****

Ερωτηματολόγιο συλλογής πληροφοριών για την Εκτίμηση Αντικτύπου σχετικά με

την προστασία των προσωπικών δεδομένων

|  |  |
| --- | --- |
| **Διαβάθμιση Εγγράφου:** | **Εμπιστευτικό** |
| **Έκδοση:** | **2** |
| **Ημερομηνία:** | **Δεκέμβριος 2021** |
| **Συντάκτης Εγγράφου:** |  |
| **Ιδιοκτήτης Εγγράφου:** |  |

**Ιστορικό Ανασκόπησης**

|  |  |  |  |
| --- | --- | --- | --- |
| **Έκδοση** | **Ημερομηνία** | **Συντάκτης Ανασκόπησης**  | **Περίληψη Αλλαγών** |
| 1.0 | Νοέμβριος/ 2020 | Ομάδα υλοποίησης GDPR | Αποδοχή έκδοσης |
| 2.0 | Δεκέμβριος /2021 | Ομάδα υποστήριξης DPO | Αναλυτική περιγραφή στα πεδία και στις ενότητες του ερωτηματολογίου. Προσθήκη νέων πινάκων καθοδήγησης στην ενότητα 3.Προσθήκη βοηθητικού Παραρτήματος σχετικά με την ανάλυση κινδύνων |

**Διανομή**

|  |  |
| --- | --- |
| **Όνομα** | **Τίτλος** |
| Βικελίδου Κορνηλία | Υπεύθυνη Προστασίας Δεδομένων  |
| Όλοι οι ενδιαφερόμενοι  |  |
|  |  |
|  |  |
|  |  |

**Έγκριση**

|  |  |  |  |
| --- | --- | --- | --- |
| **Όνομα** | **Θέση** | **Υπογραφή** | **Ημερομηνία** |
| Καθηγητής Νίκος Παπαϊωάννου | Πρύτανης Πανεπιστημίου |  |  |

Ερωτηματολόγιο συλλογής πληροφοριών για την Εκτίμηση Αντικτύπου σχετικά με

την προστασία των προσωπικών δεδομένων

Αυτή η φόρμα αποτελεί ένα εργαλείο συλλογής πληροφοριών για τις πράξεις επεξεργασίας[[1]](#footnote-1) προσωπικών δεδομένων τις οποίες εκτελούνται στα πλαίσια υλοποίησης ενός έργου ή μιας υπηρεσίας ή μιας διαδικασίας που συμμετέχετε. Από αυτές τις επεξεργασίες μπορεί να προκύψουν υψηλοί κίνδυνοι παραβίασης[[2]](#footnote-2) των προσωπικών δεδομένων και κατά συνέπεια βλάβες στα δικαιώματα και τις ελευθερίες του φυσικού προσώπου στο οποίο ανήκουν τα προσωπικά δεδομένα.

Υποχρέωση του Υπεύθυνου Επεξεργασίας είναι να διασφαλίσει εκ των προτέρων αλλά και να τεκμηριώσει ότι έχει λάβει όλα τα κατάλληλα μέτρα που μειώνουν τον κίνδυνο τη παραβίασης των προσωπικών δεδομένων, ειδικά όταν σχεδιάζει να επεξεργαστεί ειδικής κατηγορίας προσωπικών δεδομένων (ή ευαίσθητα)[[3]](#footnote-3), μεγάλης κλίμακας επεξεργασία ( > 1000 άτομα), εισαγωγή νέας τεχνολογίας στην επεξεργασία, αυτοματοποιημένη λήψη απόφασης ‘η και δημιουργία προφίλ κλπ.

Η εκτίμηση των αντικτύπου (επιπτώσεων) των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα, εφόσον υπάρχει υψηλός κίνδυνος σύμφωνα με τα παραπάνω κριτήρια, είναι υποχρέωση του άρθρου 35 του GDPR.

