

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

|  |  |
| --- | --- |
| **Διαβάθμιση Εγγράφου:** | Εμπιστευτικό |
| **Έκδοση:** | **2** |
| **Ημερομηνία:** |  |
| **Συντάκτης Εγγράφου:** |  |
| **Ιδιοκτήτης Εγγράφου:** | **Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης**  |

**Ιστορικό Αναθεώρησης**

|  |  |  |  |
| --- | --- | --- | --- |
| **Έκδοση** | **Ημερομηνία** | **Συντάκτης Αναθεώρησης** | **Σύνοψη Αλλαγών** |
| 1 | Νοέμβριος 2020 | Ομάδα Υλοποίησης Συμμόρφωσης με το ΓΚΠΔ  | Πρώτη έκδοση |
| 2 | Ιανουάριος 2022 | Ομάδα Υποστήριξης ΥΠΔ  | Σημαντικές αλλαγές στους τίτλους των στηλών στους διάφορους πίνακες, αναπροσαρμογή των ερωτημάτων, προσθήκη υπομνημάτων και σημαντική βελτίωση των σχολίων. Προσθήκη παραδειγμάτων στους πινακες.Προσθήκη νέων πεδίων στον πίνακα 1 και 2 του παραρτήματος |
|  |  |  |  |

**Διανομή**

|  |  |
| --- | --- |
| **Όνομα** | **Τίτλος** |
|  | Πρύτανης Πανεπιστημίου |
|  | Υπεύθυνη Προστασίας Δεδομένων  |
| Όλοι οι ενδιαφερόμενοι |  |
|  |  |
|  |  |

**Έγκριση**

|  |  |  |  |
| --- | --- | --- | --- |
| **Όνομα** | **Θέση** | **Υπογραφή** | **Ημερομηνία** |
|  | Πρύτανης Πανεπιστημίου |  |  |

**Εισαγωγή**

Στο πλαίσιο της δέσμευσης του οργανισμού για την προστασία των προσωπικών Δεδομένων έναντι παραβίασης[[1]](#footnote-1), διασφαλίζει ότι για τις σημαντικές λειτουργικές δραστηριότητες/διαδικασίες και τα έργα που αφορούν τη χρήση προσωπικών δεδομένων υπόκεινται σε αξιολόγηση αντίκτυπου προστασίας δεδομένων ( Data Protection Impact Assessment – **DPIA**). Σκοπός της αξιολόγησης είναι να διασφαλιστεί ότι η επεξεργασία[[2]](#footnote-2) 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 των προσωπικών δεδομένων κατά τη διάρκεια του κύκλου ζωής της επεξεργασίας τους. Περισσότερες λεπτομέρειες για την διεξαγωγή DPIA προτρέπουμε να διαβάσετε στο Παράρτημα.

|  |
| --- |
| **Γενικές Πληροφορίες για το έργο/την διαδικασία που γίνεται η DPIA** |
| Τίτλος: |  |
| Τα Μέρη που συμμετέχουν στη DPIA: |  |
| Το παρόν συμπληρώθηκε από: |  |
| Σχετικά με το έργο/ τη διαδικασία (*περιεκτική περιγραφή για την κατανόηση του έργου/διαδικασίας και των εκτελούμενων επεξεργασιών προσωπικών δεδομένων*): |  |
| Ημερομηνία έναρξης :  |  |
| Ημερομηνία ολοκλήρωσης:  |  |
| Διάρκεια: |  |
| Ιστοσελίδα:  |   |

**Βήμα 1: Επισκόπηση του έργου/ της διαδικασίας**

|  |
| --- |
| **Επισκόπηση της/των επεξεργασίας /ών των προσωπικών δεδομένων στο έργο/διαδικασία** |
| Σκοπός του έργου/της διαδικασίας  |  |
| Τύπος των επεξεργασιών (*τι αφορά γενικά πχ έρευνα, υπηρεσία, ενημέρωση, ασφάλεια κλπ*) |  |
| Φύση των επεξεργασιών (*πολύ σύντομη αλλά περιεκτική περιγραφή του τρόπου των επεξεργασιών με έμφαση στα μέσα πχ έντυπη καταγραφή, βιντεοσκόπηση, δημιουργία βάσης δεδομένων, ηλεκτρονική διαβίβαση κλπ*) |  |
| Το εδαφικό πεδίο εφαρμογής των επεξεργασιών[[3]](#footnote-3) *(αν και ποιες επεξεργασίες συμβαίνουν εντός ή εκτός ΕΕ)*   |  |
| Υπεύθυνοι Επεξεργασίας / Από κοινού Υπεύθυνοι της Επεξεργασίας[[4]](#footnote-4)  |  |
| Εκτελών την Επεξεργασία[[5]](#footnote-5) |  |
| Αναφορά στη γραπτή συμφωνία των από κοινού Υπεύθυνων Επεξεργασίας, εφόσον υφίσταται η σχέση |  |
| Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ) στο έργο/ στη διαδικασία |  |

|  |
| --- |
| **Κώδικες δεοντολογίας που εφαρμόζονται στην επεξεργασία[[6]](#footnote-6)** |
|  |
|  |

