Εκτίμηση Αντικτύπου (PIA)

ΜΕΘΟΔΟΛΟΓΙΑ

Έκδοση Φεβρουαρίου 2018

Περιεχόμενα

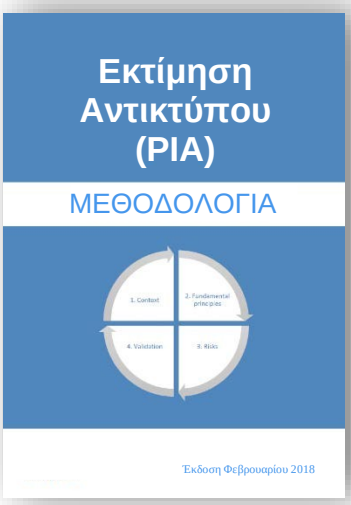
Πρόλογος **1**
Εισαγωγή **2**
Πως διενεργείται η PIA; **3**
1 Μελέτη των περιστάσεων **4**
1.1 Επισκόπηση 4
1.2 Προσωπικά δεδομένα, επεξεργασίες και υποστηρικτικά στοιχεία 4
2 Μελέτη των θεμελιωδών αρχών **5**
2.1 Αξιολόγηση των μέτρων που εγγυούνται την αναλογικότητα και την αναγκαιότητα της επεξεργασίας 5
2.2 Αξιολόγηση των μέτρων που προστατεύουν τα δικαιώματα των υποκειμένων των δεδομένων 5
3 Μελέτη των κινδύνων που σχετίζονται με την ασφάλεια των προσωπικών δεδομένων **6**
Τί είναι ο κίνδυνος ιδιωτικότητας; 6
3.1 Αξιολόγηση υφιστάμενων ή προγραμματισμένων μέτρων 7
3.2 Αξιολόγηση κινδύνου: ενδεχόμενες παραβιάσεις ιδιωτικότητας 7
4 Επικύρωση της PIA **8**
4.1 Προετοιμασία των στοιχείων που απαιτούνται για την επικύρωση 8
4.2 Επίσημη επικύρωση 8
Παραρτήματα **9**
Ορισμοί 9
Βιβλιογραφία 10
Σύνοψη των κριτηρίων των [Κατευθυντήριων Γραμμών της ΟΕ29] 11

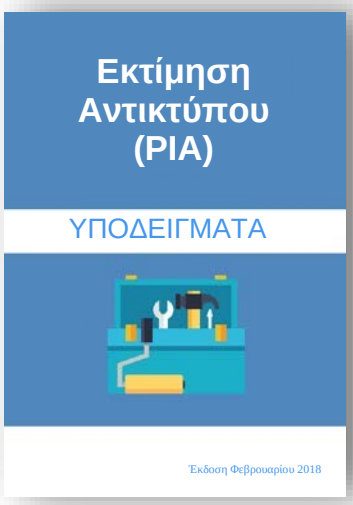
Πρόλογος

Η μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (CNIL) περιλαμβάνει τρεις οδηγούς: έναν που καθορίζει την προσέγγιση, έναν δεύτερο που περιλαμβάνει γεγονότα που θα μπορούσαν να χρησιμοποιηθούν για να ενταχθεί σε κανόνες η ανάλυση και έναν τρίτο που αποτελεί συλλογή γνώσεων (έναν κατάλογο μέτρων που στοχεύουν στη συμμόρφωση με τις νομικές υποχρεώσεις και την αντιμετώπιση των κινδύνων, καθώς και παραδείγματα):

Μπορείτε να κατεβάσετε αυτούς τους οδηγούς από τον ιστότοπο της CNIL:

https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual





Καθιερωμένες πρακτικές σχετικά με τη γραφή για όλα αυτά τα έγγραφα:

- ο όρος «**ιδιωτικότητα**» χρησιμοποιείται ως συντομογραφία για την αναφορά σε όλα τα θεμελιώδη δικαιώματα και ελευθερίες (ιδίως εκείνων που αναφέρονται στον [ΓΚΠΔ], τα άρθρα 7 και 8 του [Χάρτη της ΕΕ] και το Άρθρο 1 του [DP-Act]: «ιδιωτικότητα, ανθρώπινη ταυτότητα, ανθρώπινα δικαιώματα και ατομικές ή πολιτικές ελευθερίες»)·
- το ακρωνύμιο «**PIA**» χρησιμοποιείται εναλλάξιμα για την αναφορά στην Εκτίμηση Αντικτύπου Ιδιωτικότητας (PIA) και στην Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (DPIA)·
- οι διατυπώσεις σε αγκύλες ([τίτλος]) προσδιορίζουν αναφορές.

Εισαγωγή

Αυτός ο οδηγός εξηγεί πώς διενεργείται μια «εκτίμηση αντικτύπου προστασίας δεδομένων» (βλέπε Άρθρο 35 του [ΓΚΠΔ]), που πιο συχνά αναφέρεται ως Εκτίμηση Αντικτύπου στην Ιδιωτικότητα (PIA).

Περιγράφει τον τρόπο χρήσης της μεθόδου [EBIOS][1] στο συγκεκριμένο πλαίσιο της «Προστασίας Προσωπικών Δεδομένων». Η προσέγγιση είναι σύμφωνη με τα κριτήρια των Κατευθυντήριων Γραμμών της Ομάδας Εργασίας του άρθρου 29] (βλέπε επισυναπτόμενη σύνοψη) και είναι συμβατή με τα διεθνή πρότυπα διαχείρισης κινδύνων (όπως το [ISO 31000]).

Πρόκειται για μια μεθοδολογία επαναληπτικής διαδικασίας που θα πρέπει να εγγυάται μια αιτιολογημένη και αξιόπιστη χρήση των προσωπικών δεδομένων κατά τη διάρκεια της επεξεργασίας.