Για την συμπλήρωση του ερωτηματολογίου θα πρέπει να αφιερώσετε τον ανάλογο χρόνο ώστε να αποκτήσετε μια σαφή εικόνα των επεξεργασιών που εμπλέκεστε με τους όρους του GDPR. Αν χρειαστεί μπορείτε να επιστρέφετε σε προηγούμενα σημεία του ερωτηματολογίου, εφόσον αποκτάται καλύτερη γνώση των επεξεργασιών.

Οι απαντήσεις σας θα αξιοποιηθούν στην εκπόνηση της μελέτης εκτίμησης αντικτύπου και για τον λόγο αυτό παρακαλούμε να είστε όσο πιο λεπτομερείς στις περιγραφές καθώς να και να συμπεριλάβετε κάθε διακριτή επεξεργασίας σχετικά με το έργο/την διαδικασία που εξετάζεται.

Παρακαλούμε το ερωτηματολόγιο μετά την ολοκλήρωσή του θα πρέπει να σταλεί στο data.protection@auth.gr

Γενικές πληροφορίες για τις εξεταζόμενες επεξεργασίες

|  |  |
| --- | --- |
| **Όνομα του έργου/ διαδικασίας/ υπηρεσίας που αφορούν οι επεξεργασίες** |  |
| **Σκοπός του έργου/ διαδικασίας/ υπηρεσίας που αφορά η επεξεργασία:** |  |
| **Υπεύθυνος έργου/ διαδικασίας/ υπηρεσίας (Owner):** |  |
| **Αναφέρετε τα ονόματα των υπο-έργων/ υπο-διαδικασιών/ υπο-υπηρεσιών που λαμβάνουν χώρα οι επεξεργασίες ( εφόσον είναι εφικτό)** |  |

# ΑΝΑΛΥΣΗ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

## Περιγραφή των επεξεργασιών

|  |
| --- |
| *[να απαριθμήσετε και περιγράψετε με σαφήνεια ώστε να γίνουν κατανοητές οι επεξεργασίες που λαμβάνετε μέρος, με όρους:** *Τίτλος επεξεργασίας που μπορεί να προσδώσετε πχ συλλογή δεδομένων μέσω κινητού, ηχογράφηση, ανωνυμοποίηση, κοινοποίηση κλπ*
* *Σειράς εκτέλεσης των επεξεργασιών*
* *γεωγραφικής τοποθεσίας π.χ. χώρες, γραφεία, κέντρα δεδομένων που γίνεται η επεξεργασία*
* *οργανωτικές μονάδες π.χ. συγκεκριμένα τμήματα που μετέχουν*
* *άλλες διαδικασία (-ες) του οργανισμού σας που εμπλέκονται άμεσα με αυτή ( πχ διαδικασίες από όπου αναμένονται ή και που πρόκειται να διαβιβαστούν δεδομένα)*
* *κατηγορίες φυσικών προσώπων που αφορά πχ μαθητές, φοιτητές, εργαζόμενους, ασθενεί, πολίτες, δημότες, συνδρομητές κλπ*
* *Συστήματα που θα χρησιμοποιηθούν για την συγκεκριμένη επεξεργασία (υποδομές και εργαλεία τεχνολογιών πληροφορικής και δικτύων , άλλος εξοπλισμός που θα χρησιμοποιηθεί πχ ντουλάπες)*

*]* |

## Προσωπικά δεδομένα που περιλαμβάνονται

|  |
| --- |
| *[Περιγράψτε τις κατηγορίες των προσωπικών δεδομένων που θα χρησιμοποιήσετε ανά επεξεργασία χρησιμοποιώντας του τίτλους της 1.1 ( π.χ όνομα, διεύθυνση, τηλέφωνα, ημερομηνία πρόσληψης, κλπ). Να αναφέρετε ξεχωριστά σε άλλη παράγραφο τα ευαίσθητα προσωπικά δεδομένα (Δες υποσημείωση 3 παραπάνω) αν υπάρχουν ]*  |

