



**Διαδικασία Εκτίμησης Αντίκτυπου σχετικά με την Προστασία Δεδομένων**

|  |  |
| --- | --- |
| **Διαβάθμιση Εγγράφου:** | Εμπιστευτικό |
| **Έκδοση:** | **1** |
| **Ημερομηνία:** | **Νοέμβριος 2020** |
| **Συντάκτης Εγγράφου:** | **Ομάδα Υλοποίησης Συμμόρφωσης με το ΓΚΠΔ**  |
| **Ιδιοκτήτης Εγγράφου:** | **Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης**  |

**Ιστορικό Αναθεώρησης**

|  |  |  |  |
| --- | --- | --- | --- |
| **Έκδοση** | **Ημερομηνία** | **Συντάκτης Αναθεώρησης** | **Σύνοψη Αλλαγών** |
|  |  |  |  |
|  |  |  |  |

**Διανομή**

|  |  |
| --- | --- |
| **Όνομα** | **Τίτλος** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Έγκριση**

|  |  |  |  |
| --- | --- | --- | --- |
| **Όνομα** | **Θέση** | **Υπογραφή** | **Ημερομηνία** |
|  |  |  |  |

**Περιεχόμενα**

[1 Εισαγωγή 3](#_Toc39425201)

[1.1 Ορισμοί 3](#_Toc39425202)

[2 Διαδικασία Εκτίμησης Αντίκτυπου Σχετικά με την Προστασία Δεδομένων 5](#_Toc39425203)

[2.1 Διάγραμμα Διαδικασίας 5](#_Toc39425204)

[2.2 Καθορισμός της Ανάγκης και του Πλαισίου 6](#_Toc39425205)

[2.3 Τεκμηρίωση της Χρήσης Προσωπικών Δεδομένων 7](#_Toc39425206)

[2.4 Προσδιορισμός των Κινδύνων 8](#_Toc39425207)

[2.4.1 Προσδιορισμός των Σεναρίων Κινδύνου 8](#_Toc39425208)

[2.5 Ανάλυση των Κινδύνων 8](#_Toc39425209)

[2.5.1 Αξιολόγηση της πιθανότητας 8](#_Toc39425210)

[2.5.2 Εκτίμηση του Αντίκτυπου 9](#_Toc39425211)

[2.5.3 Διαβάθμιση Κινδύνου 12](#_Toc39425212)

[2.6 Αξιολόγηση των Κινδύνων 12](#_Toc39425213)

[2.7 Καθορισμός Σχεδίου Αντιμετώπισης Κινδύνων 13](#_Toc39425214)

[2.7.1 Επιλογές Αντιμετώπισης Κινδύνου 13](#_Toc39425215)

[2.7.2 Επιλογή των Ελέγχων 13](#_Toc39425216)

[2.7.3 Έκθεση της Εκτίμησης Αντίκτυπου Σχετικά με την Προστασία Δεδομένων 14](#_Toc39425217)

[2.8 Λήψη Έγκρισης της Διοίκησης για Υπολειπόμενους Κινδύνους 14](#_Toc39425218)

[2.9 Προηγούμενη Διαβούλευση με την Εποπτική Αρχή 14](#_Toc39425219)

[2.10 Εφαρμογή Ενεργειών Αντιμετώπισης Κινδύνων 15](#_Toc39425220)

[2.11 Παρακολούθηση και Αναφορά των Κινδύνων 15](#_Toc39425221)

[2.12 Τακτική επισκόπηση 15](#_Toc39425222)

[2.13 Ρόλοι και Ευθύνες 16](#_Toc39425223)

[2.13.1 Πίνακας ΥΛΣΕ (RACI) 16](#_Toc39425224)

[3 Συμπέρασμα 17](#_Toc39425225)

**Κατάλογος Σχημάτων**

[*Σχήμα 1 – Διάγραμμα Διαδικασίας Εκτίμησης Αντίκτυπου Σχετικά με την Προστασία Δεδομένων* 5](#_Toc512502968)

[*Σχήμα 2 - Διάγραμμα πίνακα κινδύνου* 12](#_Toc512502969)

**Κατάλογος Πινάκων**

[*Πίνακας 1 - Κατευθυντήριες οδηγίες σχετικά με την πιθανότητα κινδύνου* 9](#_Toc512502959)

[*Πίνακας 2 - Καθοδήγηση για τον αντίκτυπο του κινδύνου* 11](#_Toc512502960)

[*Πίνακας 3 – Διάγραμμα ΥΛΣΕ (RACI)* 16](#_Toc512502961)

# Εισαγωγή

Το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (ΑΠΘ) δεσμεύεται πλήρως να προστατεύει τα προσωπικά δεδομένα των φοιτητών, των εργαζομένων και των άλλων ενδιαφερόμενων μερών, σύμφωνα με τις απαιτήσεις του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679 της Ευρωπαϊκής Ένωσης. Λαμβάνουμε υπόψη την ιδιωτικότητα των προσωπικών δεδομένων με σοβαρότητα και εισάγουμε ποικιλία μεθόδων και ελέγχων για να διασφαλίσουμε ότι γνωρίζουμε ποια δεδομένα συλλέγουμε και διατηρούμε και ότι τα προστατεύουμε κατάλληλα.