Η μεθοδολογία δεν εξετάζει τις αρχικές συνθήκες που καθορίζουν εάν απαιτείται ή όχι η διενέργεια μιας PIA (βλ. Άρθρο 35 παρ. 1 του [ΓΚΠΔ]) ή τις επακόλουθες συνθήκες που καθορίζουν εάν χρειάζεται ή όχι να γίνει διαβούλευση με την εποπτική αρχή (βλέπε άρθρο 36 παρ. 1 του [ΓΚΠΔ]).

Εκτελούμενη κατ' αρχήν από υπεύθυνο επεξεργασίας δεδομένων, ο σκοπός μιας PIA είναι να δημιουργηθεί και να αποδειχθεί η εφαρμογή των αρχών για την προστασία της ιδιωτικότητας, ώστε τα υποκείμενα των δεδομένων να διατηρούν τον έλεγχο των προσωπικών τους δεδομένων.

Προορίζεται για υπεύθυνους επεξεργασίας δεδομένων που επιθυμούν να αποδείξουν την προσέγγισή τους στη συμμόρφωση και τα μέτρα που επέλεξαν (αρχή της λογοδοσίας, βλέπε Άρθρο 25 του [ΓΚΠΔ]), καθώς και για παρόχους προϊόντων που επιθυμούν να αποδείξουν ότι οι λύσεις τους δεν παραβιάζουν την προστασία της ιδιωτικότητας χάρη σε έναν σχεδιασμό που σέβεται την προστασία της ιδιωτικότητας (αρχή της Προστασίας των δεδομένων ήδη από τον Σχεδιασμό, βλ. άρθρο 25 του [ΓΚΠΔ])[2]. Είναι χρήσιμος για όλους τους ενδιαφερόμενους φορείς που εμπλέκονται στη δημιουργία ή τη βελτίωση της επεξεργασίας προσωπικών δεδομένων ή προϊόντων:

- αρχές λήψης αποφάσεων οι οποίες αναθέτουν και επικυρώνουν τη δημιουργία νέων επεξεργασιών προσωπικών δεδομένων ή προϊόντων·
- ιδιοκτήτες έργων, οι οποίοι πρέπει να διενεργούν αξιολόγηση των κινδύνων για τα συστήματά τους και να ορίζουν τους στόχους ασφαλείας·
- κύριους εργολάβους, οι οποίοι πρέπει να προτείνουν λύσεις για την αντιμετώπιση των κινδύνων σύμφωνα με τους στόχους που προσδιορίζονται από τους ιδιοκτήτες έργων·
- υπεύθυνους προστασίας δεδομένων (ΥΠΔ), οι οποίοι πρέπει να υποστηρίζουν τους ιδιοκτήτες έργων και τις αρχές λήψης αποφάσεων στον τομέα της προστασίας των προσωπικών δεδομένων·
- υπεύθυνους ασφάλειας κεντρικών συστημάτων πληροφορικής (ΥΑΚΠ – CISO), οι οποίοι πρέπει να υποστηρίξουν τους ιδιοκτήτες έργων στον τομέα της ασφάλειας των πληροφοριών (IS).

[1] EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité (Έκφραση των Αναγκών και Προσδιορισμός των Στόχων Ασφαλείας) - είναι το όνομα της μεθοδολογίας διαχείρισης του κινδύνου που δημοσιεύεται από την Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI / Γαλλική Εθνική Υπηρεσία Ασφάλειας Δικτύων και Πληροφοριών).

[2] Στο λοιπό έγγραφο, ο όρος «επεξεργασία προσωπικών δεδομένων» είναι εναλλάξιμος με τον όρο «προϊόν».

Πώς διενεργείται η PIA;

Η προσέγγιση συμμόρφωσης που εφαρμόζεται με τη διεξαγωγή μιας PIA βασίζεται σε δύο πυλώνες:

1. τα **θεμελιώδη δικαιώματα και αρχές**[3], τα οποία είναι «μη διαπραγματεύσιμα», θεσπίζονται από τον νόμο και τα οποία πρέπει να τηρούνται, ανεξάρτητα από τη φύση, τη σοβαρότητα και την πιθανότητα κινδύνων·
2. τη **διαχείριση των κινδύνων ιδιωτικής ζωής των υποκειμένων των δεδομένων**[4], η οποία καθορίζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων[5].

Σχήμα 1 - Προσέγγιση συμμόρφωσης με τη χρήση PIA

Συνοψίζοντας, για να διενεργηθεί μια PIA είναι απαραίτητο να:

1. καθοριστεί και περιγραφεί τις **περιστάσεις** της επεξεργασίας των υπό εξέταση δεδομένων προσωπικού χαρακτήρα·
2. αναλυθούν τα μέτρα που εγγυώνται τη συμμόρφωση με τις **θεμελιώδεις αρχές**: την αναλογικότητα και την αναγκαιότητα της επεξεργασίας και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων·
3. αξιολογηθούν οι **κίνδυνοι** για την προστασία της ιδιωτικότητας που συνδέονται με την ασφάλεια των δεδομένων και διασφαλιστεί ότι αντιμετωπίζονται κατάλληλα·
4. τεκμηριωθεί επισήμως η **επικύρωση** της PIA εν όψει των προηγούμενων διαθέσιμων στοιχείων ή αποφασιστεί η αναθεώρηση των προηγούμενων βημάτων.