## Από που προέρχονται τα δεδομένα;

|  |
| --- |
| *[Αναφέρατε εάν τα δεδομένα συλλέγονται απευθείας από το υποκείμενο των δεδομένων ή προέρχονται από δεδομένα που διατηρεί ο οργανισμός ( βάσεις δεδομένων, έντυπα ή ψηφιακά αρχεία ) ή από τρίτους ( εκτός οργανισμού).]* |

## Τι επεξεργασία θα γίνει στα δεδομένα;

|  |
| --- |
| *[Αναγνωρίστε και περιγράψτε με ακρίβεια τον σκοπό ή τους σκοπούς που θα επεξεργαστείτε τα προσωπικά δεδομένα και συνδέστε τους σκοπού με τις κατηγορίες των δεδομένων. Προσπαθήστε να απαντήστε στα ερωτήματα:** *Τα δεδομένα που χρησιμοποιούνται είναι τα κατάλληλα, συναφή και περιορίζονται στα αναγκαία* *για να εξυπηρετήσουν τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία; ( αρχή της ελαχιστοποίησης)*
* *Πως εξασφαλίζεται ότι τα δεδομένα που χρησιμοποιούνται είναι ακριβή;*
* *Η επεξεργασία θα γίνει εσωτερικά από το προσωπικό του οργανισμού ή θα την αναλάβουν ένα ή περισσότερα τρίτα μέρη;*

*]* |

## Ποιος είναι ο χρόνος διατήρησης των δεδομένων;

|  |
| --- |
| *[ τα δεδομένα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας τους.* *Προσπαθήστε να ορίσετε το χρόνο διατήρησης για κάθε σκοπό και να αιτιολογήσετε την απόφασή σας. Για παράδειγμα υπάρχει συγκεκριμένο νομικό πλαίσιο που καθορίζει τον χρόνο διατήρησης ή υπάρχει εσωτερικός κανονισμός ή απόφαση της διοίκησης ή καθορίζεται από τις ανάγκες του έργου/ της διαδικασίας/ της υπηρεσίας;]* |

## Πως γίνεται η διαγραφή / καταστροφή των δεδομένων;

|  |
| --- |
| *[Σε περίπτωση που ο οργανισμός δε χρειάζεται πλέον τα δεδομένα ή έχει περάσει ο χρόνος διατήρησης, με ποιον τρόπο γίνεται η διαγραφή; Υπάρχει καταγεγραμμένη η διαδικασία που ακολουθήθηκε κατά τη διαγραφή;**Τα εν λόγω δεδομένα υπάρχουν και σε άλλη τοποθεσία; Εάν ναι, με ποιον τρόπο καλύπτονται τα παραπάνω]* |

## Πως θα γίνει η αποθήκευση των δεδομένων;

|  |
| --- |
| *[Που θα αποθηκευτούν (πχ προσωπικός υπολογιστής, κεντρικός server, βάση δεδομένων , ντουλάπα/συρτάρι ) και τι μέτρα λαμβάνονται για την ασφάλεια της επεξεργασίας, σύμφωνα με το άρθρο 32 του ΓΚΠΔ;* *π.χ. κρυπτογράφηση ή ανωνυμοποίηση των αποθηκευμένων δεδομένων, ή ντουλάπα που κλειδώνει και εν γένει τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση. Ποια επιπλέον μέτρα λαμβάνονται στα πλαίσια της προστασίας δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, σύμφωνα με το άρθρο 25 του ΓΚΠΔ και τις οδηγίες 4/2019 της EDPB:*[*https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\_guidelines\_201904\_dataprotection\_by\_design\_and\_by\_default\_v2.0\_en.pdf*](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf)*]* |

## Υπάρχει πιθανότητα άλλων μελλοντικών χρήσεων των δεδομένων;

|  |
| --- |
| *[Είναι πιθανό τα δεδομένα να χρησιμοποιηθούν (ή να χρησιμοποιούνται) για σκοπούς άλλους από εκείνους για τους οποίους συλλέγονται (ή συλλέχθηκαν )και αν ναι, ποιούς σκοπούς;]* |

