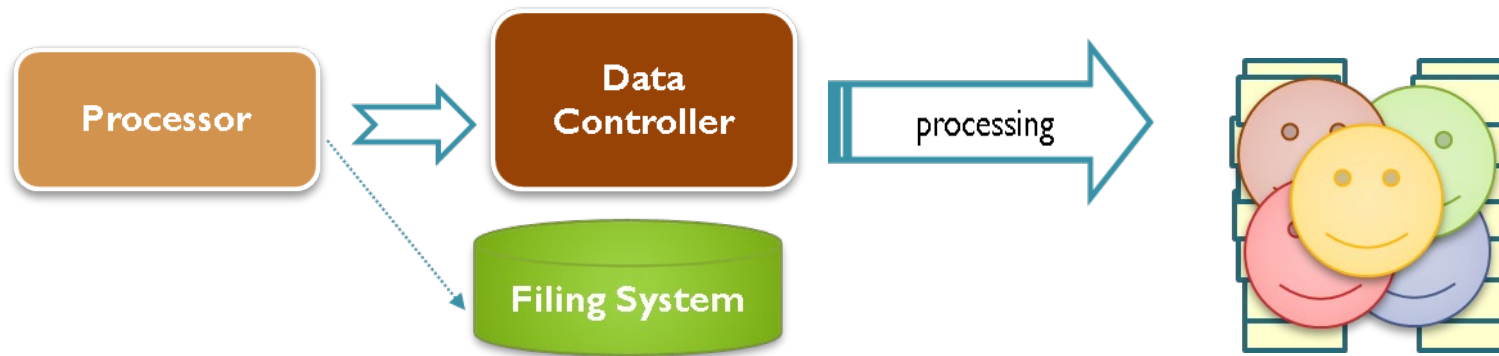
Ο υπεύθυνος επεξεργασίας είναι αυτός ο οποίος **αποφασίζει πώς και γιατί να συλλεχθούν και να χρησιμοποιηθούν τα δεδομένα**. Αυτό συνήθως είναι ένας οργανισμός , αλλά μπορεί να είναι και ένα φυσικό πρόσωπο (π.χ. ένας έμπορος, ένας γιατρός, ένας δικηγόρος κλπ.).

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

Συλλέγονται 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.

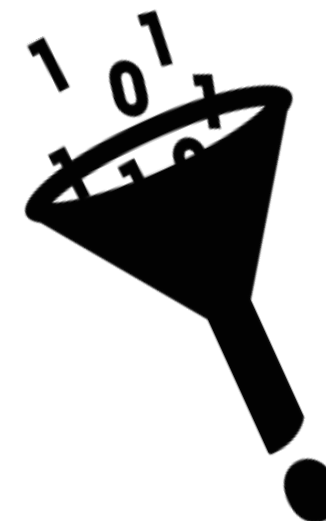
iii. Ελαχιστοποίηση των Δεδομένων

‘Επαρκής, σχετική και περιορισμένη η συλλογή των δεδομένων σε ό,τι 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.

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 παραβίασης δεδομένων.

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.

Η έννοια του κινδύνου στην προστασία δεδομένων

- Ο GDPR ακολουθεί μια προσέγγιση βασισμένη στον κίνδυνο (risk-based approach), χωρίς όμως να ορίζει με σαφήνεια την έννοια του κινδύνου.
- Υιοθετείται μια από τις δύο προηγούμενες ερμηνείες του κινδύνου και αξιολογείται με βάση το πιθανό συμβάν, τον τρόπο με τον οποίο μπορεί να συμβεί και τις επιπτώσεις του.
- Ο κίνδυνος δεν αφορά μόνο το αν θα συμβεί ένα γεγονός, αλλά και πόσο σοβαρές θα είναι οι συνέπειές του

Κίνδυνος στην ασφάλεια πληροφοριών και στον GDPR

- Ασφάλεια Πληροφοριών:
 - Εστίαση σε απειλές κατά:
 - Εμπιστευτικότητας (Confidentiality)
 - Ακεραιότητας (Integrity)
 - Διαθεσιμότητας (Availability)
 - Οι επιπτώσεις αξιολογούνται κυρίως για τον οργανισμό (π.χ. οικονομική ζημία, απώλεια φήμης)
- GDPR:
 - Η αξιολόγηση αφορά κυρίως τους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων
 - διακρίσεις, κλοπή ταυτότητας, οικονομική ζημία, βλάβη της φήμης, περιορισμός θεμελιωδών δικαιωμάτων.
- Στο GDPR το επίκεντρο δεν είναι ο οργανισμός αλλά ο πολίτης.

Κίνδυνος στο AI Act

- Ορίζει τον κίνδυνο ως
Πιθανότητα πρόκλησης βλάβης × Σοβαρότητα της βλάβης
- Οι κίνδυνοι αφορούν
 - υγεία,
 - ασφάλεια,
 - θεμελιώδη δικαιώματα,
 - δημοκρατικές αξίες

Εκτίμηση Επιπτώσεων

- Διεθνώς χρησιμοποιούνται:
 - Data Protection Impact Assessment (DPIA)
 - Fundamental Rights Impact Assessment (FRIA)
 - Ethical Impact Assessment (EIA)
 - Surveillance Impact Assessment
 - Algorithmic Impact Assessment
- Η αξιολόγηση κινδύνου πρέπει να εξετάζει όχι μόνο την προστασία δεδομένων, αλλά και τις ευρύτερες κοινωνικές και ηθικές επιπτώσεις των τεχνολογιών

