Ανάλυση Αντικτύπου για την Ιδιωτικότητα

Τσώχου Αγγελική

Βασισμένο στη μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων (CNIL)

Περιεχόμενα

- Κρισιμότητα των δεδομένων
- Απαίτηση εκπόνησης ανάλυσης αντικτύπου για την ιδιωτικότητα
- Η μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων (CNIL)
- Ενδεικτικά Μέτρα Προστασίας

Άρθρο 35 του ΓΚΠΔ: Κρισιμότητα Δεδομένων

- Συγκεκριμένα είδη επεξεργασίας ενδέχεται να επιφέρουν **υψηλό κίνδυνο** για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων:
  - συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών φυσικών προσώπων βασισμένη σε αυτοματοποιημένη επεξεργασία
  - μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων
  - συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

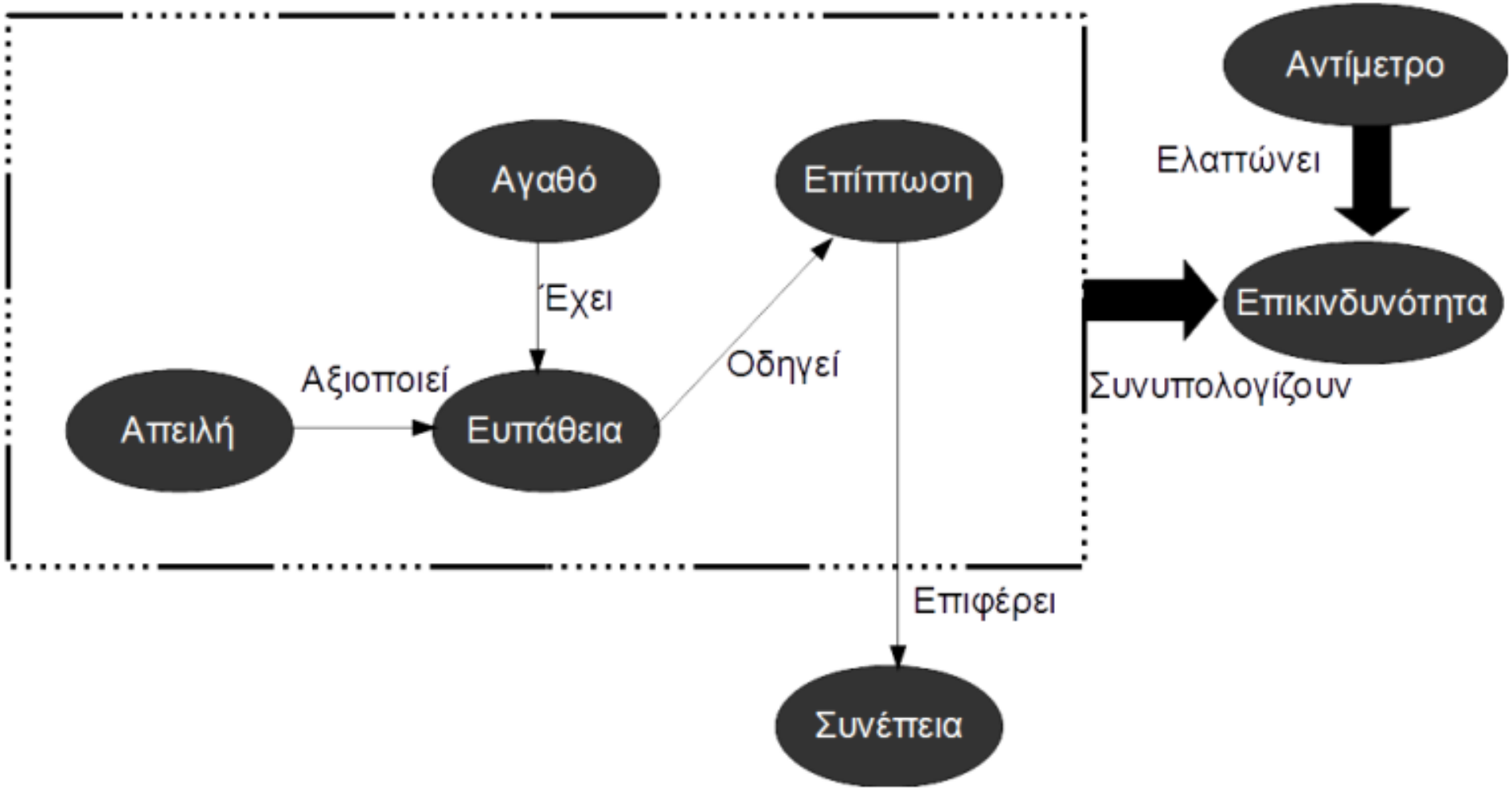
Αντίκτυπος σχετικά με την προστασία δεδομένων: Παραδείγματα

Είδος Επεξεργασίας	Παράδειγμα
Συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών φυσικών προσώπων βασισμένη σε αυτοματοποιημένη επεξεργασία	Δημιουργία προφίλ χρηστών ενός περιηγητή Διαδικτύου βάση της αναζήτησης που διεξάγουν στο Διαδίκτυο, με στόχο την αποστολή διαφημίσεων από εταιρείες προώθησης, όπως προϊόντα, ταξίδια, εστιατόρια, κτλ.
Μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων	Επεξεργασία ιατρικών φακέλων ασθενών (ευαίσθητα προσωπικά δεδομένα) από νοσηλευτικά ιδρύματα, συμπεριλαμβανομένου του ιατρικού ιστορικού ιστορικό, των παθήσεων και της φαρμακευτικής περίθαλψης των ασθενών.
Συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα	Παρακολούθηση την κίνησης των αυτοκινητοδρόμων, προκειμένου να εξυπηρετηθεί η ενημέρωση των οδηγών για τη γρηγορότερη διαδρομή κάθε φορά. Παρακολούθηση εισόδου πολυκατοικίας. Παρακολούθηση των χώρων πρόσβασης στο μετρό.