## Που θα μεταφερθούν τα δεδομένα και υπό ποιες συνθήκες;

|  |
| --- |
| *[Τα δεδομένα που επεξεργάζεστε θα σταλούν εκτός οργανισμού σε άλλες περιοχές ή τρίτα μέρη σε άλλες χώρες; Αν ναι, Ποιες είναι οι χώρες; γιατί θα γίνει η μεταφορά, πως θα γίνει;]* |

## Ποιος θα έχει πρόσβαση στα δεδομένα και με ποιο τρόπο;

|  |
| --- |
| *[Ποιος θα έχει πρόσβαση στα δεδομένα εντός και εκτός του οργανισμού σας και με τι μέτρα ελέγχεται η πρόσβαση; ]* |

# ΑΠΕΙΛΕΣ και ΚΙΝΔΥΝΟΙ

Ως απειλή μπορούμε να θεωρήσουμε αθροιστικά την ικανότητα, την πρόθεση και την ευκαιρία κάποιου ή μιας ομάδας ή ενός συστήματος ( τεχνικού ή φυσικού) να θέσει σε κίνδυνο τα προσωπικά δεδομένα. Η ευκαιρία συνήθως παρέχεται όταν υπάρχει αδυναμία ( ευπάθεια) στα μέτρα προστασία των δεδομένων

Για παράδειγμα, η φωτιά ( απειλή με ικανότητα αλλά όχι πρόθεση) από βραχυκύκλωμα σε κατεστραμμένα καλώδια ( ευκαιρία) στο γραφείο μπορεί να κάψει τον υπολογιστή και την ντουλάπα ή κάποιος τρίτος ( χάκερ με ικανότητα και πρόθεση) έκλεψε την βάση δεδομένων επειδή ο κωδικός πρόσβασης ήταν προβλέψιμος ( ευκαιρία)

Ο κίνδυνος για τα προσωπικά δεδομένα είναι το γεγονός ή η κατάσταση που, σε περίπτωση προκύψει, έχει ως αποτέλεσμα την παραβίαση τουλάχιστον μιας εκ των τριών: εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας ( δείτε παρακάτω τους ορισμούς)

Έτσι μια φωτιά έχει σαν αποτέλεσμα την παραβίαση της εμπιστευτικότητας, ενώ η πράξη του χάκερ παραβιάζει την εμπιστευτικότητα και ενδεχομένως και την ακεραιότητα

*[Στη συνέχεια προσπαθήστε να καταγράψετε τις απειλές και τους αντίστοιχους κινδύνους που αντιλαμβάνεστε ότι υπάρχουν και αντιμετωπίζετε κατά την εκτέλεση των επεξεργασιών. Αυτές οι απειλές και αυτοί οι κίνδυνοι μπορεί να υπάρχουν ήδη και για άλλες επεξεργασίες που εκτελείτε]*

|  |  |  |
| --- | --- | --- |
| Α/Α | **Απειλή** | **Κίνδυνος** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ

Συμπληρώστε τους παρακάτω πίνακες επιπτώσεων, με βάση τις ακόλουθες κατηγορίες παραβιάσεων για τους κινδύνους όπως τους έχετε περιγράψει παραπάνω και για ποιες επεξεργασίες προσωπικών δεδομένων ισχύουν αυτοί. Ακόμη θα μπορείτε να εκτιμήσετε τις επιπτώσεις και για άλλες εμπιστευτικές πληροφορίες οι οποίες μετέχουν στην επεξεργασία χωρίς όμως περιέχουν προσωπικά δεδομένα, αλλά πρέπει να προστατευτούν εξίσου.