Περιορισμοί των υφιστάμενων προσεγγίσεων

- Εστίαση στην παραβίαση νομικών απαιτήσεων του GDPR αντί στις πραγματικές επιπτώσεις για τα άτομα.
- Υπερβολική έμφαση στην ασφάλεια πληροφοριών, με περιορισμένη κάλυψη άλλων αρχών (π.χ. ελαχιστοποίηση δεδομένων).
- Τα εργαλεία DPIA και FRIA είναι συχνά πολύπλοκα, σχεδιασμένα για περιπτώσεις υψηλού κινδύνου, δύσκολα στην εφαρμογή από ΜΜΕ.
- Η αναγνώριση κινδύνων από συστήματα Τεχνητής Νοημοσύνης είναι ιδιαίτερα δύσκολη, καθώς οι χρήστες (ιδίως οι ΜΜΕ) συχνά δεν γνωρίζουν πλήρως τον τρόπο λειτουργίας των μοντέλων ΑΙ.
- Απαιτούνται πιο απλές, πρακτικές και ανθρωποκεντρικές μεθοδολογίες αξιολόγησης κινδύνου, που να λαμβάνουν υπόψη όχι μόνο την ασφάλεια των δεδομένων αλλά και τις επιπτώσεις στα θεμελιώδη δικαιώματα και στις αξίες της κοινωνίας

Διερεύνηση των αναγκών των ΜΜΕ

Στόχος της έρευνας ήταν να κατανοηθεί κατά πόσο οι ελληνικές ΜΜΕ:

- ✓ αναγνωρίζουν τους κινδύνους προστασίας προσωπικών δεδομένων
- ✓ εφαρμόζουν διαδικασίες αξιολόγησης κινδύνου
- ✓ χρησιμοποιούν εργαλεία ή μεθοδολογίες εκτίμησης κινδύνου
- ✓ χρησιμοποιούν ή σχεδιάζουν να χρησιμοποιήσουν εφαρμογές Τεχνητής Νοημοσύνης
- ✓ χρειάζονται νέα εργαλεία υποστήριξης για την αναγνώριση και αξιολόγηση κινδύνων

Μεθοδολογία

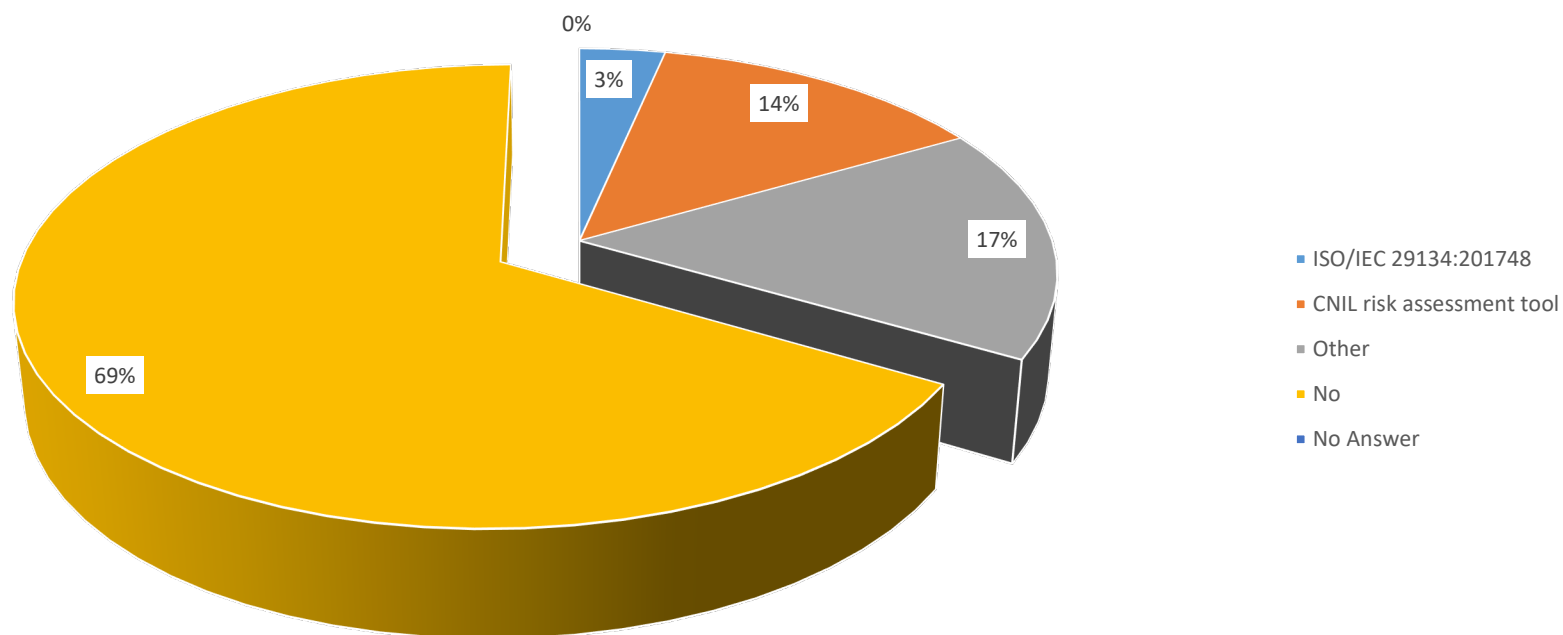
- Ηλεκτρονικό ερωτηματολόγιο (EU Survey)
- Ανώνυμη συμμετοχή
- 29 επιχειρήσεις
- Επιλεγμένοι κλάδοι υψηλού ενδιαφέροντος:
 - Τουρισμός
 - Εκπαίδευση
 - Λιανικό εμπόριο
 - Εστίαση
 - Υγεία
 - Υπηρεσίες Πληροφορικής