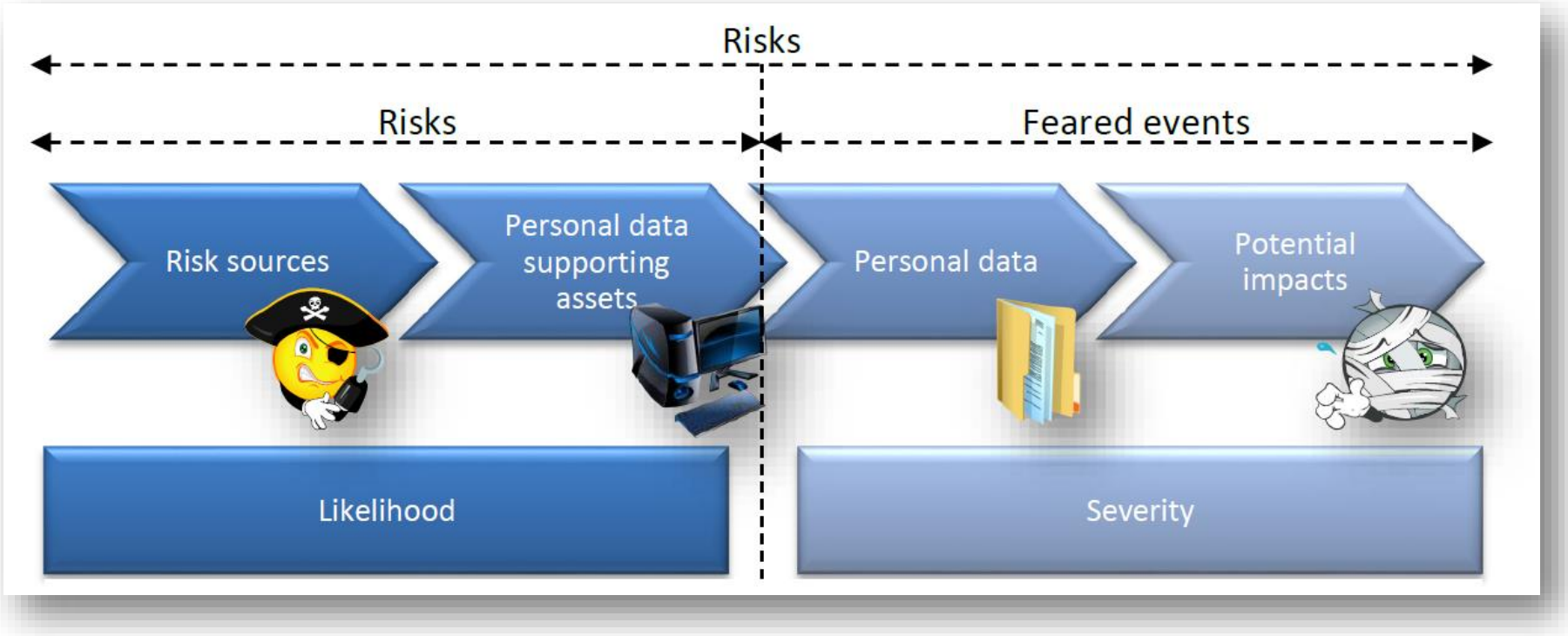
Κίνδυνος κατά της Ιδιωτικότητας (1/4)

- Ένας κίνδυνος (Risk) είναι ένα υποθετικό σενάριο σύμφωνα με το οποίο:
  - οι πηγές κινδύνου (για παράδειγμα κακόβουλοι εσωτερικού χρήστες)
  - θα μπορούσαν να εκμεταλλευτούν ευπάθειες των αγαθών που υποστηρίζουν την επεξεργασία των προσωπικών δεδομένων (για παράδειγμα μία βάση δεδομένων τήρησης των προσωπικών δεδομένων)
  - μέσω κάποιων απειλών (για παράδειγμα προσπάθεια μη εξουσιοδοτημένης πρόσβασης)
  - με αποτέλεσμα την πραγματοποίηση περιστατικού παραβίασης (για παράδειγμα διαρροή προσωπικών δεδομένων)
  - που θα έχει επιπτώσεις στην ιδιωτικότητα των υποκειμένων των δεδομένων

Κίνδυνος κατά της Ιδιωτικότητας (2/4)

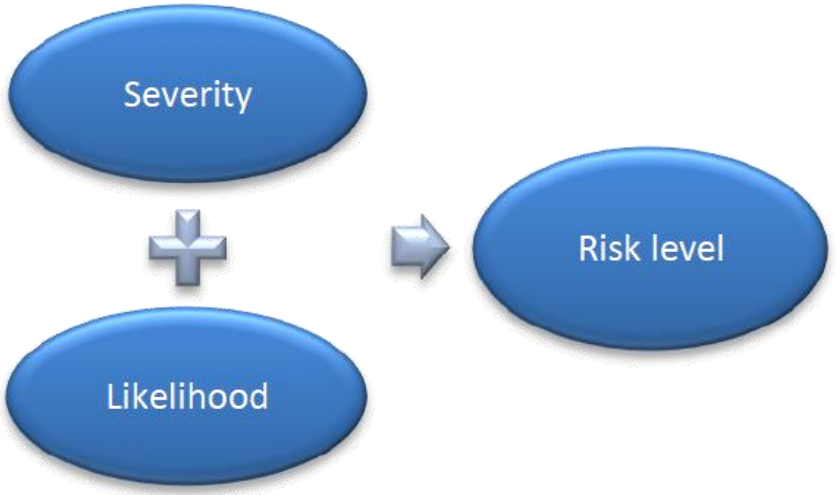


Κίνδυνος κατά της Ιδιωτικότητας (3/4)



Κίνδυνος κατά της Ιδιωτικότητας (4/4)

- Το επίπεδο του κινδύνου εξαρτάται από:
  - **τη βαρύτητα (severity)** των πιθανών επιπτώσεων σε περίπτωση περιστατικού παραβίασης της ιδιωτικότητας
  - **την πιθανότητα (likelihood)** πραγματοποίησης του κινδύνου (εξαρτάται από το επίπεδο των ευπαθειών των αγαθών του συστήματος και τη δυνατότητα εκμετάλλευσης των από τις απειλές).