Στο πλαίσιο αυτής της δέσμευσης, το ΑΠΘ διασφαλίζει ότι όλες οι λειτουργικές δραστηριότητες και τα έργα που αφορούν τη χρήση προσωπικών δεδομένων υπόκεινται σε αξιολόγηση αντίκτυπου προστασίας δεδομένων. Σκοπός της αξιολόγησης αυτής είναι να διασφαλιστεί ότι η χρήση των προσωπικών δεδομένων γίνεται πλήρως κατανοητή, ότι οι κίνδυνοι για τα δεδομένα αυτά εξετάζονται προσεκτικά και ότι θεσπίζονται όλα τα κατάλληλα μέτρα για την προστασία της κατά τη διάρκεια του κύκλου ζωής της.

Το παρόν έγγραφο καθορίζει τη διαδικασία αξιολόγησης αντίκτυπου προστασίας δεδομένων και, σε συνδυασμό με τις σχετικές μορφές και κατευθυντήριες γραμμές, θα πρέπει να χρησιμοποιείται για να διασφαλιστεί η εκπλήρωση των υποχρεώσεών μας και των πολιτικών μας σε αυτόν τον τομέα.

## Ορισμοί

Οι ακόλουθοι ορισμοί των όρων που χρησιμοποιούνται σε αυτό το έγγραφο διαδικασίας λαμβάνονται από τον GDPR:

*«προσωπικά δεδομένα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («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*

*«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*

*«ψευδωνυμοποίηση»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο;*

*«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 της επεξεργασίας ή τα ειδικά κριτήρια για το διορισμό του μπορούν να προβλεφθούν από το δίκαιο της Ένωσης ή των κρατών μελών;*

*«εκτελών την επεξεργασία»: φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας;*

# Διαδικασία Εκτίμησης Αντίκτυπου Σχετικά με την Προστασία Δεδομένων

## Διάγραμμα Διαδικασίας



*Σχήμα 1 – Διάγραμμα Διαδικασίας Εκτίμησης Αντίκτυπου Σχετικά με την Προστασία Δεδομένων*

## Καθορισμός της Ανάγκης και του Πλαισίου

Υπάρχουν ορισμένα κριτήρια που καθορίζουν πότε θα πρέπει να πραγματοποιηθεί εκτίμηση αντίκτυπου προστασίας δεδομένων στο πλαίσιο του ΑΠΘ . Ο Γενικός Κανονισμός Προστασίας Δεδομένων (Άρθρο 35) ορίζει ότι *απαιτείται* μια εκτίμηση αντίκτυπου όταν η προτεινόμενη επεξεργασία περιλαμβάνει:

* *συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,*
* *μεγάλη κλίμακα επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή*
* *συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα*.

*Σημείωση: Το άρθρο 9(1) αναφέρεται σε επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.*

Γενικά, το ΑΠΘ διευκρινίζει ότι οι εκτιμήσεις αντίκτυπου προστασίας δεδομένων είναι κατάλληλες για έργα όπου ισχύει ένα ή περισσότερα από τα ακόλουθα:

1. προσωπικά δεδομένα που θα συλλέγονται και θα υποβάλλονται σε επεξεργασία για πρώτη φορά
2. Προσωπικά δεδομένα που θα μοιραστούν με ανθρώπους ή οργανισμούς που προηγουμένως δεν είχαν πρόσβαση σε αυτά
3. αλλαγή χρήσης των υπαρχόντων προσωπικών δεδομένων
4. χρήση νέας τεχνολογίας που συλλέγει ή χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα, π.χ. βιομετρικά στοιχεία, αλλαγή λογισμικού
5. Επεξεργασία ευαίσθητων προσωπικών δεδομένων ( και κυρίως υγείας, βιομετρικά, γενετικά, ποινικά )
6. Δημιουργία profile ενός φυσικού προσώπου ( αξιολόγηση χαρακτήρα, συμπεριφοράς, εργασιακής ή εκπαιδευτικής απόδοσης, κοινωνικότητας κλπ)
7. Δεδομένα παρακολούθησης γεωγραφικής θέσης ή συμπεριφοράς
8. Μεγάλης κλίμακας δεδομένα ( ΑΠΔΠΧ: αν αφορούν >1000 άτομα) και ειδικά όταν αυτά δεν λαμβάνονται από τα φυσικά πρόσωπα
9. Δεδομένα από συνδυασμό διαφορετικών datasets
10. Επεξεργασία δεδομένων που μπορεί να οδηγήσει σε κίνδυνο την φυσική υγεία και ασφάλεια των προσώπων