**Για την ανάλυση και αξιολόγηση των κινδύνων θα πρέπει να συμβουλευτείτε το ΠΑΡΑΡΤΗΜΑ:**

|  |
| --- |
| ***ΚΑΤΗΓΟΡΙΕΣ ΚΙΝΔΥΝΩΝ ΩΣ ΠΡΟΣ ΤΙΣ ΕΠΙΠΤΩΣΕΙΣ*** |
| **Υψηλός** | Σε περίπτωση που ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. |
| **Μεσαίος** | Σε περίπτωση που ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει μεσαίου επιπέδου κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. |
| **Χαμηλός** | Σε περίπτωση ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει χαμηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. |

## Εμπιστευτικότητα Δεδομένων

Η προστασία από την αποκάλυψη προσωπικών δεδομένων εσκεμμένα ή μη σε άτομα που δεν είναι ανάγκη να γνωρίζουν. Εκτιμήστε τον κίνδυνο ( Υψηλός, Μεσαίος, Χαμηλός ) από την παραβίαση της εμπιστευτικότητας, που μπορεί να υπάρξει για τον οργανισμό για κάθε επεξεργασία προσωπικών δεδομένων που εκτελείτε η μετέχετε, θεωρώντας ότι η αποκάλυψη γίνεται σε άτομα που δεν είναι ανάγκη να γνωρίσουν εκτός οργανισμού ή ακόμη και εντός οργανισμού. Δηλώστε την εκτίμηση σας με σαφή ένδειξη στο αντίστοιχο κελί ( πχ ΝΑΙ, ✓, Χ κλπ.),

|  |
| --- |
| ***Κίνδυνος παραβίασης Εμπιστευτικότητας Δεδομένων (εσκεμμένη ή μη)*** |
| **Επεξεργασία** | Χαμηλός | Μεσαίος | Υψηλός | Σχόλια/Παρατηρήσεις |
| 1…. |  |  |  |  |
| 2…. |  |  |  |  |

Αν ο κίνδυνος εκτιμάται ότι είναι **Χαμηλός**, να αναφέρετε τα τεχνικά και οργανωτικά μέτρα που οφείλεται αυτή η εκτίμηση:

|  |  |
| --- | --- |
| **Α/Α** | **Μέτρα που καθιστούν τον κίνδυνο Χαμηλό ( αποδεκτό)** |
| 1. |  |
| 2. |  |

Αν η εκτίμηση του κινδύνου για αυτή την παραβίαση είναι **Υψηλός ή Μεσαίος,** περιγράψτε τις επιπτώσεις που μπορεί να έχει αυτός.

Επίσης αναφέρετε στη συνέχεια τις προτάσεις σας για την μείωση ή την εξάλειψή του κινδύνου για κάθε επεξεργασία με υψηλό ή μεσαίο κίνδυνο, εφόσον μπορείτε .

|  |  |
| --- | --- |
| **Επίπτωση στα:** | **Περιγραφή** |
| Υποκείμενα των δεδομένων  |  |
| Νομική και συμβατική συμμόρφωση: |  |
| Επιχειρησιακή Λειτουργία: |  |
| Εμπιστοσύνη υποκειμένων των δεδομένων / προμηθευτών/ Προσωπικού, Φήμη του οργανισμού: |  |

|  |  |
| --- | --- |
| **Επεξεργασία**  | **Προστάσεις μέτρων για την μείωση ή την εξάλειψη του κινδύνου** |
| 1… |  |
| 2… |  |

##  Ακεραιότητα Δεδομένων

Η προστασία των δεδομένων από εσφαλμένη τροποποίηση των δεδομένων η οποία μπορεί να γίνει εσκεμμένα ή ακούσια από εξουσιοδοτημένα ή μη εξουσιοδοτημένα πρόσωπα. Εκτιμήστε τον κίνδυνο ( Υψηλός, Μεσαίος, Χαμηλός ) από την παραβίαση της ακεραιότητας που μπορεί να υπάρξει για τον οργανισμό για κάθε επεξεργασία προσωπικών δεδομένων που εκτελείτε η μετέχετε και δηλώστε το με σαφή ένδειξη στο αντίστοιχο κελί ( πχ ΝΑΙ, ✓, Χ κλπ.)