Σχήμα 2 - Γενική προσέγγιση για τη διενέργεια μιας PIA

Πρόκειται για μια διαδικασία συνεχούς βελτίωσης.
Επομένως, μερικές φορές απαιτούνται αρκετές επαναλήψεις για να επιτευχθεί ένα αποδεκτό σύστημα προστασίας της ιδιωτικότητας. Απαιτείται επίσης η παρακολούθηση των αλλαγών με την πάροδο του χρόνου (στις περιστάσεις, τα μέτρα, τους κινδύνους κ.λπ.), για παράδειγμα, κάθε έτος, και επικαιροποίηση κάθε φορά που συμβαίνει μια σημαντική αλλαγή.

Η προσέγγιση πρέπει να υλοποιείται μόλις σχεδιαστεί μια νέα επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η εξαρχής υλοποίηση αυτής της προσέγγισης καθιστά δυνατό τον καθορισμό των αναγκαία και επαρκή μέτρα και, κατά συνέπεια, τη βελτιστοποίηση του κόστους. Αντίθετα, η υλοποίησή της μετά τη δημιουργία του συστήματος και την υλοποίηση των μέτρων μπορεί να θέσει υπό αμφισβήτηση τις επιλογές που έχουν γίνει.

[3] Καθορισμένος, ρητός και νόμιμος σκοπός· κατάλληλα, συναφή και όχι υπερβολικά δεδομένα· σαφείς και πλήρεις πληροφορίες για τα υποκείμενα των δεδομένων· περιορισμένη διάρκεια αποθήκευσης· δικαίωμα πρόσβασης, εναντίωσης, διόρθωσης και διαγραφής κλπ.
[4] Σχετικά με την ασφάλεια των προσωπικών δεδομένων και με αντίκτυπο στην ιδιωτικότητα των υποκειμένων.
[5] Προκειμένου να «*ληφθούν όλες οι χρήσιμες προφυλάξεις, όσον αφορά στη φύση των δεδομένων και τους κινδύνους της επεξεργασίας, να διατηρηθεί η ασφάλεια των δεδομένων και, ιδίως, να αποφευχθεί η αλλοίωση και η ζημία τους ή η πρόσβαση από μη εξουσιοδοτημένους τρίτους*» (Άρθρο 34 του [DP-Act]).

1 Μελέτη των περιστάσεων

Γενικά διεξάγεται από τον ιδιοκτήτη του έργου[6], με τη βοήθεια ενός επικεφαλής για θέματα «Προστασίας δεδομένων»[7].

Σκοπός: να αποκτήσετε μια σαφή επισκόπηση των υπό εξέταση πράξεων επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

1.1 Επισκόπηση

- Παρουσιάστε μια σύντομη περιγραφή της υπό εξέταση **επεξεργασίας** προσωπικών δεδομένων, της **φύσης**, του **πεδίου εφαρμογής**, των **περιστάσεων**, των **σκοπών** και των **διακυβευμάτων**[8].
- Προσδιορίστε τον **υπεύθυνο επεξεργασίας** και ενδεχόμενους **εκτελούντες την επεξεργασία**.
- Να απαριθμηθούν οι **αναφορές που ισχύουν** για την επεξεργασία, οι οποίες είναι απαραίτητες ή πρέπει να τηρούνται[9], και ιδίως οι εγκεκριμένοι κώδικες δεοντολογίας (βλ. Άρθρο 40 του [ΓΚΠΔ]) και οι πιστοποιήσεις σχετικά με την προστασία δεδομένων (βλ. Άρθρο 42 του [ΓΚΠΔ])[10].

1.2 Προσωπικά δεδομένα, επεξεργασίες και υποστηρικτικά στοιχεία

- Καθορίστε και περιγράψτε λεπτομερώς το πεδίο εφαρμογής:
  - τα σχετικά **προσωπικά δεδομένα**, τους **αποδέκτες** τους και τις **διάρκειες αποθήκευσής** τους·
  - την **επεξεργασία** προσωπικών δεδομένων και τα **υποστηρικτικά στοιχεία** για την προστασία των προσωπικών δεδομένων για ολόκληρο τον κύκλο ζωής των προσωπικών δεδομένων (από τη συλλογή έως τη διαγραφή).

[6] Με την επιχειρηματική έννοια. Αυτό μπορεί να ανατεθεί, να εκπροσωπηθεί ή να διεκπεραιωθεί από άλλο ενδιαφερόμενο μέρος.
[7] Όπως για παράδειγμα ο υπεύθυνος προστασίας δεδομένων.
[8] Απαντήστε στην ερώτηση «Ποια είναι τα αναμενόμενα οφέλη (για τον οργανισμό, για τα υποκείμενα των δεδομένων, για την κοινωνία εν γένει, *κλπ.*);».
[9] Ανάλογα με την περίπτωση, θα είναι ιδιαίτερα χρήσιμες για την απόδειξη της συμμόρφωσης με τις θεμελιώδεις αρχές, για τη δικαιολόγηση των μέτρων ή την απόδειξη ότι αντιστοιχούν στην αιχμή της τεχνολογίας.
[10] Άλλα παραδείγματα: πολιτική ασφάλειας, νομικά πρότυπα εξειδικευμένα ανά τομέα, *κλπ.*

2 Μελέτη των θεμελιωδών αρχών

Γενικά εκτελείται από τον ιδιοκτήτη του έργου και στη συνέχεια αξιολογείται από έναν επικεφαλής για θέματα «Προστασίας Δεδομένων».

Στόχος: δημιουργία του συστήματος που εξασφαλίζει τη συμμόρφωση με τις αρχές προστασίας της ιδιωτικής ζωής.