Εάν υπάρχει αβεβαιότητα ως προς το κατά πόσον είναι σκόπιμο να διενεργηθεί εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων για ένα συγκεκριμένο έργο, εξ ορισμού η ομάδα του έργου πρέπει να πραγματοποιήσει μια εκτίμηση αντικτύπου. Μπορεί να ζητηθεί η γνώμη του Υπεύθυνου Προστασίας Δεδομένων για αποσαφήνιση και μπορεί να έχει εκδοθεί περαιτέρω καθοδήγηση από την Αρχή Προστασίας Προσωπικών Δεδομένων που εκπροσωπεί την ΕΕ εντός της χώρας ή την εποπτική αρχή των χωρών όπου θα διεξαχθεί η επεξεργασία, οπότε και θα πρέπει να ζητηθεί η γνώμη της.

Πρέπει να περιγραφεί το γενικό περιβάλλον εντός του οποίου πραγματοποιείται η εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων και να εξηγηθούν οι λόγοι αυτής. Αυτό θα πρέπει να περιλαμβάνει μια περιγραφή του εσωτερικού και εξωτερικού πλαισίου του έργου και των γενικών στόχων του.

Το πεδίο εφαρμογής της αξιολόγησης θα πρέπει επίσης να ορίζεται σαφώς. Αυτό μπορεί να εκφραστεί με βάση το καθορισμένο πεδίο εφαρμογής του ίδιου του έργου και μπορεί να περιλαμβάνει παράγοντες όπως:

* Γεωγραφική θέση π.χ. χώρες, γραφεία, κέντρα δεδομένων
* Οργανωσιακές μονάδες π.χ. συγκεκριμένα τμήματα
* Λειτουργική διαδικασία (ες)
* Υπηρεσίες, συστήματα και δίκτυα πληροφορικής
* Φοιτητές ή υπηρεσίες

Οποιαδήποτε συγκεκριμένη εξαίρεση στο πεδίο εφαρμογής θα πρέπει να αναφέρεται με λόγους.

## Τεκμηρίωση της Χρήσης Προσωπικών Δεδομένων

Θα πρέπει να συγκεντρωθεί και να τεκμηριωθεί ένα ενδεδειγμένο επίπεδο λεπτομέρειας όσον αφορά τα προσωπικά δεδομένα που σχετίζονται με το έργο, όπως:

* Ορισμοί των συγκεκριμένων στοιχείων δεδομένων που πρόκειται να αποθηκευτούν και να υποστούν επεξεργασία
* Πως θα αποκτηθούν τα δεδομένα
* Πως θα υποστούν επεξεργασία τα δεδομένα
* Χρονικά όρια διατήρησης των δεδομένων
* Πως θα αποθηκευτούν τα δεδομένα
* Πιθανές μελλοντικές χρήσεις των δεδομένων
* Που μπορεί να μεταφερθούν τα δεδομένα και κάτω από ποιες περιστάσεις
* Ποιος θα έχει πρόσβαση στα δεδομένα και πως

οι πληροφορίες αυτές μπορούν να συλλέγονται και να αναπαριστώνται από έναν κατάλληλο συνδυασμό μητρώων πληροφοριακών στοιχείων, διαγραμμάτων ροής και μέσω της χρήσης σχετικών εργαλείων χαρτογράφησης δεδομένων, εφόσον υπάρχουν.

## Προσδιορισμός των Κινδύνων

Η διαδικασία προσδιορισμού των κινδύνων για τα προσωπικά δεδομένα που συλλέγουμε, επεξεργαζόμαστε και διατηρούμε θα αποτελείται από τα ακόλουθα βήματα.

### Προσδιορισμός των Σεναρίων Κινδύνου

Ο προσδιορισμός των κινδύνων για τα ταυτοποιημένα ή ταυτοποιήσιμα πρόσωπα θα πραγματοποιηθεί με συνδυασμό ομαδικής συζήτησης και συνέντευξης με τα ενδιαφερόμενα μέρη.

Τα εν λόγω ενδιαφερόμενα μέρη θα περιλαμβάνουν συνήθως (όπου είναι δυνατόν):

* Διαχειριστής (ες) / υπεύθυνος (οι) για κάθε κρίσιμη λειτουργική δραστηριότητα
* Εκπρόσωποι των ατόμων που κανονικά εκτελούν κάθε πτυχή της δραστηριότητας
* Παρόχους των εισροών στη δραστηριότητα
* Αποδέκτες των αποτελεσμάτων της δραστηριότητας
* Κατάλληλα τρίτα μέρη με σχετικές γνώσεις
* Εκπρόσωποι εκείνων που παρέχουν υπηρεσίες υποστήριξης και πόρους στη δραστηριότητα
* Οποιοδήποτε άλλο μέρος θεωρείται ότι παρέχει χρήσιμη συμβολή στη διαδικασία προσδιορισμού κινδύνου

Οι εντοπισθέντες κίνδυνοι θα καταγράφονται με όσο το δυνατόν πληρέστερη περιγραφή που θα επιτρέπει την αξιολόγηση της πιθανότητας και της επίδρασης του κινδύνου. Κάθε κίνδυνος θα πρέπει επίσης να ανατεθεί σε έναν ιδιοκτήτη.