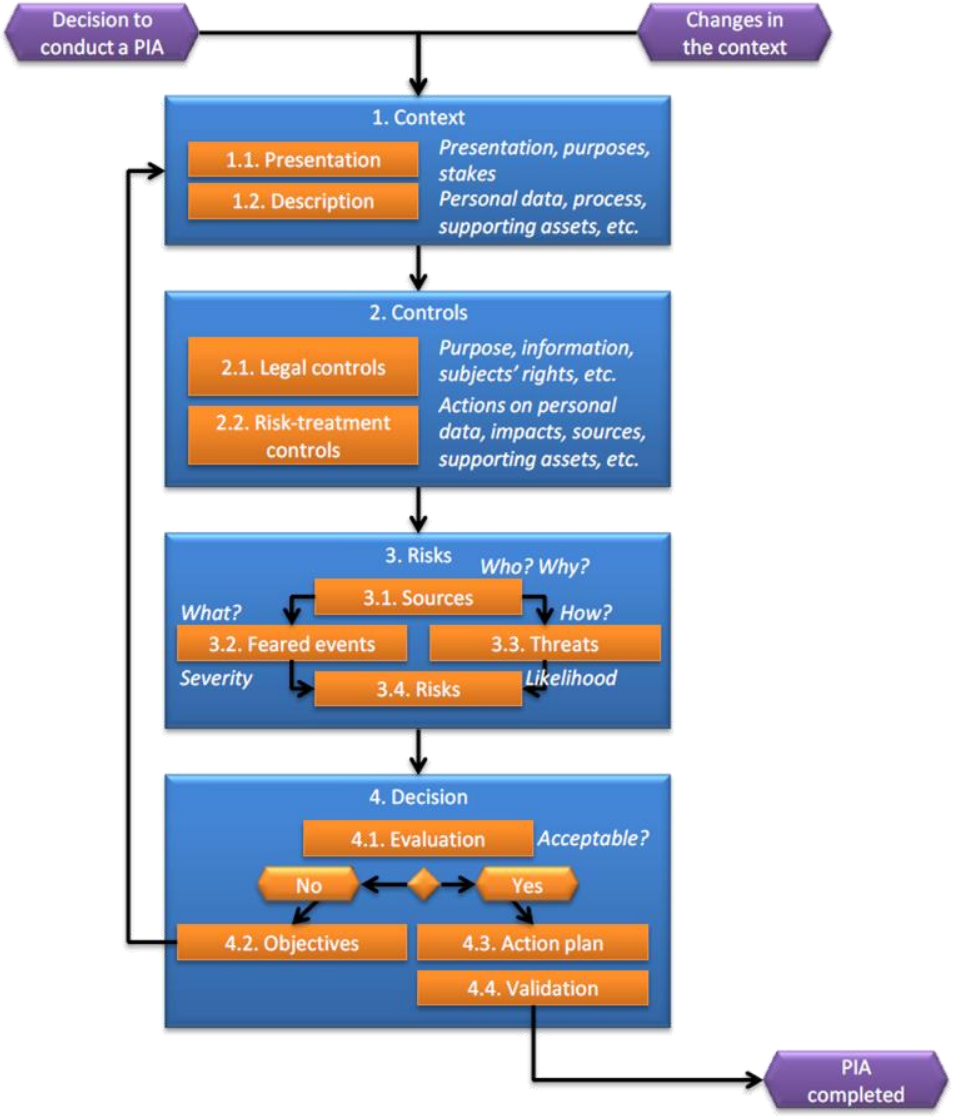
Η μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων (CNIL)

Πώς εκπονείται η Ανάλυση Αντικτύπου για την Ιδιωτικότητα (PIA);

1. Ορισμός του πλαισίου (context) επεξεργασίας των προσωπικών δεδομένων
2. Αναγνώριση υπαρχόντων ή μελλοντικών μέτρων (διαδικαστικά / τεχνικά / οργανωτικά) που απαιτούνται για την ικανοποίηση των όποιων νομικών απαιτήσεων και τη διαχείριση των κινδύνων κατά της ιδιωτικότητας (τηρώντας την αρχή της αναλογικότητας)
3. Αξιολόγηση των κινδύνων κατά της ιδιωτικότητας με στόχο να επιβεβαιωθεί ότι τα μέτρα διαχείρισης είναι τα κατάλληλα
4. Λήψη απόφασης σχετικά με τον τρόπο που θα ικανοποιηθούν οι βασικές αρχές για την προστασία της ιδιωτικότητας και για την αντιμετώπιση των κινδύνων.

Πώς εκπονείται η Ανάλυση Αντικτύπου για την Ιδιωτικότητα (PIA);

- Είναι μία επαναλαμβανόμενη διαδικασία
- Πρέπει να υλοποιείται κατά το σχεδιασμό του συστήματος και κάθε φορά σχεδιάζεται νέα επεξεργασία προσωπικών δεδομένων



1. Πλαίσιο: Αναγνώριση πλαισίου της PIA

- Στόχος: Κατανόηση των τρόπων επεξεργασίας προσωπικών δεδομένων

Step	Description	Report
		❑ Presentation of the processing(s) of personal data under consideration ❑ Description of the scope ❑ Detailed description of the scope

- Περιγραφή των Σκοπών Επεξεργασίας
- Αναγνώριση του Υπεύθυνου Επεξεργασίας και του Εκτελούντος την Επεξεργασία
- Αναγνώριση των Προσωπικών Δεδομένων (κατηγορίες) και των πιθανών Παραληπτών τους
- Αναγνώριση του απαιτούμενου Χρόνου Τήρησης των Δεδομένων
- Αναγνώριση των διεργασιών (processes) και των άλλων υποστηρικτικών αγαθών για την επεξεργασία των δεδομένων (από τη συλλογή μέχρι τη διαγραφή τους)

2. Μέτρα Προστασίας: Οι παράμετροι συμμόρφωσης (1 /5)

- **Στόχος**: Ανάπτυξη συστήματος που είναι συμβατό με τις αρχές προστασίας της ιδιωτικότητας (privacy principles).