2.1 Αξιολόγηση των μέτρων που εγγυώνται την αναλογικότητα και την αναγκαιότητα της επεξεργασίας

- Εξηγήστε και αιτιολογήστε τις **επιλογές που έγιναν για να συμμορφωθείτε με τις ακόλουθες απαιτήσεις**:
  1. **σκοπός (-οι)**: καθορισμένος, ρητός και νόμιμος (βλ. Άρθρο 5 παράγραφος 1 στοιχείο β του [ΓΚΠΔ])·
  2. **βάση**: νομιμότητα της επεξεργασίας, απαγόρευση της κατάχρησης (βλ. Άρθρο 6 του [ΓΚΠΔ])[11]·
  3. **ελαχιστοποίηση των δεδομένων**: κατάλληλα, συναφή και περιορισμένα στο αναγκαίο (βλ. Άρθρο 5 παρ. 1 στοιχείο γ του [ΓΚΠΔ])[12]·
  4. **ποιότητα των δεδομένων**: ακριβή και επικαιροποιημένα (βλ. Άρθρο 5 παρ. 1 στοιχείο δ του [ΓΚΠΔ])·
  5. **διάρκειες αποθήκευσης**: περιορισμένες (βλ. Άρθρο 5 παρ. 1 στοιχείο ε του [ΓΚΠΔ]).
- Ελέγξτε ότι η βελτίωση του τρόπου με τον οποίο κάθε σημείο σχεδιάζεται, διευκρινίζεται και δικαιολογείται, σύμφωνα με τον [ΓΚΠΔ], είτε δεν είναι απαραίτητη είτε δεν είναι εφικτή.
- Ανάλογα με την περίπτωση, επανεξετάστε την περιγραφή τους ή προτείνετε πρόσθετα μέτρα.

2.2 Αξιολόγηση των μέτρων που προστατεύουν τα δικαιώματα των υποκειμένων των δεδομένων

- Αναγνωρίστε ή καθορίστε και περιγράψτε τα **μέτρα** (υπάρχοντα ή σχεδιαζόμενα) **που έχουν επιλεγεί για τη συμμόρφωση με τις ακόλουθες νομικές απαιτήσεις** (είναι απαραίτητο να εξηγηθεί ο τρόπος με τον οποίο προορίζονται να εφαρμοστούν):
  1. **ενημέρωση** για τα υποκείμενα των δεδομένων (δίκαιη και διαφανής επεξεργασία, βλέπε Άρθρα 12, 13 και 14 του [ΓΚΠΔ])·
  2. **λήψη συγκατάθεσης**, κατά περίπτωση[13]: ρητή, μπορεί να αποδειχθεί και να ανακληθεί (βλ. Άρθρα 7 και 8 του [ΓΚΠΔ])·
  3. **άσκηση του δικαιώματος πρόσβασης και του δικαιώματος φορητότητας δεδομένων** (βλ. Άρθρα 15 και 20 του [ΓΚΠΔ])·
  4. **άσκηση των δικαιωμάτων διόρθωσης και διαγραφής** (βλέπε Άρθρα 16 και 17 του [ΓΚΠΔ])·
  5. **άσκηση του δικαιώματος περιορισμού της επεξεργασίας και του δικαιώματος εναντίωσης** (βλ. Άρθρα 18 και 21 του [ΓΚΠΔ])·
  6. **εκτελούντες την επεξεργασία**: προσδιορισμένοι και δεσμευόμενοι από σύμβαση (βλέπε Άρθρο 28 του [ΓΚΠΔ])·
  7. **διαβιβάσεις**: συμμόρφωση με τις υποχρεώσεις που αφορούν στη διαβίβαση δεδομένων εκτός του Ευρωπαϊκού Οικονομικού Χώρου (βλέπε Άρθρα 44 έως 49 του [ΓΚΠΔ]).
- Ελέγξτε ότι η βελτίωση κάθε μέτρου και της περιγραφής του, σύμφωνα με τον [ΓΚΠΔ], είτε δεν είναι απαραίτητη είτε δεν είναι εφικτή.
- Ανάλογα με την περίπτωση, επανεξετάστε την περιγραφή τους ή προτείνετε πρόσθετα μέτρα.

[11] Αποδείξτε επίσης ότι οι αποδέκτες είναι νόμιμοι.
[12] Αποδείξτε επίσης ότι οι αποδέκτες πρέπει πραγματικά να έχουν πρόσβαση στα δεδομένα.
[13] Αιτιολογήστε τις περιπτώσεις όπου δεν έχει ληφθεί συγκατάθεση.

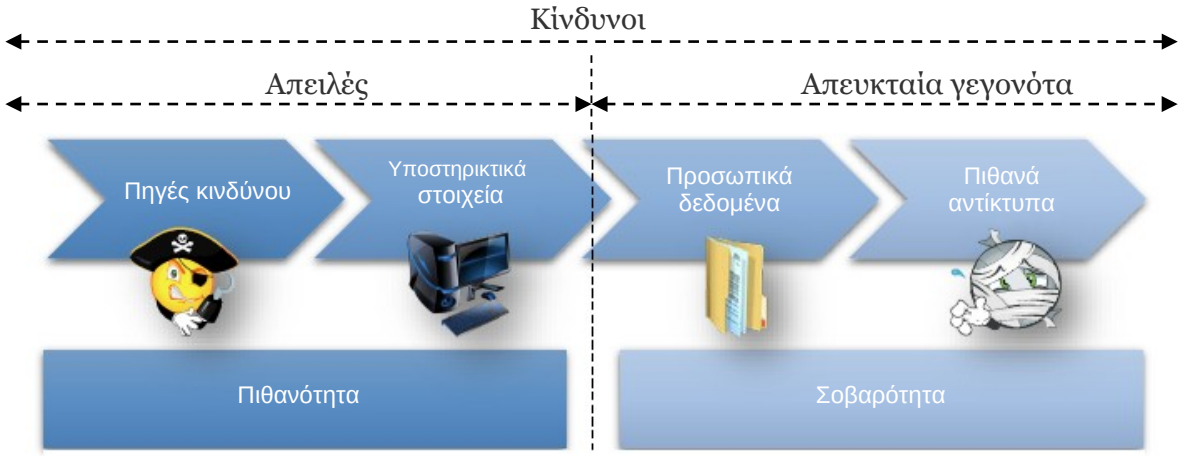
3 Μελέτη των κινδύνων που σχετίζονται με την ασφάλεια των δεδομένων[14]