## Ανάλυση των Κινδύνων

Η ανάλυση κινδύνου στο πλαίσιο αυτής της διαδικασίας περιλαμβάνει την εκχώρηση μιας αριθμητικής τιμής α) στην πιθανότητα και β) στον αντίκτυπο ενός κινδύνου. Αυτές οι τιμές στη συνέχεια πολλαπλασιάζονται για να φθάσουν σε ένα επίπεδο ταξινόμησης υψηλού, μεσαίου ή χαμηλού κινδύνου.

### Αξιολόγηση της πιθανότητας

Πρέπει να γίνει εκτίμηση της πιθανότητας εμφάνισης κινδύνου. Αυτό θα πρέπει να λαμβάνει υπόψη το αν έχει συμβεί ξανά είτε στο Πανεπιστήμιο είτε σε παρόμοιους φορείς στον ίδιο κλάδο ή στον ίδιο τόπο και εάν υπάρχει επαρκές κίνητρο, ευκαιρία και ικανότητα για την αναγνώριση μιας απειλής.

Η πιθανότητα κάθε κινδύνου πρέπει να βαθμολογείται σε αριθμητική κλίμακα από 1 (χαμηλή) έως 5 (υψηλή). Γενικές οδηγίες για την έννοια κάθε βαθμού δίνονται στον πίνακα 1. Κατά την εκτίμηση της πιθανότητας εμφάνισης κινδύνου πρέπει να λαμβάνονται υπόψη οι υπάρχοντες έλεγχοι. Αυτό μπορεί να απαιτεί την εκτίμηση της αποτελεσματικότητας των υφιστάμενων ελέγχων.

Μπορούν να αποφασιστούν λεπτομερέστερες οδηγίες για κάθε βαθμό πιθανότητας, ανάλογα με το αντικείμενο της εκτίμησης κινδύνου.

|  |  |  |
| --- | --- | --- |
| **Βαθμός** | **Περιγραφή** | **Σύνοψη** |
| 1 | Εντελώς Απίθανο | Δεν έχει συμβεί ποτέ πριν και δεν υπάρχει λόγος να πιστεύουμε ότι είναι πλέον πιθανό τώρα. |
| 2 | Σχεδόν Απίθανο | Υπάρχει μια πιθανότητα να συμβεί, αλλά μάλλον δεν θα συμβεί. |
| 3 | Πιθανό | Σε ισορροπία, ο κίνδυνος είναι πιθανότερο να συμβεί. |
| 4 | Πολύ πιθανό | Θα ήταν έκπληξη εάν ο κίνδυνος δεν συνέβη ούτε με βάση την προηγούμενη συχνότητα ούτε με τις τρέχουσες συνθήκες |
| 5 | Σχεδόν βέβαιο | Είτε συμβαίνει ήδη τακτικά είτε υπάρχει κάποιος λόγος να πιστέψουμε ότι είναι σχεδόν επικείμενο |

*Πίνακας 1 - Κατευθυντήριες οδηγίες σχετικά με την πιθανότητα κινδύνου*

Η λογική της κατανομής του βαθμού που δίδεται, θα πρέπει να καταγράφεται για να διευκολύνει την κατανόηση και να επιτρέπει την επαναληψιμότητα σε μελλοντικές εκτιμήσεις.

### Εκτίμηση του Αντίκτυπου

Θα πρέπει να δοθεί μια εκτίμηση του αντικτύπου που θα μπορούσε να έχει ο κίνδυνος στο Πανεπιστήμιο. Αυτό θα πρέπει να λαμβάνει υπόψη τους υφιστάμενους ελέγχους που μειώνουν τον αντίκτυπο, εφόσον οι έλεγχοι αυτοί θεωρούνται αποτελεσματικοί.

Θα πρέπει να εξεταστεί ο αντίκτυπος στους ακόλουθους τομείς:

* Γενικές επιπτώσεις στο Υποκείμενο των δεδομένων
* Υγεία και ασφάλεια του Υποκειμένου των δεδομένων
* Οικονομικά του Πανεπιστημίου
* Φήμη του Πανεπιστημίου
* Νομικές, συμβατικές ή οργανωτικές υποχρεώσεις

Η επίπτωση κάθε κινδύνου πρέπει να βαθμολογείται σε αριθμητική κλίμακα από 1 (χαμηλή) έως 5 (υψηλή). Γενικές οδηγίες για τη σημασία κάθε βαθμού δίνονται στον πίνακα 2.