Βασικές Θεματικές του Ερωτηματολογίου

- 1 Προφίλ της επιχείρησης (μέγεθος, κλάδος δραστηριότητας)
- 2 Επεξεργασία προσωπικών δεδομένων (σκοποί επεξεργασίας, δραστηριότητες υψηλού κινδύνου)
- 3 Αναγνώριση κινδύνων (στάδια επεξεργασίας, εργαλεία αξιολόγησης, αιτίες κινδύνων)
- 4 Κίνδυνοι για τα θεμελιώδη δικαιώματα (διακρίσεις, οικονομική ζημία, απώλεια ελέγχου, παραβίαση προσωπικότητας)
- 5 Τεχνητή Νοημοσύνη (χρήση AI, κίνδυνοι, διαφάνεια, bias, ανθρώπινη εποπτεία)
- 6 Ανάγκες των ΜΜΕ (χαρακτηριστικά ενός αποτελεσματικού εργαλείου αξιολόγησης κινδύνου)

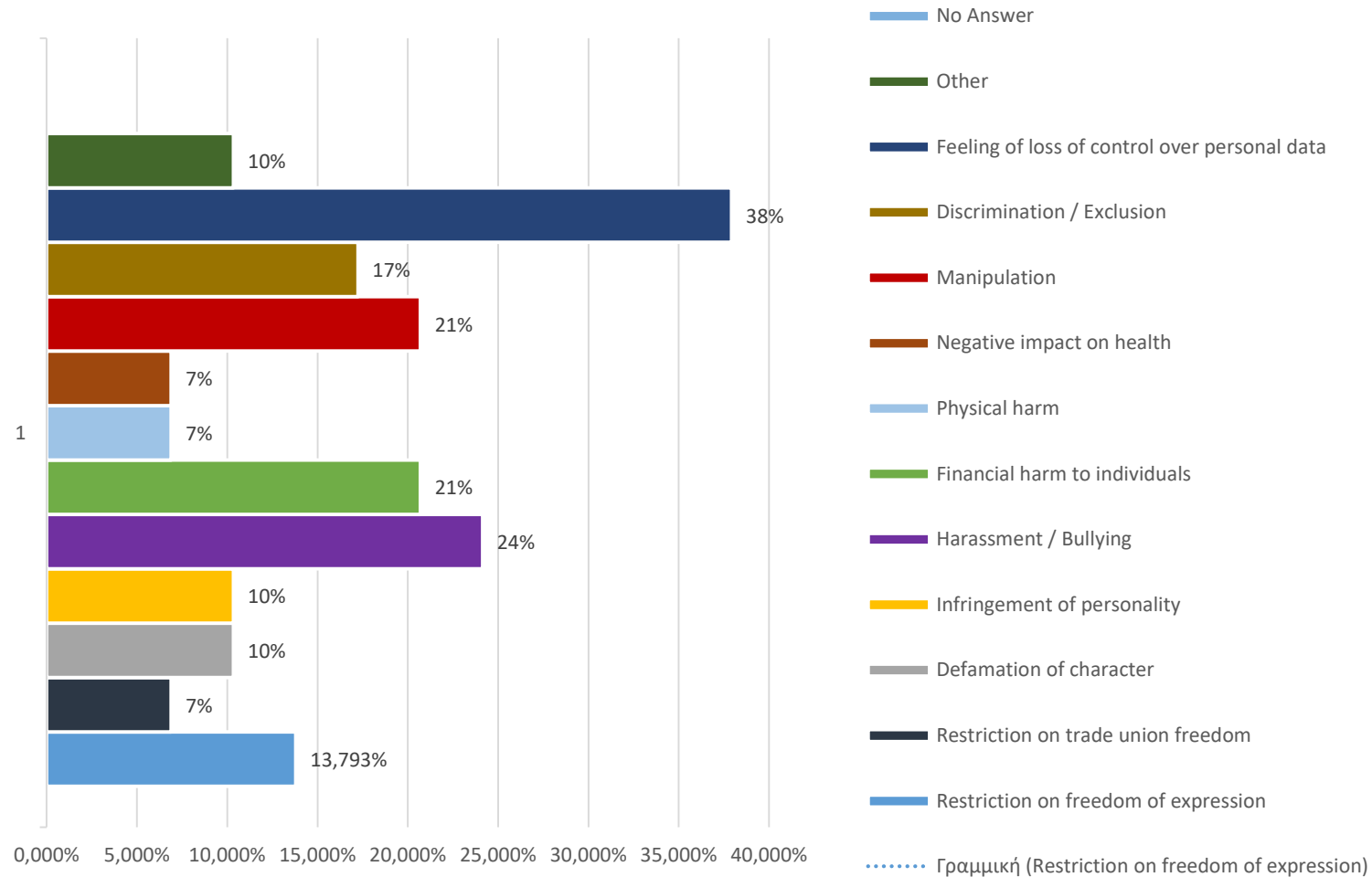
Ενδεικτικά αποτελέσματα....