Τι είναι ο κίνδυνος ιδιωτικότητας;

Ένας κίνδυνος είναι ένα υποθετικό σενάριο που περιγράφει ένα απευκταίο γεγονός και όλες τις απειλές που θα επέτρεπαν να συμβεί αυτό. Πιο συγκεκριμένα, περιγράφει:

- πώς πηγές κινδύνου (π.χ.: ένας υπάλληλος δωροδοκημένος από έναν ανταγωνιστή)
- θα μπορούσαν να εκμεταλλευτούν τα τρωτά σημεία των υποστηρικτικών στοιχείων (π.χ.: το σύστημα διαχείρισης αρχείων που επιτρέπει την παραποίηση δεδομένων)
- σε πλαίσιο απειλών (π.χ. κατάχρηση με αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου)
- και να επιτρέψουν την επέλευση απευκταίων γεγονότων (π.χ. αθέμιτη πρόσβαση σε προσωπικά δεδομένα)
- σε προσωπικά δεδομένα (π.χ. αρχείο πελάτη)
- δημιουργώντας έτσι αντίκτυπα στην ιδιωτική ζωή των υποκειμένων των δεδομένων (π.χ. ανεπιθύμητη άγρα πελατών, αισθήματα εισβολής στην ιδιωτικότητα, προσωπικά ή επαγγελματικά προβλήματα).

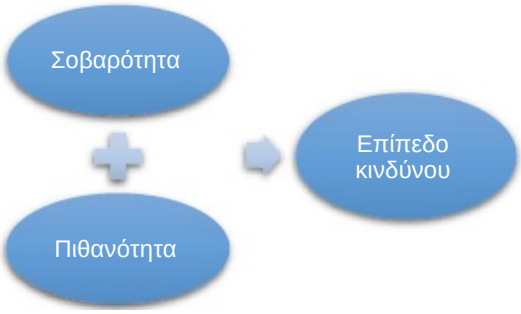
Το ακόλουθο διάγραμμα συνοψίζει όλες τις παραπάνω έννοιες:



Εικόνα 3 – Συστατικά στοιχεία κινδύνου

Το επίπεδο κινδύνου εκτιμάται ως προς την σοβαρότητα και την πιθανότητα:

- η **σοβαρότητα** αντιπροσωπεύει το μέγεθος ενός κινδύνου. Εξαρτάται κατά κύριο λόγο από τον επιζήμιο χαρακτήρα των πιθανών αντικτύπων[15].
- η **πιθανότητα** εκφράζει την δυνατότητα επέλευσης του κινδύνου. Εξαρτάται κυρίως από το επίπεδο ευπάθειας των υποστηρικτικών στοιχείων όταν βρίσκονται υπό απειλή και από το επίπεδο των ικανοτήτων των πηγών κινδύνου για την εκμετάλλευσή τους.



Σχήμα 4 - Παράγοντες που χρησιμοποιούνται για την εκτίμηση των κινδύνων

[14] βλέπε Άρθρο 32 του [ΓΚΠΔ].
[15] Στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (φύση δεδομένων, υποκείμενα των δεδομένων, σκοπός της επεξεργασίας, κλπ.).

3.1 Αξιολόγηση υφιστάμενων ή προγραμματισμένων μέτρων

Γενικά, εκτελείται από τον κύριο ανάδοχο[16] και στη συνέχεια αξιολογείται από έναν επικεφαλής για θέματα «Ασφάλειας δεδομένων»[17].

Στόχος: η απόκτηση καλής κατανόησης των μέτρων που συμβάλλουν στην ασφάλεια.

- ❑ Αναγνωρίστε ή καθορίστε **τα υφιστάμενα ή προγραμματισμένα μέτρα** (που έχουν ήδη αναληφθεί), τα οποία μπορούν να λάβουν τρεις διαφορετικές μορφές:
  1. **μέτρα που αφορούν ειδικά στα υπό επεξεργασία προσωπικά δεδομένα**: κρυπτογράφηση, ανωνυμοποίηση, κατανομή, έλεγχος πρόσβασης, ανιχνευσιμότητα, *κλπ.*·
  2. **γενικά μέτρα ασφαλείας σχετικά με το σύστημα στο οποίο πραγματοποιείται η επεξεργασία**: ασφάλεια λειτουργίας, αντίγραφα ασφαλείας, ασφάλεια υλικού, *κλπ.*·
  3. **οργανωτικά μέτρα (διακυβέρνηση)**: πολιτική, διαχείριση έργων, διαχείριση προσωπικού, διαχείριση περιστατικών και παραβιάσεων, σχέσεις με τρίτους, *κλπ.*·
- ❑ Ελέγξτε ότι η βελτίωση κάθε μέτρου και της περιγραφής του, σύμφωνα με τις βέλτιστες πρακτικές ασφαλείας, είτε δεν είναι απαραίτητη είτε δεν είναι δυνατή.
- ❑ Κατά περίπτωση, επανεξετάστε την περιγραφή τους ή προτείνετε πρόσθετα μέτρα.

3.2 Αξιολόγηση κινδύνου: ενδεχόμενες παραβιάσεις ιδιωτικότητας

Γενικά εκτελείται από τον ιδιοκτήτη του έργου και στη συνέχεια αξιολογείται από έναν επικεφαλής για θέματα «Προστασίας δεδομένων».

Στόχος: να αποκτήσετε μια καλή κατανόηση των αιτιών και των συνεπειών των κινδύνων.