Step	Description	Report
	2. Controls 2.1. Legal controls — *Purpose, information, subjects' rights, etc.* 2.2. Risk-treatment controls — *Actions on personal data, impacts, sources, supporting assets, etc.*	❑ List of selected controls ❑ Detailed description of the controls

- **Νομικές Απαιτήσεις (υποχρεωτικές)** Απαιτείται συμμόρφωση (και αναλυτική τεκμηρίωση του τρόπου με τον οποίο θα επιτευχθεί η συμμόρφωση) με τις παρακάτω νομικές απαιτήσεις:

1. **Σκοπός Επεξεργασίας**: προσδιορισμός
2. **Ελαχιστοποίηση**: περιορισμός των δεδομένων που συλλέγονται/τηρούνται μόνο στα απολύτως απαραίτητα για την εξυπηρέτηση του σκοπού.
3. **Ποιότητα**: Διατήρηση της ποιότητας / ακρίβειας των προσωπικών δεδομένων
4. **Χρόνος τήρησης**: απουσία άλλων νομικών υποχρεώσεων, χρόνος τήρησης είναι αυτός που απαιτείται για την εκπλήρωση του σκοπού επεξεργασίας
5. **Πληροφόρηση**: Σεβασμός στο δικαίωμα ενημέρωσης των υποκειμένων
6. *6.-10. : … (επόμενη διαφάνεια)*

2. Μέτρα Προστασίας: Οι παράμετροι συμμόρφωσης (2/5)

- **Νομικές Απαιτήσεις (υποχρεωτικές)**

1.-5. : ... (προηγούμενη διαφάνεια)

6. **Συναίνεση**: να έχει εξασφαλιστεί η συναίνεση των υποκειμένων, εκτός αν υφίσταται νομική υποχρέωση, για την επεξεργασία των προσωπικών δεδομένων
7. **Δικαίωμα αντίρρησης**: να υποστηρίζεται η δυνατότητα άσκησης του δικαιώματος αντίρρησης του υποκειμένου για την επεξεργασία των προσωπικών δεδομένων του
8. **Δικαίωμα Πρόσβασης**: να υποστηρίζεται η δυνατότητα άσκησης του δικαιώματος πρόσβασης από κάποιο υποκείμενο δεδομένων.
9. **Δικαίωμα Διόρθωσης**: να υποστηρίζεται η δυνατότητα άσκησης του δικαιώματος διόρθωσης / διαγραφής των προσωπικών δεδομένων από τα υποκείμενα
10. **Μεταβίβαση**: συμμόρφωση με τις διατάξεις του Κανονισμού για τη μεταβίβαση προσωπικών δεδομένων εκτός ΕΕ.

2. Μέτρα Προστασίας: Οι παράμετροι συμμόρφωσης (3/5)

- **Μέτρα Αντιμετώπισης Κινδύνων κατά της Ιδιωτικότητας:**
  - Οργανωτικά Μέτρα (organizational controls):
    - Πολιτικές ιδιωτικότητας (εσωτερικές και εξωτερικές)
    - Αποτελέσματα αποτίμησης επικινδυνότητας
    - Πρακτικές διοίκησης και διαχείρισης έργων
    - Πλαίσιο διαχείρισης περιστατικών
    - Διοίκηση ανθρώπινου δυναμικού
    - Διαβάθμιση πληροφοριών/δεδομένων
    - Εποπτεία προσωπικού και εργασιών
    - Τήρηση αρχείων

2. Μέτρα Προστασίας: Οι παράμετροι συμμόρφωσης (4/5)

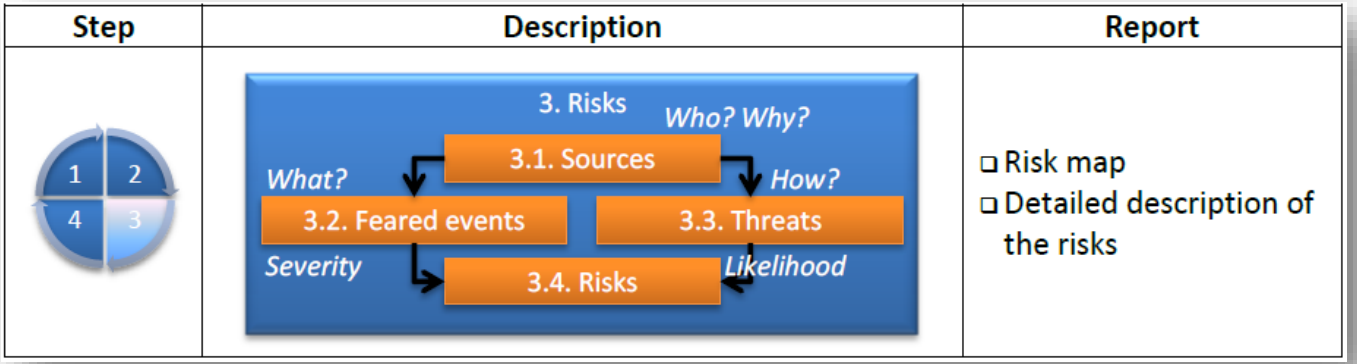
- **Μέτρα Αντιμετώπισης Κινδύνων κατά της Ιδιωτικότητας:**
  - Λογικά Μέτρα Ασφάλειας (logical security controls):
    - Ανωνυμοποίηση δεδομένων
    - Κρυπτογράφηση
    - Έλεγχος ακεραιότητας
    - Αντίγραφα ασφάλειας
    - Διαχωρισμός δεδομένων σε τμήματα
    - Έλεγχος πρόσβασης
    - Παρακολούθηση
    - Διαχείριση σταθμών εργασίας
    - Προστασία από κακόβουλο και κατασκοπευτικό λογισμικό

2. Μέτρα Προστασίας: Οι παράμετροι συμμόρφωσης (5/5)

- **Μέτρα Αντιμετώπισης Κινδύνων κατά της Ιδιωτικότητας:**
  - Φυσικά Μέτρα Ασφάλειας (physical security controls):
    - Απομάκρυνση από πηγές κινδύνων (επικίνδυνα υλικά, επικίνδυνες γεωγραφικές περιοχές, κλ.π.)
    - Έλεγχος φυσικής πρόσβασης
    - Ασφαλής διαχείριση υλισμικού
    - Ασφαλής διαχείριση εντύπων
    - Ασφαλής διαχείριση εκτυπώσεων
    - Προστασία από φυσικές καταστροφές

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Στόχος**: Κατανόηση των πηγών των κινδύνων καθώς και των πιθανών επιπτώσεων τους