Risk Analysis Tools usage



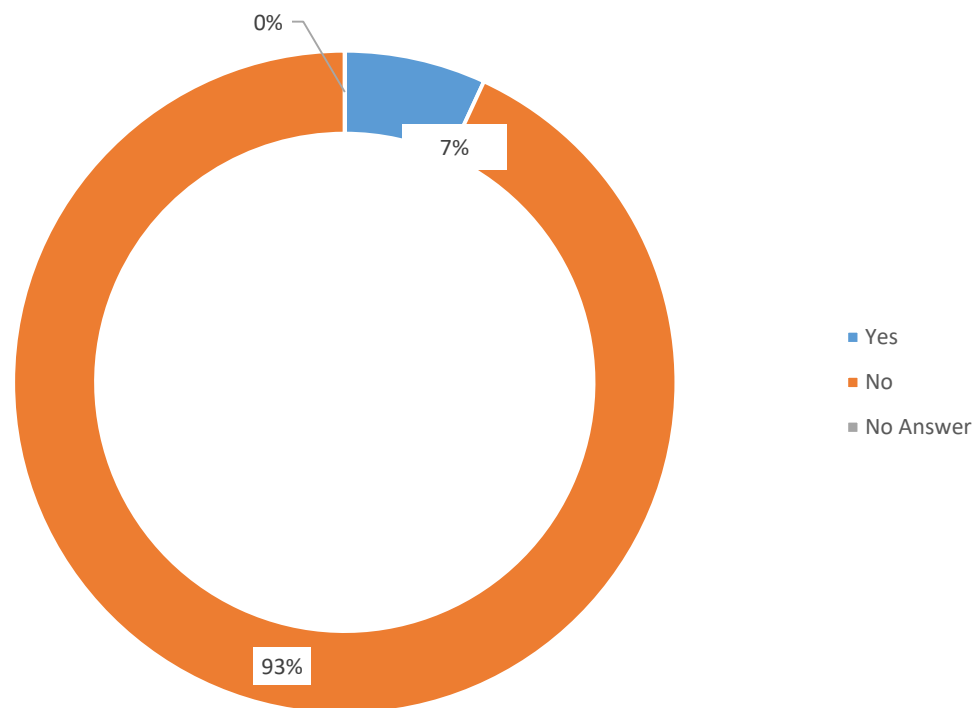
Ενδεικτικά αποτελέσματα.....

Risks to the rights and freedoms for which a concern is identified

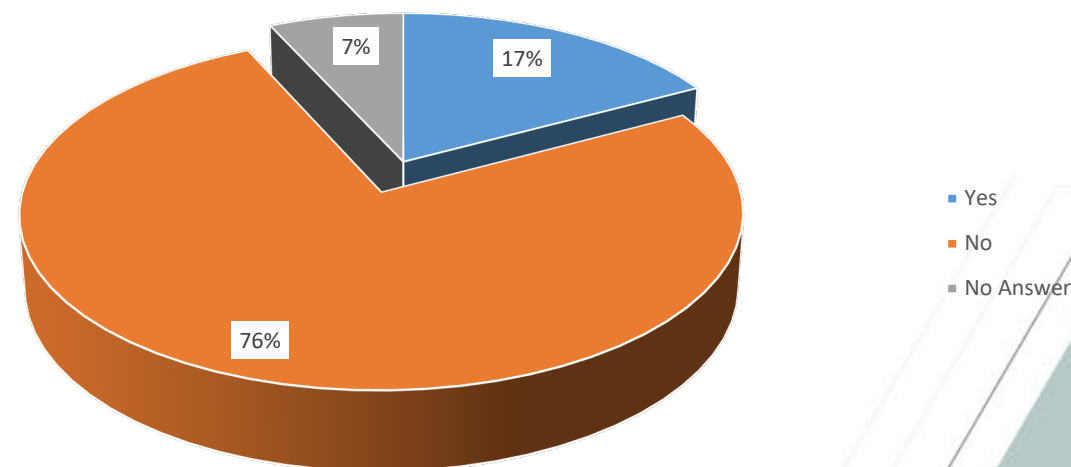


Ενδεικτικά αποτελέσματα.....

AI application usage

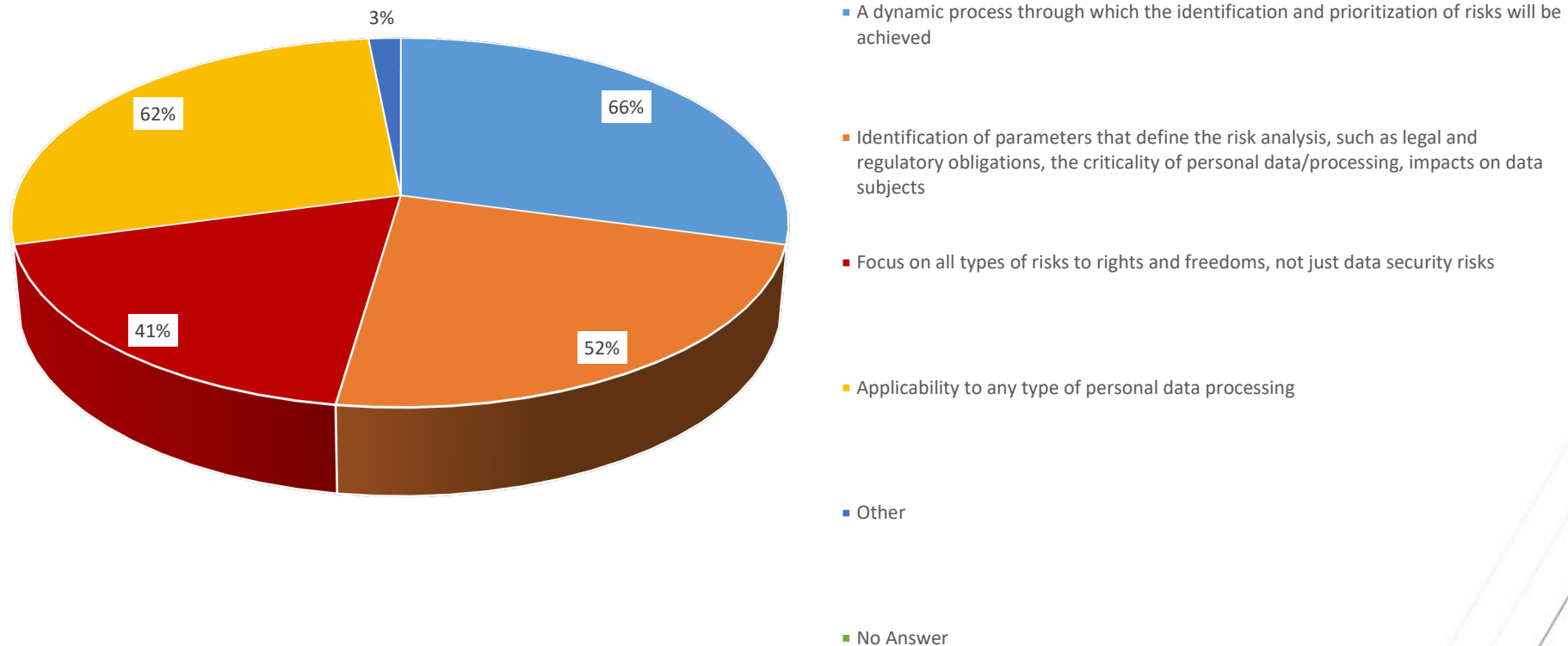


Consideration on usage of AI application



Ενδεικτικά αποτελέσματα.....