|  |
| --- |
| ***Κίνδυνος παραβίαση Ακεραιότητας Δεδομένων (εσκεμμένη ή μη)*** |
| **Επεξεργασία** | Χαμηλός | Μεσαίος | Υψηλός | Σχόλια/Παρατηρήσεις |
| 1….. |  |  |  |  |
| 2…. |  |  |  |  |

Αν ο κίνδυνος εκτιμάται ότι είναι **Χαμηλός**, να αναφέρετε τα τεχνικά και οργανωτικά μέτρα που οφείλεται αυτή η εκτίμηση:

|  |  |
| --- | --- |
| **Α/Α** | **Μέτρα που καθιστούν τον κίνδυνο Χαμηλό ( αποδεκτό)** |
| 1. |  |
| 2. |  |

Αν η εκτίμηση του κινδύνου για αυτή την παραβίαση είναι **Υψηλός ή Μεσαίος,** περιγράψτε τις επιπτώσεις που μπορεί να έχει αυτός.

Επίσης αναφέρετε στη συνέχεια τις προτάσεις σας για την μείωση ή την εξάλειψή του κινδύνου για κάθε επεξεργασία με υψηλό ή μεσαίο κίνδυνο, εφόσον μπορείτε .

|  |  |
| --- | --- |
| **Επίπτωση στα:** | **Περιγραφή** |
| Υποκείμενα των δεδομένων  |  |
| Νομική και συμβατική συμμόρφωση: |  |
| Επιχειρησιακή Λειτουργία: |  |
| Εμπιστοσύνη υποκειμένων των δεδομένων / προμηθευτών/ Προσωπικού, Φήμη του οργανισμού: |  |

|  |  |
| --- | --- |
| **Επεξεργασία**  | **Προστάσεις μέτρων για την μείωση ή την εξάλειψη του κινδύνου** |
| 1… |  |
| 2… |  |

## Διαθεσιμότητα Δεδομένων

Ο μέγιστος χρόνος που τα δεδομένα μπορούν να μην είναι διαθέσιμα για χρήση χωρίς να δημιουργηθούν νομικά, συμβατικά, επιχειρησιακά ή άλλα προβλήματα στον οργανισμό. Εκτιμήστε τον κίνδυνο ( Υψηλός, Μεσαίος, Χαμηλός ) από την παραβίαση της διαθεσιμότητας που μπορεί να υπάρξει για τον οργανισμό για κάθε επεξεργασία προσωπικών δεδομένων που εκτελείτε η μετέχετε και δηλώστε τις ενδείξεις **Υψηλός, Μεσαίος, Χαμηλός** στο αντίστοιχο κελί (.) που επεξεργάζεστε στα παρακάτω χρονικά όρια.

|  |
| --- |
| ***Κίνδυνος παραβίαση Διαθεσιμότητας Δεδομένων (πχ μη δυνατότητα ανάκτησης από αντίγραφα ασφαλείας, μη εύρεση δεδομένων έγκαιρα)*** |
| **Επεξεργασία** | Μέχρι 1 ώρα | Από 1 ώρα μέχρι 1 μέρα | Από 1 μέρα μέχρι 1 εβδομάδα | Από 1 εβδομάδα μέχρι 1 μήνα | Από 1 μήνα και πέρα |
| 1… |  |  |  |  |  |
| 2… |  |  |  |  |  |

Αν ο κίνδυνος εκτιμάται ότι είναι **Χαμηλός**, να αναφέρετε τα τεχνικά και οργανωτικά μέτρα που οφείλεται αυτή η εκτίμηση:

|  |  |
| --- | --- |
| **Α/Α** | **Μέτρα που καθιστούν τον κίνδυνο Χαμηλό ( αποδεκτό)** |
| 1. |  |
| 2. |  |

Αν η εκτίμηση του κινδύνου για αυτή την παραβίαση είναι **Υψηλός ή Μεσαίος,** περιγράψτε τις επιπτώσεις που μπορεί να έχει αυτός.