Λεπτομερέστερη καθοδήγηση μπορεί να οριστεί για κάθε βαθμό επίπτωσης, ανάλογα με το αντικείμενο της εκτίμησης κινδύνου.

Η λογική της κατανομής του βαθμού που δίδεται θα πρέπει να καταγράφεται για να διευκολύνει την κατανόηση και να επιτρέπει την επαναληψιμότητα σε μελλοντικές εκτιμήσεις.

| **Βαθμός** | **Περιγραφή** | **Επίπτωση στο υποκείμενο των δεδομένων** | **Υγεία και Ασφάλεια** | **Οικονομική Επίπτωση** | **Επίπτωση στην Φήμη** | **Νομικές Επιπτώσεις** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Αμελητέος | Κανένα αποτέλεσμα | Πολύ μικρός πρόσθετος κίνδυνος | Πολύ λίγο ή καθόλου | Αμελητέα | Δεν υπάρχουν επιπτώσεις |
| 2 | Μικρός | Τα άτομα μπορεί να αντιμετωπίσουν μερικές δευτερεύουσες δυσκολίες, τις οποίες θα ξεπεράσουν χωρίς κανένα πρόβλημα (χρόνος ξοδεύοντας πληροφορίες, ενόχληση, ερεθισμούς κλπ.). | Μέσα στα επιτρεπόμενα όρια | Μερική | Μικρή | Μικρός κίνδυνος μη συμμόρφωσης |
| 3 | Μέτριος | Τα άτομα μπορεί να αντιμετωπίσουν σημαντικές δυσκολίες, τις οποίες θα μπορέσουν να ξεπεράσουν παρά ορισμένες δυσκολίες (επιπλέον έξοδα, άρνηση πρόσβασης σε υπηρεσίες, φόβος, έλλειψη κατανόησης, άγχος, μικρές σωματικές ασθένειες κ.λπ.). | Αυξημένος κίνδυνος που απαιτεί άμεση προσοχή | Ανεπιθύμητη αλλά μπορεί να αντιμετωπιστεί  | Μέτρια | Σε σαφή κίνδυνο παράνομης λειτουργίας |
| 4 | Υψηλός | Τα άτομα μπορούν να αντιμετωπίσουν σημαντικές συνέπειες, τις οποίες θα πρέπει να αντιμετωπίσουν, αν και με σοβαρές δυσκολίες (υπεξαίρεση κεφαλαίων, μαύρη λίστα από χρηματοπιστωτικά ιδρύματα, υλικές ζημιές, απώλεια απασχόλησης, κλήτευση, επιδείνωση της υγείας κ.λπ.). | Σημαντικός κίνδυνος για τη ζωή | Σοβαρή επίδραση στα οικονομικά του Πανεπιστημίου | Υψηλή | Παράνομη λειτουργία σε ορισμένες περιοχές |
| 5 | Πολύ υψηλός | Άτομα που ενδέχεται να αντιμετωπίσουν σημαντικές ή ακόμη και μη αναστρέψιμες συνέπειες, τις οποίες δεν μπορούν να ξεπεράσουν (ανικανότητα προς εργασία, μακροχρόνιες ψυχολογικές ή σωματικές ασθένειες, θάνατος κλπ.). | Πραγματική ή ισχυρά πιθανή απώλεια ζωής | Παράλυση. Ενδέχεται να περιοριστούν δραστηριότητες του Πανεπιστημίου | Πολύ υψηλή | Σοβαρά πρόστιμα και πιθανή φυλάκιση προσωπικού |

*Πίνακας 2 - Καθοδήγηση για τον αντίκτυπο του κινδύνου*

### Διαβάθμιση Κινδύνου

Με βάση την αξιολόγηση του βαθμού πιθανότητας και επίπτωσης, υπολογίζεται ένας βαθμός για κάθε κίνδυνο πολλαπλασιάζοντας τους δύο αριθμούς. Αυτή η βαθμολογία χρησιμοποιείται στη συνέχεια για να αποφασίσει την ταξινόμηση του κινδύνου με βάση τον πίνακα που φαίνεται στο σχήμα 2.

Σε κάθε κίνδυνο θα δοθεί μια διαβάθμιση με βάση τη βαθμολογία του ως εξής:

* ΥΨΗΛΟΣ – 12 ή παραπάνω
* ΜΕΤΡΙΟΣ – από 5 έως και 10
* ΧΑΜΗΛΟΣ – από 1 έως και 4



*Σχήμα 2 - Διάγραμμα πίνακα κινδύνου*

Η ταξινόμηση κάθε κινδύνου θα καταγραφεί ως εισροή στο στάδιο αξιολόγησης του κινδύνου της διαδικασίας.