Risk identification tool main characteristic



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



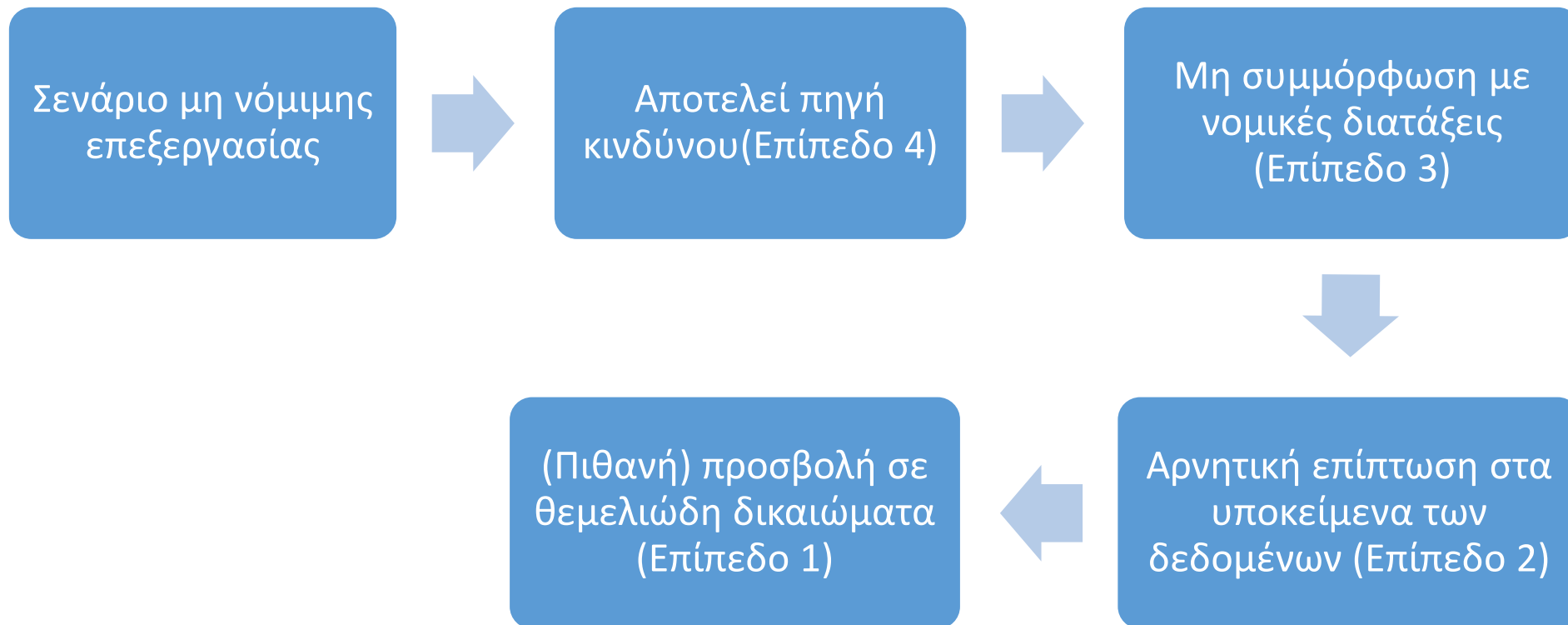
Επίπεδο 3: Μη συμμόρφωση με το κανονιστικό πλαίσιο



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)

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 αντιστοίχισή 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 (1/17)

- 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 (2/17)

Οι πηγές κινδύνου έχουν οργανωθεί σε 7 κατηγορίες για την καλύτερη κατανόηση και δόμηση τους.

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 έγκυρης 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

Επίπεδο 4: Πηγές Κινδύνων (3/17)

1) Έλλειψη σαφούς ενημέρωσης και διαφάνειας

- Έλλειψη πληροφόρησης σχετικά με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- Ασαφή, πολύ γενικά ή πολύ σύνθετα κείμενα ενημερώσεων.
- Χρήση αδιαφανών μοντέλων ΤΝ που δεν παρέχουν πληροφορίες σχετικά με τον τρόπο με τον οποίο οι είσοδοι μετατρέπονται σε εξόδους *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα)*.
- Απουσία ερμηνευσιμότητας *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα)*.
- Μη (ορθή) ενημέρωση των υποκειμένων των δεδομένων σχετικά με τα δικαιώματά τους

Επίπεδο 4: Πηγές Κινδύνων (4/17)

Παραδείγματα που αντιστοιχούν στην κατηγορία «Έλλειψη σαφούς ενημέρωσης και διαφάνειας»:

- Κρυφή παρακολούθηση των δραστηριοτήτων του εργαζομένου (π.χ. περιήγηση του εργαζομένου).
- Κρυφή παρακολούθηση της θέσης του χρήστη (π.χ. χρήση δεδομένων GPS για σκοπό που δεν είναι γνωστός στον χρήστη).
- Πολιτικές γραμμένες από νομικά τμήματα που χρησιμοποιούν σε μεγάλο βαθμό νομικούς όρους, χωρίς απλή γλώσσα.
- Χρήση της ίδιας πολιτικής για διαφορετικά προϊόντα/διαδικασίες με διαφορετικές επεξεργασίες δεδομένων.
- Ανεπαρκής τεκμηρίωση σχετικά με τον σχεδιασμό μοντέλων, τις διαδικασίες εκπαίδευσης και τις παραδοχές στις οποίες αυτό βασίζεται.
- Ο ιστότοπος δεν διαθέτει πολιτική προστασίας δεδομένων.
- Οι όροι της σύμβασης με το υποκείμενο των δεδομένων δεν είναι πλήρεις.