- ❑ Για κάθε απευκταίο γεγονός (αθέμιτη πρόσβαση σε προσωπικά δεδομένα[18], ανεπιθύμητη τροποποίηση προσωπικών δεδομένων[19] και εξαφάνιση προσωπικών δεδομένων[20]):
  1. προσδιορίστε τις πιθανές **επιπτώσεις** στην ιδιωτικότητα των υποκειμένων των δεδομένων, εάν αυτό συμβεί[21]·
  2. εκτιμήστε τη **σοβαρότητά** του, ιδίως ανάλογα με τον επιζήμιο χαρακτήρα των πιθανών επιπτώσεων και, ενδεχομένως, τα μέτρα που είναι πιθανό να τις τροποποιήσουν·
  3. αναγνωρίστε τις **απειλές** για τα υποστηρικτικά των προσωπικών δεδομένων στοιχεία που θα μπορούσαν να οδηγήσουν σε αυτό το απευκταίο γεγονός[22] και τις **πηγές κινδύνου** που θα μπορούσαν να το προκαλέσουν·
  4. εκτιμήστε την **πιθανότητά** του, ιδίως ανάλογα με το επίπεδο ευπάθειας των υποστηρικτικών στοιχείων για τα προσωπικά δεδομένα, το επίπεδο των ικανοτήτων των πηγών κινδύνου για την εκμετάλλευσή τους και τα μέτρα που ενδέχεται να τα τροποποιήσουν.
- ❑ Προσδιορίστε το αν οι κίνδυνοι που αναγνωρίστηκαν με αυτόν τον τρόπο[23] μπορούν να θεωρηθούν αποδεκτοί ενόψει των υφιστάμενων ή προγραμματισμένων μέτρων.
- ❑ Αν όχι, προτείνετε πρόσθετα μέτρα και επαναξιολογήστε το επίπεδο κάθε κινδύνου ενόψει των τελευταίων, ώστε να προσδιορίσετε τους εναπομένοντες κινδύνους.

[16] Μπορεί να είναι ανάδοχος, αντιπρόσωπος ή εκτελών την επεξεργασία.
[17] Υπεύθυνος Ασφάλειας Κεντρικών συστημάτων Πληροφορικής (ΥΑΚΠ – CISO) ή άλλος.
[18] Καθίστανται γνωστά σε μη εξουσιοδοτημένα άτομα (παραβίαση της εμπιστευτικότητας των προσωπικών δεδομένων).
[19] Έχουν μεταβληθεί ή τροποποιηθεί (παραβίαση της ακεραιότητας των προσωπικών δεδομένων).
[20] Δεν είναι διαθέσιμα ή δεν είναι πλέον διαθέσιμα (παραβίαση της διαθεσιμότητας των προσωπικών δεδομένων).
[21] Απαντήστε στην ερώτηση «Τι φοβόμαστε ότι θα μπορούσε να συμβεί στα υποκείμενα δεδομένων;».
[22] Απαντήστε στην ερώτηση «Πώς ενδέχεται να συμβεί αυτό;».
[23] Ο κίνδυνος βασίζεται σε ένα απευκταίο γεγονός και σε όλες τις απειλές που θα το επέτρεπαν.

4 Επικύρωση της PIA

Γενικά εκτελείται από τον υπεύθυνο επεξεργασίας, με τη βοήθεια ενός επικεφαλής για θέματα "Προστασίας Δεδομένων".

Στόχος: να αποφασιστεί εάν θα γίνει αποδεκτή ή όχι η PIA υπό το φως των ευρημάτων της μελέτης.

4.1 Προετοιμασία των στοιχείων που απαιτούνται για την επικύρωση

- Ενοποίηση και παρουσίαση των πορισμάτων της μελέτης:
  1. προετοιμάστε μια οπτική παρουσίαση των **μέτρων που έχουν επιλεγεί για να διασφαλιστεί η συμμόρφωση με τις θεμελιώδεις αρχές**, ανάλογα με τη συμμόρφωσή τους με τον [ΓΚΠΔ] (π.χ.: εξαρτώμενοι από βελτίωση ή θεωρούμενοι συμβατοί)·
  2. προετοιμάστε μια οπτική παρουσίαση των **μέτρων που έχουν επιλεγεί για να συμβάλλουν στην ασφάλεια των δεδομένων**, ανάλογα με τη συμμόρφωσή τους με τις βέλτιστες πρακτικές ασφαλείας (π.χ.: εξαρτώμενοι από βελτίωση ή θεωρούμενοι συμβατοί)·
  3. χαρτογραφήστε οπτικά τους **κινδύνους** (αρχικούς και υπολειπόμενους, όπου χρειάζεται[24]) ανάλογα με τη σοβαρότητα και την πιθανότητα τους·
  4. καταρτίστε ένα **σχέδιο δράσης** με βάση τα πρόσθετα μέτρα που εντοπίστηκαν κατά τα προηγούμενα βήματα: για κάθε μέτρο, καθορίστε τουλάχιστον το πρόσωπο που είναι υπεύθυνο για την υλοποίησή του, το κόστος του (οικονομικό ή από την άποψη του φόρτου εργασίας) και το εκτιμώμενο χρονοδιάγραμμα.
- Καταχωρίστε επίσημα τη σκέψη των ενδιαφερομένων:
  1. τις **συμβουλές του υπεύθυνου για θέματα «Προστασίας Δεδομένων»** (βλ. Άρθρο 35, παράγραφος 2 του [ΓΚΠΔ]) ·
  2. την **άποψη των υποκειμένων των δεδομένων ή των εκπροσώπων τους** (βλ. Άρθρο 35 παράγραφος 9 του [ΓΚΠΔ]).