Επίσης αναφέρετε στη συνέχεια τις προτάσεις σας για την μείωση ή την εξάλειψή του κινδύνου για κάθε επεξεργασία με υψηλό ή μεσαίο κίνδυνο, εφόσον μπορείτε .

|  |  |
| --- | --- |
| **Επίπτωση στα:** | **Περιγραφή** |
| Υποκείμενα των δεδομένων  |  |
| Νομική και συμβατική συμμόρφωση: |  |
| Επιχειρησιακή Λειτουργία: |  |
| Εμπιστοσύνη υποκειμένων των δεδομένων / προμηθευτών/ Προσωπικού, Φήμη του οργανισμού: |  |

|  |  |
| --- | --- |
| **Επεξεργασία**  | **Προστάσεις μέτρων για την μείωση ή την εξάλειψη του κινδύνου** |
| 1… |  |
| 2… |  |

# Γενικά σχόλια / παρατηρήσεις:

**Στοιχεία του υπεύθυνου συμπλήρωσης του ερωτηματολογίου**

|  |  |
| --- | --- |
| **Υπογραφή:** |  |
| **Όνομα:** |  |
| **Ημερομηνία:** |  |

**Στοιχεία του υπεύθυνου αξιολόγησης**

|  |  |
| --- | --- |
| **Υπογραφή:** |  |
| **Όνομα:** |  |
| **Ημερομηνία:** |  |

**ΠΑΡΑΡΤΗΜΑ**

# Ανάλυση και αξιολόγηση 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.

* 1. **Αξιολόγηση της πιθανότητας**

Πρέπει να γίνει εκτίμηση της πιθανότητας εμφάνισης κινδύνου. Αυτό θα πρέπει να λαμβάνει υπόψη το αν έχει συμβεί ξανά είτε στη Τράπεζα είτε σε παρόμοιους οργανισμούς 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** | **Πιθανότητα παραβίασης** | **Περιγραφή** | **Σύνοψη** |
| 1 | Μικρή | 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 | Μεσαία | Πιθανό | Σε ισορροπία, ο κίνδυνος είναι πιθανότερο να συμβεί. |
| 4 | Μεγάλη | 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.

* 1. **Εκτίμηση του Αντίκτυπου**

Θα πρέπει να δοθεί μια εκτίμηση του αντικτύπου που θα μπορούσε να έχει ο κίνδυνος στον οργανισμό. 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:

* Υποκείμενο των δεδομένων
* Υγεία και ασφάλεια του υποκειμένου
* Οικονομικά του οργανισμού
* Φήμη οργανισμού
* Επιπτώσεις μέσα στον οργανισμό
* 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** | **Βαθμός Επιπτώσεων** | **Περιγραφή** | **Επίπτωση στο υποκείμενο των δεδομένων** | **Υγεία και Ασφάλεια** | **Οικονομική Επίπτωση** | **Επίπτωση στην Φήμη** | **Νομικές Επιπτώσεις** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Μικρός | 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 | Σημαντικός | 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 | Σοβαρός | 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 οργανισμού | 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 οργανισμού | Πολύ υψηλή | Σοβαρά πρόστιμα και πιθανή φυλάκιση προσωπικού |

*Πίνακας 2 - Καθοδήγηση για τον αντίκτυπο του κινδύνου*

* 1. **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 1 - Διάγραμμα πίνακα κινδύνου*

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

* 1. **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 1* 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 τον Οργανισμό.

1. «**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 [↑](#footnote-ref-1)
2. «**παραβίαση δεδομένων προσωπικού χαρακτήρα**» :η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία [↑](#footnote-ref-2)
3. δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και τα γενετικά δεδομένα, βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό φυσικού προσώπου [↑](#footnote-ref-3)