Επίπεδο 4: Πηγές Κινδύνων (5/17)

2) Έλλειψη συγκατάθεσης ή άλλης έγκυρης νομικής βάσης

- Χρήση των δεδομένων του πελάτη / χρήστη για στοχευμένη διαφήμιση.
- Χρήση των δεδομένων των εργαζομένων για αξιολόγηση χωρίς νομική βάση.
- Κοινοποίηση δεδομένων σε τρίτους χωρίς εκ νέου προσδιορισμό του σκοπού και χωρίς νομική βάση.
- Μη ανανέωση της συγκατάθεσης για τον νέο σκοπό (για τον οποίο απαιτείται νέα συγκατάθεση)
- 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).*
- Ένα μοντέλο ΤΝ που έχει εκπαιδευτεί για ένα πλαίσιο επαναχρησιμοποιείται σε άλλο *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).*

Επίπεδο 4: Πηγές Κινδύνων (6/17)

- Έλλειψη σχεδιασμού συλλογής δεδομένων για συγκεκριμένο σκοπό.
- Συλλογή δεδομένων χωρίς ειδική συγκατάθεση ή δυνατότητα εξαίρεσης.
- Δεν υπάρχει μηχανισμός για την εξασφάλιση της συγκατάθεσης των χρηστών (αν και απαιτείται συγκατάθεση).
- Παραπλανητικά μοτίβα στη συλλογή συγκατάθεσης.
- Εσφαλμένη εκτίμηση ως προς τη συμβατότητα νέου σκοπού επεξεργασίας με τον αρχικό.

Επίπεδο 4: Πηγές Κινδύνων (7/17)

Παραδείγματα που αντιστοιχούν στην έλλειψη συγκατάθεσης ή άλλης νομικής βάσης:

- Οι πολιτικές απορρήτου δεν αναφέρουν σαφώς ότι τα δεδομένα των χρηστών θα χρησιμοποιηθούν για διαφήμιση ή η χρήση αυτή είναι «κρυμμένες» σε αόριστες ή σύνθετες διατυπώσεις.
- Τα δεδομένα που συλλέχθηκαν αρχικά για διοικητικούς σκοπούς ή για σκοπούς μισθοδοσίας χρησιμοποιούνται για άλλους σκοπούς (π.χ. παρακολούθηση των επιδόσεων ή για πειθαρχικό έλεγχο) χωρίς να ενημερώνεται ο εργαζόμενος.
- Τα δεδομένα κοινοποιούνται σε διαφημιστικά δίκτυα, παρόχους ανάλυσης δεδομένων κ.λπ. χωρίς να λαμβάνεται έγκυρη συγκατάθεση.
- Θεώρηση ότι η ευρεία ή γενική συγκατάθεση που ελήφθη αρχικά είναι επαρκής για κάθε νέα δραστηριότητα επεξεργασίας.
- Κοινοποίηση δεδομένων χρηστών σε άλλους οργανισμούς για ανάπτυξη εφαρμογών τεχνητής νοημοσύνης.
- Συλλογή πρόσθετων δεδομένων που «θα μπορούσαν να είναι χρήσιμα στο μέλλον».
- Ζητείται μία συγκατάθεση για περισσότερους από έναν διαφορετικούς σκοπούς.

Επίπεδο 4: Πηγές Κινδύνων (8/17)

3) Υπερβολική ή/και μη αναγκαία συλλογή δεδομένων

- Η διάρκεια αποθήκευσης των δεδομένων δεν καθορίζεται καθόλου.
- Η διάρκεια αποθήκευσης των δεδομένων δεν είναι τεκμηριωμένη.
- Συλλογή προσωπικών πληροφοριών ταυτοποίησης χωρίς να είναι απαραίτητες.
- Επανα-ταυτοποίηση χρήστη χωρίς να είναι απαραίτητο για τον επιδιωκόμενο σκοπό.
- Μη δικαιολογημένη παρακολούθηση της τοποθεσίας ή της διαδικτυακής συμπεριφοράς.

Επίπεδο 4: Πηγές Κινδύνων (9/17)

Παραδείγματα που αντιστοιχούν σε υπερβολική ή/και μη αναγκαία συλλογή δεδομένων :

- Δεν υπάρχει χρονοδιάγραμμα/πολιτική για την περίοδο αποθήκευσης δεδομένων για διαφορετικούς τύπους δεδομένων προσωπικού χαρακτήρα.
- Δεν υπάρχει τεκμηριωμένη αιτιολόγηση για την περίοδο διατήρησης δεδομένων.
- Υπερβολική διατήρηση δεδομένων CCTV.
- Ανθρώπινο σφάλμα κατά τη μη αυτόματη διαγραφή.
- Χρήση εργαλείων αναγνώρισης προσώπου χωρίς νομική βάση.
- Χρήση δεδομένων GPS χωρίς να είναι απαραίτητα για τον επιδιωκόμενο σκοπό επεξεργασίας.
- Παρακολούθηση θέσης σε πραγματικό χρόνο με οποιοδήποτε άλλο μέσο (εκτός από δεδομένα GPS και ιχνηλάτες) χωρίς νομική βάση.

Επίπεδο 4: Πηγές Κινδύνων (10/17)

4) Προβλήματα χρήσης Τεχνητής Νοημοσύνης και σχετικών δεδομένων.