4.2 Επίσημη επικύρωση

- Αποφασίστε εάν τα επιλεγμένα μέτρα, οι υπολειπόμενοι κίνδυνοι και το σχέδιο δράσης είναι αποδεκτά, με αιτιολόγηση, υπό το πρίσμα των προηγουμένως αναγνωρισμένων διακυβευμάτων και των απόψεων των ενδιαφερομένων. Με αυτόν τον τρόπο, η PIA μπορεί να θεωρείται:
  1. επικυρωμένη·
  2. εξαρτώμενη από βελτίωση (εξηγήστε με ποιον τρόπο)·
  3. απορριφθείσα (μαζί με την υπό εξέταση επεξεργασία).
- Όπου είναι απαραίτητο, επαναλάβετε τα προηγούμενα βήματα ώστε να είναι δυνατή η επικύρωση της PIA.

[24] Κίνδυνοι που παραμένουν μετά την εφαρμογή των μέτρων.

Παραρτήματα

Ορισμοί

Σημείωση: Οι λέξεις στις παρενθέσεις αντιστοιχούν στους συντομότερους όρους που χρησιμοποιούνται σε αυτό το έγγραφο.

Μέτρο	Δράση που πρέπει να αναληφθεί. *Σημείωση: αυτή μπορεί να είναι τεχνική ή οργανωτική και ενδέχεται να συνεπάγεται την εφαρμογή των θεμελιωδών αρχών ή την αποφυγή, μείωση, μεταφορά ή ανάληψη όλων ή μέρους των κινδύνων.*
Υπεύθυνος επεξεργασίας	Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, ο οργανισμός ή άλλος φορέας ο οποίος, από μόνος του ή από κοινού με άλλους, καθορίζει τους σκοπούς και τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και τα μέσα αυτής της επεξεργασίας καθορίζονται από το δίκαιο της Ένωσης ή του Κράτους Μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον καθορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή των Κρατών Μελών. [ΓΚΠΔ] *Σημείωση: εκτός εάν ορίζεται ρητά από νομοθετικές ή κανονιστικές διατάξεις σχετικά με αυτή την επεξεργασία.* [DP-Act]
Υποκείμενα δεδομένων	Τα πρόσωπα στα οποία αναφέρονται τα δεδομένα που αφορά η επεξεργασία. [DP-Act]
Απευκταίο γεγονός	Πιθανή παραβίαση δεδομένων που ενδέχεται να έχει επιπτώσεις στην ιδιωτικότητα των υποκειμένων των δεδομένων.
Πιθανότητα	Εκτίμηση της δυνατότητας επέλευσης του κινδύνου. *Σημείωση: αυτή εξαρτάται κυρίως από το επίπεδο των εκμεταλλεύσιμων τρωτών σημείων και από το επίπεδο των ικανοτήτων των πηγών κινδύνου για την εκμετάλλευσή τους.*
Δεδομένα προσωπικού χαρακτήρα (προσωπικά δεδομένα)	Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (εφεξής καλούμενο «υποκείμενο των δεδομένων»)· το «ταυτοποιήσιμο φυσικό πρόσωπο» είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. [ΓΚΠΔ] *Σημείωση: Για να προσδιοριστεί αν ένα άτομο είναι ταυτοποιήσιμο, θα πρέπει να ληφθούν υπόψη όλα τα μέσα που μπορεί να χρησιμοποιήσει ή στα οποία μπορεί να έχει πρόσβαση ο υπεύθυνος επεξεργασίας ή οποιοδήποτε άλλο πρόσωπο.* [DP-Act]
Επεξεργασία δεδομένων προσωπικού χαρακτήρα (επεξεργασία)	Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή. [ΓΚΠΔ]
Κίνδυνος	Σενάριο που περιγράφει ένα απευκταίο γεγονός και όλες τις απειλές που το καθιστούν πιθανό. *Σημείωση: εκτιμάται ως προς τη σοβαρότητα και την πιθανότητα.*
Πηγή κινδύνου	Πρόσωπο ή μη ανθρώπινη πηγή που μπορεί να προκαλέσει κίνδυνο. *Σημείωση: αυτή η πηγή μπορεί να ενεργήσει άθελά της ή σκόπιμα.*

Σοβαρότητα	Εκτίμηση του μεγέθους των πιθανών επιπτώσεων στην ιδιωτικότητα των υποκειμένων των δεδομένων. *Σημείωση: αυτό εξαρτάται κυρίως από τον επιζήμιο χαρακτήρα των πιθανών επιπτώσεων.*
Υποστηρικτικό στοιχείο	Στοιχείο επί του οποίου βασίζονται προσωπικά δεδομένα. *Σημείωση: αυτό μπορεί να είναι υλισμικό, λογισμικό, δίκτυα, άνθρωποι, χαρτί ή κανάλια μετάδοσης χαρτιού.*
Απειλή	Διαδικασία που περιλαμβάνει μία ή περισσότερες μεμονωμένες ενέργειες σχετικά με υποστηρικτικά των προσωπικών δεδομένων στοιχεία. *Σημείωση: χρησιμοποιείται, σκόπιμα ή άλλως, από πηγές κινδύνου και μπορεί να προκαλέσει ένα απευκταίο γεγονός.*

Βιβλιογραφία

[Χάρτης της ΕΕ]	Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, 2010/C 83/02.
[ΓΚΠΔ]	Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).
[DP-Act]	Γαλλικός Νόμος περί Προστασίας Δεδομένων υπ' αριθ. 78-17 της 6ης Ιανουαρίου 1978, όπως τροποποιήθηκε[25].
[Κατευθυντήριες Γραμμές Ομάδας Εργασίας άρθρου 29]	Κατευθυντήριες Γραμμές για την Εκτίμηση Αντικτύπου στην Προστασία των Δεδομένων (DPIA) και τον προσδιορισμό κατά πόσον η επεξεργασία είναι «πιθανό να οδηγήσει σε υψηλό κίνδυνο» για τους σκοπούς του Κανονισμού 2016/679, wp248rev.01, Ομάδα Εργασίας του άρθρου 29.
[EBIOS]	Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS / Έκφραση των Αναγκών και Προσδιορισμός των Στόχων Ασφαλείας, Μεθοδολογία διαχείρισης κινδύνων, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI / Γαλλική Εθνική Υπηρεσία Ασφάλειας Δικτύων και Πληροφοριών).
[ISO 31000]	ISO 31000: 2009, Διαχείριση κινδύνων - Αρχές και κατευθυντήριες γραμμές, ISO.