## Αξιολόγηση των Κινδύνων

Σκοπός της αξιολόγησης του κινδύνου είναι να αποφασιστεί ποιοι κίνδυνοι μπορούν να γίνουν δεκτοί και ποιοι πρέπει να αντιμετωπιστούν. Αυτό θα πρέπει να λαμβάνει υπόψη τα κριτήρια αποδοχής κινδύνου που καθορίζονται για αυτή τη συγκεκριμένη εκτίμηση επικινδυνότητας (βλ. *Κριτήρια Αποδοχής Κινδύνου* παραπάνω).

Ο πίνακας στο *Σχήμα 2* δείχνει τις διαβαθμίσεις του κινδύνου, όπου το πράσινο δείχνει ότι ο κίνδυνος είναι κάτω από το αποδεκτό όριο. Οι πορτοκαλί και κόκκινες περιοχές γενικά υποδεικνύουν ότι ο κίνδυνος δεν πληροί τα κριτήρια αποδοχής και έτσι είναι υποψήφιος για αντιμετώπιση.

Οι κίνδυνοι θα δοθούν κατά προτεραιότητα για αντιμετώπιση ανάλογα με τη βαθμολογία και την ταξινόμησή τους, έτσι ώστε να συνιστώνται κίνδυνοι πολύ υψηλού βαθμού πριν από αυτούς με χαμηλότερα επίπεδα έκθεσης για το Πανεπιστήμιο.

## Καθορισμός Σχεδίου Αντιμετώπισης Κινδύνων

Για τους κινδύνους που έχουν συμφωνηθεί ότι υπερβαίνουν το όριο αποδοχής από το ΑΠΘ θα διερευνηθούν οι επιλογές αντιμετώπισης.

Η γενική πρόθεση της αντιμετώπισης του κινδύνου είναι η μείωση της διαβάθμισης ενός κινδύνου σε αποδεκτό επίπεδο. Αυτό δεν είναι πάντα εφικτό, καθώς μερικές φορές αν και το αποτέλεσμα μειώνεται, παραμένει στην ίδια διαβάθμιση π.χ. μειώνοντας τη βαθμολογία από 8 σε 6 σημαίνει ότι εξακολουθεί να παραμένει ένας κίνδυνος μέσου επιπέδου. Το Πανεπιστήμιο μπορεί να αποφασίσει να αποδεχθεί αυτούς τους κινδύνους, ακόμη και αν παραμείνουν σε μεσαία βαθμολογία. Αυτές οι αποφάσεις πρέπει να καταγράφονται με κατάλληλη εξήγηση.

### Επιλογές Αντιμετώπισης Κινδύνου

Για την αντιμετώπιση των κινδύνων που έχουν συμφωνηθεί ως ανεπιθύμητοι μπορούν να εφαρμοστούν οι ακόλουθες επιλογές:

1. ***Τροποποιήστε τον κίνδυνο -*** εφαρμόστε τους κατάλληλους ελέγχους για να μειώσετε την πιθανότητα και / ή την επίδραση του κινδύνου.
2. ***Αποφύγετε*** τον κίνδυνο με τη λήψη μέτρων που σημαίνει ότι δεν ισχύει πλέον
3. ***Μοιραστείτε*** τον κίνδυνο με ένα άλλο μέρος, π.χ. ασφαλιστή ή προμηθευτή

Η κρίση θα χρησιμοποιηθεί στην απόφαση ως προς ποια πορεία δράσης πρέπει να ακολουθηθεί, βασιζόμενη σε μια καλή γνώση των περιστάσεων που περιβάλλουν τον κίνδυνο π.χ.

* Λειτουργική στρατηγική
* Κανονιστικές και νομοθετικές εκτιμήσεις
* Τεχνικά θέματα
* Εμπορικά και συμβατικά θέματα

Ο Διαχειριστής Κινδύνου θα διασφαλίσει τη διαβούλευση με όλα τα μέρη που έχουν συμφέρον ή σχέση με τη μεταχείριση του κινδύνου, συμπεριλαμβανομένου του κατόχου του κινδύνου.

### Επιλογή των Ελέγχων

Θα προσδιοριστούν κατάλληλοι έλεγχοι για να μειωθεί η πιθανότητα ή ο αντίκτυπος (ή και τα δύο) κάθε κινδύνου προκειμένου να βρεθεί εντός αποδεκτών ορίων.