- Έλλειψη κατάλληλου σχεδιασμού για συλλογή δεδομένων για χρήση για εκπαίδευση ΤΝ μοντέλου *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).*
- Εξαγωγή συμπερασμάτων για (ενδεχομένως ευαίσθητες) προσωπικές πληροφορίες από το σύστημα ΤΝ (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 ΑΙ συστήματα).*
- Απομνημόνευση Προσωπικών Δεδομένων από το ΤΝ μοντέλο *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).*
- Κατάχρηση συστημάτων αναγνώρισης (π.χ. προσώπου, πινακίδων αυτοκινήτου κ.λπ.) *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).*
- Χρήση δεδομένων εκπαίδευσης χαμηλής ποιότητας (όχι ακριβή, εκτός πεδίου εφαρμογής κ.λπ.) *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται ΑΙ συστήματα).*

Επίπεδο 4: Πηγές Κινδύνων (11/17)

- Μεροληψία στα δεδομένα εκπαίδευσης *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*
- Μεροληψία του μοντέλου TN *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*
- Η είσοδος στα συστήματα TN επηρεάζεται από κακόβουλες επιθέσεις (adversarial attacks) *(Το θέμα αυτό ίσως παρουσιάζεται μόνο εάν χρησιμοποιούνται AI συστήματα).*

Επίπεδο 4: Πηγές Κινδύνων (12/17)

Παραδείγματα που σχετίζονται με προβλήματα χρήσης Τεχνητής Νοημοσύνης και σχετικών δεδομένων:

- Δεδομένα που εισάγουν οι χρήστες χρησιμοποιούνται και για εκπαίδευση του μοντέλου, χωρίς κατάλληλη νομική βάση.
- Αυτόματη καταγραφή των αλληλεπιδράσεων των χρηστών (π.χ. για τη βελτίωση του μοντέλου).
- Χρήση δεδομένων όπως ο καρδιακός ρυθμός ή ο αριθμός βημάτων (π.χ. από εφαρμογές) για τη συναγωγή ευαίσθητων πληροφοριών σχετικά με την υγεία των ατόμων.
- Συμπερίληψη σπάνιων/μοναδικών αρχείων στο σύνολο δεδομένων εκπαίδευσης.
- Κρυφή χρήση συστημάτων αναγνώρισης.
- Τα σύνολα δεδομένων που χρησιμοποιούνται για την εκπαίδευση δεν είναι αντιπροσωπευτικά.
- Χρήση συνθετικών δεδομένων για εκπαίδευση που δεν αντικατοπτρίζουν την πραγματικότητα.
- «Δηλητηρίαση» (poisoning) του συνόλου δεδομένων εκπαίδευσης λόγω έλλειψης σχετικών προστατευτικών μέτρων.

Επίπεδο 4: Πηγές Κινδύνων (13/17)

- 5) Ασφάλεια δεδομένων και περιστατικά παραβίασης.
- Τα δεδομένα δημοσιεύονται στο Διαδίκτυο χωρίς νομική βάση.
 - Τα δεδομένα διαμοιράζονται με άλλα άτομα, χωρίς νομική βάση.
 - Παραβίαση δεδομένων λόγω συμβάντος κυβερνοασφάλειας.
 - Παραβίαση δεδομένων λόγω ανθρώπινου παράγοντα (πέραν της περίπτωσης δημοσίευσης/κοινοποίησης δεδομένων).
 - Παραβίαση δεδομένων λόγω οργανωτικών ζητημάτων.

Επίπεδο 4: Πηγές Κινδύνων (14/17)

Παραδείγματα που σχετίζονται με ασφάλεια δεδομένων και περιστατικά παραβίασης:

- Ένας εργαζόμενος δημοσιεύει κατά λάθος προσωπικά δεδομένα (π.χ. εκ παραδρομής ή εν αγνοία του).
- Εκ παραδρομής αποστολή αλληλογραφίας με προσωπικά δεδομένα (ή με άλλα μέσα) σε λάθος παραλήπτες.
- Διαρροή ή διαγραφή δεδομένων λόγω κακόβουλου λογισμικού που εγκαθίσταται σε συσκευές/συστήματα.
- «Σπάσιμο» κωδικού πρόσβασης λόγω μη ισχυρής πολιτικής κωδικών πρόσβασης (π.χ. μη ισχυροί ή επαναχρησιμοποιημένοι κωδικοί πρόσβασης σε όλα τα συστήματα).
- Ένας υπάλληλος ανταποκρίνεται σε ηλεκτρονικό παραπλανητικό (Phishing) μήνυμα.
- Απώλεια ή κλοπή εγγράφων σε έντυπη μορφή που περιέχουν δεδομένα προσωπικού χαρακτήρα
- Μη ορθή καταστροφή δεδομένων ή επαναχρησιμοποίηση υλικού (hardware) (π.χ. «σκληροί» δίσκοι/φορητοί υπολογιστές με προσωπικά δεδομένα επαναχρησιμοποιούνται χωρίς διαγραφή/καθαρισμό των δεδομένων)

Επίπεδο 4: Πηγές Κινδύνων (15/17)

6) Παρακολούθηση ή/και δημιουργία προφίλ

- Κρυφή παρακολούθηση στο χώρο εργασίας (επικοινωνίες, αρχεία καταγραφής, PCs...,).
- Μη ορθή χρήση αλγορίθμων για κατάρτιση προφίλ/αυτοματοποιημένη λήψη αποφάσεων.
- Κατάρτιση προφίλ για σκοπούς μάρκετινγκ/ ανάλυσης δεδομένων χωρίς νομική βάση.
- Συστηματική παρακολούθηση των δραστηριοτήτων των εργαζομένων

Επίπεδο 4: Πηγές Κινδύνων (16/17)