- **Πηγές Κινδύνων (Sources)**
  - Αναγνώριση των πηγών κινδύνου για το συγκεκριμένο περιβάλλον που μελετάται
  - Περιγραφή των δυνατοτήτων των επιτιθέμενων (πηγών κινδύνου)

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Πηγές Κινδύνων (Sources):**
  - Εσωτερικές ανθρώπινες πηγές:
    - Υπάλληλοι, διευθυντές, στελέχη, εκπαιδευόμενοι
  - Εξωτερικές ανθρώπινες πηγές:
    - Αποδέκτες προσωπικών δεδομένων, πάροχοι υπηρεσιών, επιτιθέμενοι σε δίκτυα και συστήματα, επισκέπτες, πρότεροι υπάλληλοι, ακτιβιστές, δημοσιογράφοι, μη κυβερνητικοί οργανισμοί, εγκληματικές και τρομοκρατικές οργανώσεις
  - Μη ανθρώπινες πηγές:
    - Κακόβουλος κώδικας, εκρηκτικές και εύφλεκτες ύλες, πηγές νερού (σωλήνες, υδρορροές)

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Πιθανά περιστατικά παραβίασης της Ιδιωτικότητας (Feared events)**
  - Για κάθε πιθανό περιστατικό παραβίασης (μη εξουσιοδοτημένη πρόσβαση ή/και τροποποίηση προσωπικών δεδομένων, καταστροφή / απώλεια προσωπικών δεδομένων):
    - εκτιμώνται οι πιθανές συνέπειες (**impacts**) για την ιδιωτικότητα των υποκειμένων
    - εκτιμάται η βαρύτητα (**severity**), με βάση το πόσο επιζήμιες θα είναι οι συνέπειες του περιστατικού για τα υποκείμενα των δεδομένων

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Πιθανά περιστατικά παραβίασης της Ιδιωτικότητας (Feared events):**
  - Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα
    - Χρήσης, αποθήκευσης, διαβίβασης, συσχέτισης, κτλ.
  - Μη εξουσιοδοτημένη τροποποίηση δεδομένων
    - Για χρήση, για πρόκληση βλάβης, κτλ.
  - Διαγραφή προσωπικών δεδομένων
    - Για χρήση, για αποκλεισμό, κτλ.

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Απειλές (Threats)**
  - Αναγνώριση των απειλών (**threats**), κατά των αγαθών που υποστηρίζουν την επεξεργασία των δεδομένων, και οι οποίες θα μπορούσαν να προκαλέσουν περιστατικό παραβίασης της ιδιωτικότητας (feared event)
  - Για κάθε απειλή :
    - θα πρέπει να εντοπιστούν οι πηγές κινδύνου (**risk sources**) που θα μπορούσαν να υλοποιήσουν τη συγκεκριμένη απειλή
    - θα πρέπει να εκτιμηθεί η πιθανότητα εμφάνισης της απειλής (**likelihood**), σε συνδυασμό με το επίπεδο των ευπαθειών των αγαθών που υποστηρίζουν την επεξεργασία των δεδομένων και τις δυνατότητες των επιτιθέμενων

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- Απειλές (Threats)
  - Απειλές που οδηγούν σε μη ορθή χρήση των πληροφοριακών πόρων (εκτός του σκοπού, χωρίς να αλλοιωθούν ή να τροποποιηθούν)
  - Απειλές που οδηγούν σε παρακολούθηση των πληροφοριακών πόρων (χωρίς να αλλοιωθούν ή να τροποποιηθούν)
  - Απειλές που οδηγούν σε υπερφόρτωση των πληροφοριακών πόρων (υπερφόρτωση υπολογιστών/εξυπηρετητών, χρήση σε μη συνιστάμενες συνθήκες)
  - Απειλές που οδηγούν σε καταστροφή ή βλάβη των πληροφοριακών πόρων
  - Απειλές που οδηγούν σε τροποποίηση των πληροφοριακών πόρων
  - Απειλές που οδηγούν σε απώλεια πληροφοριακών πόρων (π.χ. σε κλοπή, ή πώληση)

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- Απειλές που οδηγούν σε μη ορθή χρήση των πληροφοριακών πόρων:
  - Χρήση φορητών μονάδων αποθήκευσης για αποθήκευση εμπιστευτικών πληροφοριών
  - Διαγραφή ή τροποποίηση δικαιωμάτων πρόσβασης
  - Διαγραφή στοιχείων ώστε μία εφαρμογή να μη λειτουργεί σωστά
  - Επιθέσεις Man-in-the-middle
  - Παραποίηση εγγράφων

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- Απειλές που οδηγούν σε παρακολούθηση των πληροφοριακών πόρων:
  - Shoulder surfing
  - Παρείσφρηση σε δίκτυο
  - Παρακολούθηση/Καταγραφή συνομιλίας
  - Δημιουργία φωτοτυπιών εγγράφων
  - Παρακολούθηση δημόσιου ασύρματου δικτύου
  - Έλεγχος διευθύνσεων και πυλών δικτύου
  - Παρακολούθηση τοποθεσίας φορητής συσκευής

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- Απειλές που οδηγούν σε υπερφόρτωση των πληροφοριακών πόρων:
  - Υπέρμετρος φόρτος εργασίας σε εργαζομένους και συνθήκες άγχους και πιεστικών προθεσμιών
  - Ανάθεση αρμοδιοτήτων σε προσωπικό χωρίς τα κατάλληλα προσόντα
  - Υπερφόρτωση χώρου αποθήκευσης μηχανήματος
  - Υπερφόρτωση επεξεργαστικής ισχύος
  - Υπερθέρμανση
  - Επίθεση άρνησης παροχής υπηρεσιών
  - Εισαγωγή στοιχείων εκτός ορισμού σε βάση δεδομένων

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- Απειλές που οδηγούν σε καταστροφή ή βλάβη των πληροφοριακών πόρων:
  - Φυσικές καταστροφές, φωτιά, πλημμύρα
  - Τεχνικές βλάβες
  - Λογικές βόμβες σε λογισμικό
  - Καταστροφή καλωδίων και συνδέσεων
  - Ατυχήματα που οδηγούν σε ανθρώπινες βλάβες
  - Συνταξιοδότηση/απόλυση/παραίτηση
  - Καταστροφή εντύπων λόγω πολυχρονισμού