[25] Τροποποιήθηκε από τον Γαλλικό Νόμο υπ' αριθ. 2004-801 της 6ης Αυγούστου 2004 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και από τον Γαλλικό Νόμο υπ' αριθ. 2009-526 της 12ης Μαΐου 2009 για την απλούστευση και αποσαφήνιση της Γαλλικής νομοθεσίας και διευκόλυνση των διαδικασιών.

Σύνοψη των κριτηρίων των [Κατευθυντήριων Γραμμών της ΟΕ29]

Κριτήρια των [Κατευθυντήριων Γραμμών της ΟΕ29]	**Σύνοψη**	**Κεφάλαιο σε αυτόν τον οδηγό**
Παρέχεται συστηματική περιγραφή της επεξεργασίας (άρθρο 35 παράγραφος 7 στοιχείο α): - λαμβάνεται υπόψη η φύση, το πεδίο εφαρμογής, οι περιστάσεις και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90)· - καταγράφονται τα προσωπικά δεδομένα, οι παραλήπτες και η περίοδος για την οποία θα αποθηκεύονται τα προσωπικά δεδομένα· - παρέχεται λειτουργική περιγραφή της διαδικασίας της επεξεργασίας· - εντοπίζονται τα στοιχεία στα οποία βασίζονται τα προσωπικά δεδομένα (υλισμικό, λογισμικό, δίκτυα, άνθρωποι, χαρτί ή κανάλια μετάδοσης έγχαρτων εγγράφων)· - λαμβάνεται υπόψη η συμμόρφωση με τους εγκεκριμένους κώδικες δεοντολογίας (Άρθρο 35 παράγραφος 8).	☑	1. Μελέτη των περιστάσεων
Αξιολογείται η αναγκαιότητα και η αναλογικότητα (Άρθρο 35 παράγραφος 7 στοιχείο β): - καθορίζονται τα μέτρα που προβλέπονται για τη συμμόρφωση με τον Κανονισμό (Άρθρο 35 παράγραφος 7 στοιχείο δ και αιτιολογική σκέψη 90), λαμβάνοντας υπόψη: - τα μέτρα που συμβάλλουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας με βάση: - καθορισμένους, ρητούς και νόμιμους σκοπούς (Άρθρο 5 παράγραφος 1 στοιχείο β)· - τη νομιμότητα της επεξεργασίας (Άρθρο 6)· - προσωπικά δεδομένα κατάλληλα, συναφή και περιορισμένα στο αναγκαίο (Άρθρο 5 παράγραφος 1 στοιχείο γ)· - περιορισμένη διάρκεια αποθήκευσης (Άρθρο 5 παράγραφος 1 στοιχείο ε)· - μέτρα που συμβάλλουν στα δικαιώματα των υποκειμένων των δεδομένων: - πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (Άρθρα 12, 13 και 14)· - δικαιώματα πρόσβασης και φορητότητας (Άρθρα 15 και 20)· - δικαιώματα διόρθωσης και διαγραφής (Άρθρα 16 και 17)· - δικαιώματα εναντίωσης και περιορισμού της επεξεργασίας (Άρθρα 16 και 21)· - εκτελούντες την επεξεργασία (Άρθρο 28)· - εγγυήσεις που αφορούν στις διεθνείς διαβιβάσεις (Κεφάλαιο V).	☑	2. Μελέτη των θεμελιωδών αρχών
Γίνεται διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (άρθρο 35 παράγραφος 7 στοιχείο γ): - αξιολογούνται η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (βλέπε αιτιολογική σκέψη 84) ή, ειδικότερα, για κάθε κίνδυνο (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων) από την οπτική γωνία των υποκειμένων των δεδομένων: - λαμβάνονται υπόψη οι πηγές κινδύνου (αιτιολογική σκέψη 90)· - προσδιορίζονται οι πιθανές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περίπτωση αθέμιτης πρόσβασης, ανεπιθύμητης τροποποίησης και εξαφάνισης δεδομένων· - εντοπίζονται απειλές που θα μπορούσαν να οδηγήσουν σε αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων· - εκτιμάται η πιθανότητα και η σοβαρότητα (αιτιολογική σκέψη 90)· - καθορίζονται τα μέτρα που προβλέπονται για την αντιμετώπιση αυτών των κινδύνων (Άρθρο 35 παράγραφος 7 στοιχείο δ και αιτιολογική σκέψη 90).	☑	3. Μελέτη των κινδύνων ασφάλειας δεδομένων
Συμμετέχουν τα ενδιαφερόμενα μέρη: - ζητείται η συμβουλή του ΥΠΔ (Άρθρο 35 παράγραφος 2)· - ζητούνται οι απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους (Άρθρο 35 παράγραφος 9).	☑	4. Επικύρωση της PIA

Το παρόν αποτελεί μετάφραση του πρωτότυπου αγγλικού κειμένου της CNIL.
Ο μεταφράσας δικηγόρος, Δημήτριος Τζέλλης, με email: Dimitris@Tzellis.gr