### Έκθεση της Εκτίμησης Αντίκτυπου Σχετικά με την Προστασία Δεδομένων

Η αξιολόγηση των επιλογών αντιμετώπισης θα έχει ως αποτέλεσμα την εκπόνηση της έκθεσης της εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων, η οποία θα περιλαμβάνει:

* Περιγραφή των προτεινόμενων διαδικασιών επεξεργασίας και των σχετικών προσωπικών δεδομένων
* Τους σκοπούς της επεξεργασίας συμπεριλαμβανομένου, κατά περίπτωση, το νόμιμο συμφέρον του υπεύθυνου επεξεργασίας των προσωπικών δεδομένων, όπως ορίζεται από το GDPR
* Αξιολόγηση της αναγκαιότητας και της αναλογικότητας της επεξεργασίας
* Τα αποτελέσματα της εκτίμησης των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
* Εάν συνιστάται κάθε κίνδυνος για αποδοχή ή αντιμετώπιση
* Προτεραιότητα των κινδύνων για αντιμετώπιση
* Τους ιδιοκτήτες κινδύνων
* Την συνιστώμενη επιλογή αντιμετώπισης
* Τον έλεγχο (ους) που πρέπει να εφαρμοστούν
* Την ευθύνη για τις προσδιορισμένες δράσεις
* Χρονοδιαγράμματα για δράσεις
* Τα επίπεδα υπολειμμάτων κινδύνου μετά την εφαρμογή των ελέγχων

## Λήψη Έγκρισης της Διοίκησης για Υπολειπόμενους Κινδύνους

Σε κάθε στάδιο της διαδικασίας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, η διοίκηση θα ενημερώνεται για την πρόοδο και τις αποφάσεις που λαμβάνονται, συμπεριλαμβανομένης της επίσημης υπογραφής των προτεινόμενων υπολειπόμενων κινδύνων. Η διοίκηση θα εγκρίνει την έκθεση της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων και θα εξετάζει σε ποιο βαθμό θα πρέπει να δημοσιοποιείται η έκθεση, είτε σε πλήρη μορφή είτε συνοπτικά.

Η υπογραφή θα υποδεικνύεται σύμφωνα με τα πρότυπα τεκμηρίωσης του ΑΠΘ . Εκτός από τη γενική έγκριση της διοίκησης, η αποδοχή ή η αντιμετώπιση κάθε κινδύνου πρέπει να υπογράφεται από τον αντίστοιχο ιδιοκτήτη του κινδύνου.

## Προηγούμενη Διαβούλευση με την Εποπτική Αρχή

Σε περίπτωση που τα αποτελέσματα της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων δείχνουν υψηλό επίπεδο κινδύνου πριν από την εφαρμογή των αναγνωρισμένων ελέγχων, ο GDPR απαιτεί τη διαβούλευση με την εποπτική αρχή πριν από οποιαδήποτε επεξεργασία.

Πρέπει να παρέχονται οι ακόλουθες πληροφορίες:

* Λεπτομέρειες σχετικά με τις αντίστοιχες ευθύνες του υπεύθυνου επεξεργασίας, των από κοινού υπεύθυνων επεξεργασίας και του εκτελούντος την επεξεργασία, όπου είναι δυνατόν
* Οι σκοποί και τα μέσα της επεξεργασίας
* Τα στοιχεία ελέγχου που θα εφαρμοστούν για την προστασία των δεδομένων
* Στοιχεία επικοινωνίας για τον υπεύθυνο προστασίας δεδομένων (κατά περίπτωση)
* Αντίγραφο της έκθεσης της εκτίμησης αντικτύπου

Η Εποπτική Αρχή έχει οκτώ εβδομάδες (επεκτάσιμες για έξι επιπλέον εβδομάδες) προκειμένου να αποφανθεί σχετικά με την προτεινόμενη επεξεργασία και, ενδεχομένως, να δώσει λεπτομέρειες για το τι πρέπει να γίνει για να είναι η επεξεργασία αποδεκτή σύμφωνα με τον GDPR.

## Εφαρμογή Ενεργειών Αντιμετώπισης Κινδύνων

Μόλις εγκριθεί το σχέδιο αντιμετώπισης κινδύνου, οι απαραίτητες ενέργειες θα πρέπει να παρακολουθούνται και να ολοκληρώνονται ως μέρος του καθημερινού ελέγχου του έργου. Σε περίπτωση καθυστέρησης ή αδυναμίας ολοκλήρωσης οποιωνδήποτε ενεργειών, οι συνέπειες αυτής στην προστασία των προσωπικών δεδομένων πρέπει να αξιολογηθούν από τη διοίκηση και να ληφθεί απόφαση για το τι πρέπει να γίνει στη συνέχεια. Εάν ο μη αντιμετωπίσιμος κίνδυνος είναι αρκετά σοβαρός, αυτό μπορεί να έχει σημαντικό αντίκτυπο στη βιωσιμότητα του έργου από άποψη συμμόρφωσης και να ζητηθούν συμβουλές από τον Υπεύθυνο Προστασίας Δεδομένων ή / και την Εποπτική Αρχή της χώρας ή των χωρών που επηρεάζονται.