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- Απειλές που οδηγούν σε τροποποίηση των πληροφοριακών πόρων:
  - Keyloggers
  - Κακόβουλο λογισμικό
  - Τροποποίηση στοιχείων ή λάθη συστήματος μέσω αναβαθμίσεων
  - Λάθος συντήρησης υλισμικού ή λογισμικού
  - Αντικατάσταση γνήσιου εγγράφου με πλαστό
  - Αποστολή πολλαπλών αντικρουόμενων εκδοχών εγγράφου
  - Σύνδεση μη συμβατού υλισμικού

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- Απειλές που οδηγούν σε απώλεια πληροφοριακών πόρων:
  - Κλοπή φορητής συσκευής
  - Κλοπή αρχείων
  - Κλοπή εγγράφων
  - Κλοπή αποστολών
  - Κλοπή άδειας χρήσης λογισμικού

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Κίνδυνοι (Risks):**
  - Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα
  - Μη εξουσιοδοτημένη τροποποίηση δεδομένων
  - Διαγραφή προσωπικών δεδομένων

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Κίνδυνοι (Risks)**
  - Προσδιορισμός του επιπέδου του Κινδύνου :
    - Η βαρύτητα (**severity**) του κινδύνου ταυτίζεται με τη βαρύτητα του περιστατικού παραβίασης (feared event) που μπορεί να προκληθεί από το συγκεκριμένο κίνδυνο
    - Η πιθανότητα εμφάνισης του κινδύνου (**likelihood**) ταυτίζεται με την πιθανότητα εμφάνισης των απειλών που σχετίζονται με το συγκεκριμένο περιστατικό παραβίασης (feared event).

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Υπολογισμός πιθανότητας περιστατικών παραβίασης της Ιδιωτικότητας (Feared events):**
  - Παράγοντες που λαμβάνονται υπόψη:
    - Συνδεσιμότητα με το Διαδίκτυο ή άλλα δίκτυα
    - Ανταλλαγή δεδομένων με άλλες χώρες
    - Διασυνδέσεις με άλλα πληροφοριακά συστήματα
    - Πολυπλοκότητα του πληροφοριακού συστήματος
    - Το προφίλ του οργανισμού
  - Κλίμακα 1-4: Αμελητέα, Περιορισμένη, Σημαντική, Μέγιστη

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Υπολογισμός πιθανότητας (likelihood) περιστατικών παραβίασης της Ιδιωτικότητας:**
  - **Αμελητέα**: δε φαίνεται πιθανό να μπορεί η πηγή κινδύνου να υλοποιήσει την απειλή μέσω στοιχείων του συστήματος (π.χ. κλοπή εντύπων αποθηκευμένα σε δωμάτιο με έλεγχο πρόσβασης με αναγνωριστικό και κάρτα ελέγχου)
  - **Περιορισμένη**: φαίνεται δύσκολο να μπορεί η πηγή κινδύνου να υλοποιήσει την απειλή μέσω στοιχείων του συστήματος (π.χ. κλοπή εντύπων αποθηκευμένα σε δωμάτιο με έλεγχο πρόσβασης με αναγνωριστικό)

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Υπολογισμός πιθανότητας (likelihood) περιστατικών παραβίασης της Ιδιωτικότητας:**
  - **Σημαντική**: φαίνεται εφικτό να μπορεί η πηγή κινδύνου να υλοποιήσει την απειλή μέσω στοιχείων του συστήματος (π.χ. κλοπή εντύπων αποθηκευμένα σε δωμάτιο με πρόσβαση μέσω ελέγχου από τη γραμματεία)
  - **Μέγιστη**: είναι ιδιαίτερα εύκολο να μπορεί η πηγή κινδύνου να υλοποιήσει την απειλή μέσω στοιχείων του συστήματος (π.χ. κλοπή εντύπων αποθηκευμένα σε δημόσια προσβάσιμο χώρο αναμονής)

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

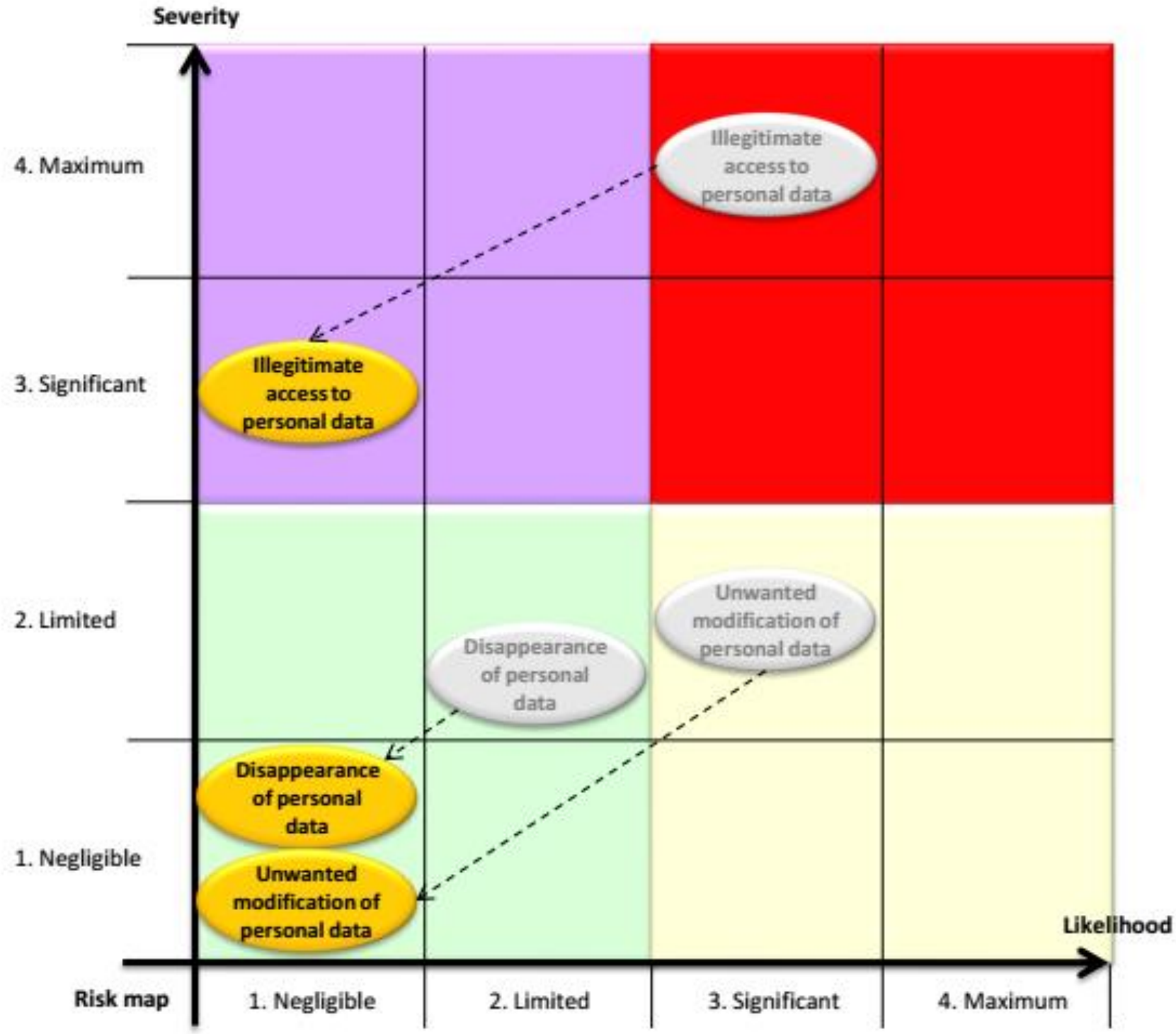
- **Υπολογισμός βαρύτητας (severity) περιστατικών παραβίασης της Ιδιωτικότητας:**
  - Παράγοντες που λαμβάνονται υπόψη:
    - Βαθμός ευκολίας ταυτοποίησης των υποκειμένων των δεδομένων
    - Φύση των πηγών κινδύνου
    - Αριθμός διασυνδέσεων με άλλα συστήματα/ οργανισμούς
    - Αριθμός διασυνδέσεων με άλλες χώρες
    - Αριθμός αποδεκτών
  - Κλίμακα 1-4: Αμελητέα, Περιορισμένη, Σημαντική, Μέγιστη