Παραδείγματα που σχετίζονται με παρακολούθηση ή/και δημιουργία προφίλ:

- Δεν υπάρχει σαφής πολιτική σχετικά με τη χρήση των σταθμών εργασίας (δηλαδή δεν είναι σαφές ποιος μπορεί να έχει πρόσβαση σε αυτούς σε περίπτωση, π.χ. εγκατάστασης κακόβουλου λογισμικού σε υπολογιστή υπαλλήλου που απουσιάζει κ.λπ.).
- Αδικαιολόγητος έλεγχος των μεταδεδομένων τηλεφωνικών κλήσεων των εργαζομένων.
- Οι χρήστες δεν έχουν σαφή ή προσβάσιμο τρόπο να αντιταχθούν στην κατάρτιση προφίλ ή να ζητήσουν ανθρώπινη επανεξέταση μιας απόφασης.
- Τα δεδομένα που συλλέχθηκαν αρχικά για την παροχή υπηρεσιών χρησιμοποιούνται αργότερα από το σύστημα για στοχευμένη διαφήμιση ή ανάλυση δεδομένων.
- “Κρυφή» σκιαγράφηση προφίλ μέσω συναγόμενων δεδομένων —π.χ. διαφημίσεις, βίντεο ή ειδήσεις που προσαρμόζονται στην ΤΝ βάσει συναγόμενων ευαίσθητων χαρακτηριστικών.

Επίπεδο 4: Πηγές Κινδύνων (17/17)

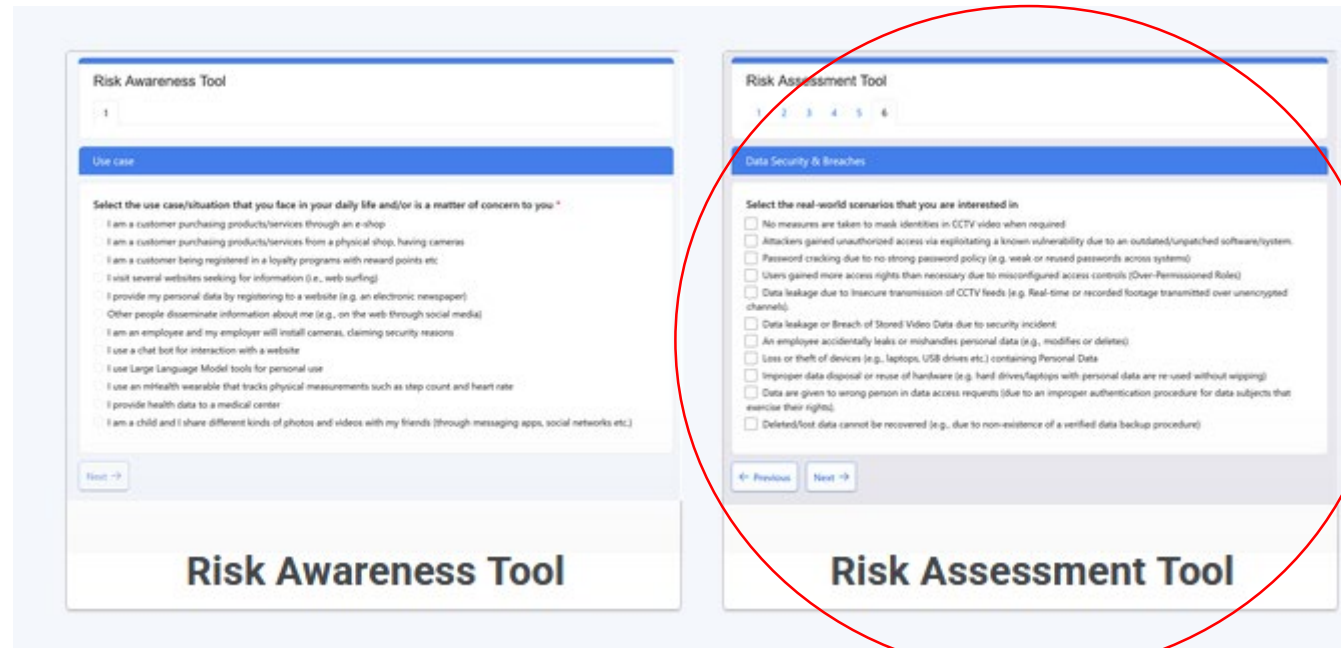
- 7) Μη αποτελεσματική διασφάλιση των δικαιωμάτων των φυσικών προσώπων.
- Τεχνικές αστοχίες όσον αφορά την ενεργοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων.
 - Συστημικές και οργανωτικές αποτυχίες στη διασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων.

Παραδείγματα που σχετίζονται με μη αποτελεσματική διασφάλιση δικαιωμάτων:

- Τα αιτήματα απαντώνται με αδικαιολόγητη καθυστέρηση.
- Δεν υπάρχουν, ή εφαρμόζονται ανεπαρκώς, διαδικασίες αιτήματος υποκειμένου δεδομένων (π.χ. δεν υπάρχει επίσημη διαδικασία ή εργαλείο για τον χειρισμό αιτημάτων πρόσβασης, διαγραφής ή διόρθωσης).
- Τα υποκείμενα των δεδομένων καλούνται να ακολουθήσουν μια πολύπλοκη διαδικασία για την άσκηση των δικαιωμάτων τους.

Το εργαλείο byRisk στην πράξη

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



The screenshot displays two side-by-side web forms. The left form, titled 'Risk Awareness Tool', has a section 'Use case' with a list of scenarios for selection. The right form, titled 'Risk Assessment Tool', has a section 'Data Security & Breaches' with a list of scenarios for selection. A red circle highlights the 'Risk Assessment Tool' form.

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 →



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

Σας ευχαριστώ για την Προσοχή σας.....