## Παρακολούθηση και Αναφορά των Κινδύνων

Στο πλαίσιο της εφαρμογής των νέων ελέγχων και της διατήρησης των υπαρχόντων, θα προσδιοριστούν βασικοί δείκτες απόδοσης οι οποίοι θα επιτρέπουν τη μέτρηση της επιτυχίας των ελέγχων στην αντιμετώπιση των σχετικών κινδύνων.

Οι δείκτες αυτοί θα γνωστοποιούνται σε τακτική βάση και θα παρέχονται πληροφορίες για τις τάσεις έτσι ώστε να εντοπίζονται και να αντιμετωπίζονται οι καταστάσεις εξαίρεσης στο πλαίσιο της διαδικασίας ανασκόπησης της διοίκησης.

## Τακτική επισκόπηση

Εκτός από μια πλήρη ετήσια ανασκόπηση, οι εκτιμήσεις κινδύνου θα αξιολογούνται σε τακτική βάση, ώστε να διασφαλίζεται ότι παραμένουν σε ισχύ και ότι οι ισχύοντες έλεγχοι είναι έγκυροι. Οι σχετικές εκτιμήσεις κινδύνου θα επανεξεταστούν επίσης κατά τις σημαντικές αλλαγές στο πανεπιστήμιο, όπως οι μετακινήσεις αρχείων, η δημιουργία νέων Τμημάτων ή οι νέες ή τροποποιημένες υπηρεσίες πληροφορικής.

## Ρόλοι και Ευθύνες

Στο πλαίσιο της διαδικασίας εκτίμησης των κινδύνων, υπάρχουν ορισμένοι βασικοί ρόλοι που συμμετέχουν στην εξασφάλιση της ταυτοποίησης, της αντιμετώπισης και της διαχείρισης όλων των κινδύνων. Αυτοί οι ρόλοι παρουσιάζονται στον παρακάτω πίνακα ΥΑΣΕ (RACI), μαζί με τις σχετικές ευθύνες τους σε κάθε στάδιο της διαδικασίας.

### Πίνακας ΥΛΣΕ (RACI)

Ο παρακάτω πίνακας διευκρινίζει τις ευθύνες-ρόλους σε κάθε βήμα χρησιμοποιώντας το μοντέλο ΥΛΣΕ (RACI), δηλαδή:

Υ= Υπεύθυνος (Responsible), Λ= Λογοδοτών (Accountable), Σ= Συμβουλευτικός (Consulted), Ε= Ενημερωτικός (Informed)

| **Ρόλος:** | **Επικεφαλής της Αξιολόγησης** | **Ιδιοκτήτες κινδύνου** | **Ανώτατη Διοίκηση** |
| --- | --- | --- | --- |
| **Βήμα** |
| Καθορισμός της ανάγκης και του πλαισίου | Υ | Σ | Λ |
| Καταγραφή της χρήσης προσωπικών δεδομένων | Υ | Σ | Λ |
| Προσδιορισμός των κινδύνων | Σ | Υ | Λ |
| Ανάλυση των κινδύνων | Σ | Υ | Λ |
| Αξιολόγηση των κινδύνων | Σ | Υ | Λ |
| Καθορισμός σχεδίου αντιμετώπισης κινδύνου | Υ | Σ | Λ |
| Έγκριση Διοίκησης για υπολειπόμενους κινδύνους | Σ | Σ | Λ/Υ |
| Εφαρμογή σχεδίου αντιμετώπισης κινδύνου | Υ | Υ | Λ/Υ |
| Παρακολούθηση και αναφορά | Υ | Ε | Λ |
| Τακτική επισκόπηση | Υ | Υ | Λ |

*Πίνακας 3 – Διάγραμμα ΥΛΣΕ (RACI)*

Περαιτέρω ρόλοι και ευθύνες μπορούν να προστεθούν στον παραπάνω πίνακα δεδομένου ότι η διαδικασία αξιολόγησης του αντίκτυπου προστασίας δεδομένων ωριμάζει μέσα στο ΑΠΘ .

# Συμπέρασμα

Η διαδικασία εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων είναι θεμελιώδους σημασίας για την εφαρμογή ενός επιτυχημένου έργου που χειρίζεται τα δεδομένα προσωπικού χαρακτήρα και αποτελεί σημαντικό μέρος της νομοθεσίας του GDPR. Μόνο με την πλήρη κατανόηση των κινδύνων όσον αφορά τα προσωπικά δεδομένα μπορεί το Πανεπιστήμιο να ελπίζει ότι οι έλεγχοι που διαθέτει θα επαρκούν για την παροχή του κατάλληλου επιπέδου προστασίας της ιδιωτικής ζωής και την τήρηση του υψηλού επιπέδου που αναμένεται από αυτόν.

Ακολουθώντας αυτή τη διαδικασία το ΑΠΘ θα καταφέρει να διασφαλίσει την αποτελεσματική διαχείριση και τον έλεγχο των κινδύνων που αντιμετωπίζει στην καθημερινή λειτουργία των δραστηριοτήτων του.