3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Υπολογισμός βαρύτητας (severity) περιστατικών παραβίασης της Ιδιωτικότητας :**
  - **Αμελητέα**: Τα υποκείμενα των δεδομένων δε θα επηρεαστούν ή μπορεί να αντιμετωπίσουν ενοχλήσεις τις οποίες θα ξεπεράσουν χωρίς σημαντικό πρόβλημα (π.χ. φόβος, απώλεια χρόνου)
  - **Περιορισμένη**: Τα υποκείμενα των δεδομένων μπορεί να αντιμετωπίσουν σημαντικές ενοχλήσεις, τις οποίες θα μπορέσουν να ξεπεράσουν με κάποια δυσκολία (π.χ. άρνηση χρήσης υπηρεσιών, ηθικές βλάβες, αίσθημα παραβίασης ιδιωτικότητας χωρίς φυσικές βλάβες)

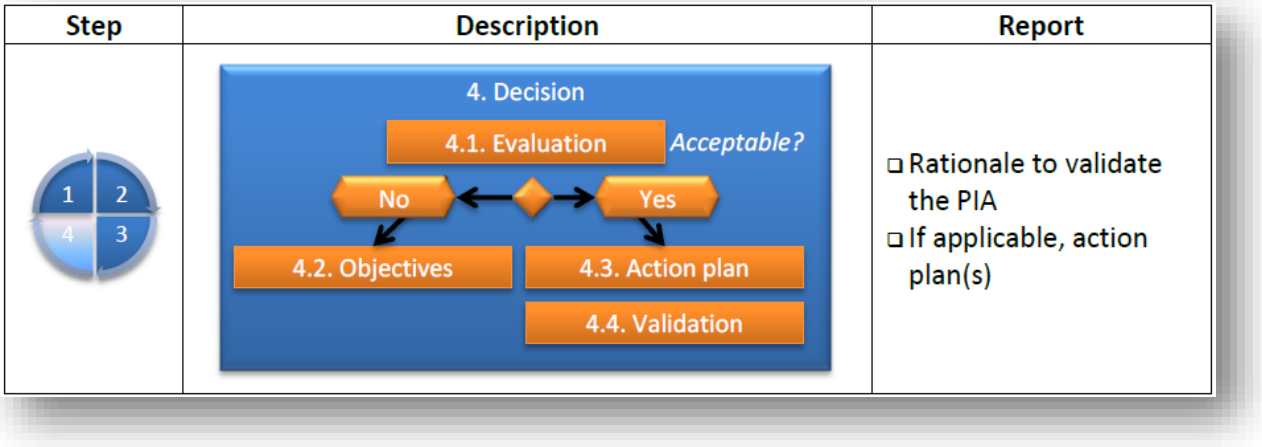
3. Κίνδυνοι: Περιστατικά παραβίασης της Ιδιωτικότητας

- **Υπολογισμός βαρύτητας (severity) περιστατικών παραβίασης της Ιδιωτικότητας :**
  - **Σημαντική**: Τα υποκείμενα των δεδομένων μπορεί να αντιμετωπίσουν σημαντικές συνέπειες τις οποίες θα μπορέσουν να ξεπεράσουν με σοβαρές δυσκολίες (π.χ. πρόκληση ψυχικής βλάβης, αίσθημα παραβίασης ιδιωτικότητας, πρόκληση παρενοχλήσεων, οικονομικές απώλειες)
  - **Μέγιστη**: Τα υποκείμενα των δεδομένων μπορεί να αντιμετωπίσουν σοβαρές, ακόμη και ανεπανόρθωτες, συνέπειες τις οποίες ενδέχεται να μη μπορούν να ξεπεράσουν (π.χ. μακροχρόνιες ψυχικές ασθένειες, ποινικές κυρώσεις, κίνδυνο ζωής, αδυναμία εργασίας)


Severity
4. Maximum
3. Significant
2. Limited
1. Negligible
Illegitimate access to personal data
Illegitimate access to personal data
Unwanted modification of personal data
Disappearance of personal data
Disappearance of personal data
Unwanted modification of personal data
Likelihood
Risk map
1. Negligible
2. Limited
3. Significant
4. Maximum

4. Απόφαση: Αξιολόγηση PIA

- **<u>Στόχος</u>**: Απόφαση αποδοχής ή μη του τρόπου ικανοποίησης των βασικών αρχών για την προστασία της ιδιωτικότητας και της διαχείρισης των κινδύνων



- **Αξιολόγηση PIA**
  - Αξιολόγηση των τρόπων ικανοποίησης των νομικών απαιτήσεων
  - Αξιολόγηση των τρόπων διαχείρισης των κινδύνων

4. Απόφαση: Αξιολόγηση PIA

- **Κίνδυνοι με μέγιστη/σημαντική πιθανότητα και επίπτωση**: Υποχρεωτική αποφυγή ή αντιμετώπιση με αντίμετρα
- **Κίνδυνοι με μέγιστη/σημαντική επίπτωση αλλά αμελητέα/περιορισμένη πιθανότητα:** Συνίσταται αποφυγή, ή πρέπει να γίνει αντιμετώπιση με αντίμετρα

4. Απόφαση: Αξιολόγηση PIA

- **Κίνδυνοι με αμελητέα/περιορισμένη επίπτωση αλλά μέγιστη/σημαντική πιθανότητα:** Πρέπει να γίνει αντιμετώπιση με την εφαρμογή αντιμέτρων που μειώνουν την πιθανότητα εμφάνισης
- **Κίνδυνοι με αμελητέα/περιορισμένη επίπτωση αλλά αμελητέα/περιορισμένη πιθανότητα:** Επιτρέπεται η αποδοχή αυτών των κινδύνων

Η αναφορά PIA

- Εισαγωγή και παρουσίαση των διεργασιών επεξεργασίας προσωπικών δεδομένων
- Ανάλυση Αντικτύπου (PIA)
  - Περιγραφή πλαισίου
  - Λίστα νομικών απαιτήσεων
  - Λίστα λογικών μέτρων προστασίας
  - Καταγραφή κινδύνων και επιπέδου τους
- Απόφαση
- Παραρτήματα
    - Αναλυτική περιγραφή πλαισίου, αναλυτική καταγραφή μέτρων προστασίας, ανάλυση κινδύνων, σχέδιο ενεργειών για την υιοθέτηση μέτρων προστασίας

Μέτρα Προστασίας

Μέτρα προστασίας των δεδομένων

- Ελαχιστοποίηση δεδομένων
- Διαχείριση χρόνου τήρησης δεδομένων
- Ενημέρωση των υποκειμένων των δεδομένων
- Συλλογή συγκατάθεσης
- Παροχή δυνατότητας αναίρεσης συγκατάθεσης
- Παροχή πρόσβασης/διόρθωσης δεδομένων
- Διαχωρισμός αρχείων δεδομένων
- Κρυπτογράφηση προσωπικών δεδομένων (στην αποθήκευση και μετάδοση)
- Ανωνυμοποίηση προσωπικών δεδομένων
- Κτλ.

Μέτρα μείωσης αντικτύπου παραβίασης

- Αντίγραφα ασφάλειας (ακεραιότητα/διαθεσιμότητα)
- Παρακολούθηση ακεραιότητας (έλεγχος ακεραιότητας/ hash functions/ ψηφιακές υπογραφές)
- Παρακολούθηση ενεργειών συστήματος (τήρηση και ανάλυση log files, τείχος προστασίας, παρακολούθηση συσκευών δικτύου)
- Διαχείριση περιστατικών παραβίασης (φόρμες αναφοράς, σχήμα και δομή διαχείρισης, διαβάθμιση περιστατικών)
- Κτλ.

Μέτρα μείωσης πιθανότητας εμφάνισης

- Αποφυγή των πηγών κινδύνου
- Διαβάθμιση αρχείων που περιέχουν προσωπικά δεδομένα
- Διαχείριση προσωπικού με πρόσβαση σε προσωπικά δεδομένα (π.χ., σύμφωνο εμπιστευτικότητας, καταγραφή ρόλων, εκπαίδευση)
- Παρακολούθηση και έλεγχος πρόσβασης (π.χ., need to know/least privilege, τήρηση ιστορικού εκχώρησης δικαιωμάτων πρόσβασης)
- κτλ.

Μέτρα μείωσης πιθανότητας εμφάνισης

- Διαχείριση λογαριασμών χρηστών και αυθεντικοποίησης
- Παρακολούθηση πρόσβασης συνεργατών και παρόχων υπηρεσιών (π.χ. καταγραφή όσων έχουν πρόσβαση σε προσωπικά δεδομένα, ορισμός διαδικασιών τερματισμού συνεργασίας σε περίπτωση παραβίασης προσωπικών δεδομένων)
- Διαχείριση εξωτερικής ανάθεσης και ενοικίασης υπολογιστικού χώρου (π.χ. συμβόλαια παροχής υπηρεσιών)
- Προστασία από κακόβουλο και ιομορφικό λογισμικό

Μέτρα μείωσης πιθανότητας εμφάνισης

- Έλεγχος φυσικής πρόσβασης στις εγκαταστάσεις (π.χ. μέτρα ελέγχου επισκεπτών, κάμερες, κλειδαριές, συναγερμοί)
- Αντιπλημμυρική προστασία
- Πυρασφάλεια
- Έλεγχος περιβαλλοντολογικών συνθηκών
- Κτ.λ.

Μέτρα προστασίας των υποστηρικτικών πόρων

- Ανίχνευση ευπαθειών
- Πολιτικές χρήσης σταθμών εργασίας και φορητών συσκευών
- Τήρηση τοπολογίας δικτύων
- Τήρηση αρχείου σημείων πρόσβασης δικτύων
- Χρήση κατάλληλων δικτύων
- Εκπαίδευση υπαλλήλων
- Πολιτικές καταστροφής εντύπων/υλικών/υλισμικού
- κτλ.

Software Tool for PIA

https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Βιβλιογραφία

[1] CNIL (2018) Privacy Impact Assessment (PIA) Methodology

[2] CNIL (2018) Privacy Impact Assessment (PIA) Tools

[3] CNIL (2018) Measures for the Privacy Risk Treatment

[4] Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα, Λαμπρινουδάκης Κ., Μήτρου Λ., Γκρίτζαλης Σ. και Κάτσικας Σ., Εκδόσεις Παπασωτηρίου, 2009