**Η ανάγκη για την διεξαγωγή εκτίμησης αντικτύπου (DPIA)**

*[στο λογικό πλαίσιο* *θα πρέπει να περιγραφεί με σαφήνεια η κάθε αιτιολογία που μας οδηγεί στην DPIA, όπως ενδεικτικά τα σχετικά παραδείγματα ενώ στο νομικό πλαίσιο να προστεθούν άλλοι νομικοί λόγοι που επιβάλουν την ανάγκη για την εκτίμηση του αντικτύπου, πχ η ύπαρξη σχετικής πολιτικής του υπεύθυνου επεξεργασίας, ρητή νομική υποχρέωση, κατάλογος της Αρχής Προστασίας με είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση κλπ ]*

|  |  |
| --- | --- |
| **Λογικό πλαίσιο**  |  **Νομικό πλαίσιο**  |
| *[ ενδεικτικά παραδείγματα:** *Επειδή υπάρχει πραγματικά υψηλός κίνδυνος για τις συγκεκριμένες κατηγορίες υποκειμένων των δεδομένων θα πρέπει να ελεγχθούν και να αξιολογηθούν τα μέτρα προστασίας των προσωπικών δεδομένων και να ληφθούν αν χρειαστεί να αναγκαία μέτρα ώστε ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων να είναι χαμηλός ή αποδεκτός*
* *Το σύνολο των δεδομένων και των υποκειμένων των δεδομένων εμπίπτουν στα ποιοτικά και ποσοτικά κριτήρια του υπεύθυνου επεξεργασίας για την διενέργεια DPIA - παρατίθενται δίπλα*
* *Υπάρχει έννομη υποχρέωση για την διενέργεια DPIA - παρατίθεται δίπλα*
* *Εκτιμάται ή δεν υπάρχει σαφής εικόνα ότι τα μέτρα δεν είναι επαρκή και υπάρχει η ανάγκη να τεκμηριωθούν ή ακόμη ότι παρά τη λήψη μέτρων ο κίνδυνος φαίνεται να είναι υψηλός*
* *…. ]*
 |

|  |  |
| --- | --- |
| Άρθρο 35, παράγραφος 1 του ΓΚΠΔ: Όταν 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, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. |  |

 |

**Βήμα 2: Περιγραφή των δεδομένων**

*[ζητείται η αναλυτική περιγραφή των δεδομένων ώστε οι πληροφορίες να ληφθούν υπόψη στα επόμενα βήματα]*

|  |  |
| --- | --- |
| **Στοιχεία περιγραφής δεδομένων** | **Περιγραφή** |
| Προσωπικά δεδομένα που χρησιμοποιούνται ή πρόκειται να χρησιμοποιηθούν. Να διαχωριστούν τα ευαίσθητα δεδομένα[[7]](#footnote-7) : |  |
| Πηγή των δεδομένων: |  |
| Παραπομπή *(αναφορά σε άλλες πηγές που θα μπορούσαν να παρέχουν περισσότερες πληροφορίες για τα προσωπικά δεδομένα)*: |  |
| Εγκεκριμένη δεοντολογία *(συνδέστε τους αναφερόμενους παραπάνω κώδικες δεοντολογίας που λαμβάνεται υπόψη, πχ ιατρικός κώδικας δεοντολογίας, με το μέρος ή το σύνολο των δεδομένων)*: |  |
| Πώς θα συλλέξετε τα δεδομένα; |  |
| Χρησιμοποιείτε όλα τα δεδομένα που συλλέγετε; Αν όχι, γιατί το κάνετε και επιπλέον τι κάνετε με αυτά που δεν τα χρησιμοποιείτε; |  |
| Ποσό συχνά συλλέγετε δεδομένα; |  |
| Πόσα άτομα επηρεάζονται; |  |
| Ποια γεωγραφική περιοχή καλύπτει η συλλογή ή η επεξεργασία των προσωπικών δεδομένων; |  |

**Μέτρα που λαμβάνετε για την Προστασία Δεδομένων**

*[σημειώστε τον τίτλο του μέτρου προστασίας που λαμβάνετε ή εναλλακτικά ένα πολύ σύντομο προσδιορισμό του και περιγράψτε αναλυτικά πως το εφαρμόζετε. Για την ψευδωνυμοποίηση και την κρυπτογράφηση απαντήστε με ένα ΟΧΙ ότι δεν εφαρμόζετε. προσθέστε και άλλα μέτρα για την προστασία των προσωπικών δεδομένων. Πχ δικαιώματα πρόσβασης, σύνθετους κωδικούς, κλειδωμένες ντουλάπες, ανωνυμοποίηση, πιστοποίηση ISO ή άλλη κλπ]*

|  |  |
| --- | --- |
| **Τίτλος του Μέτρου** | **Αναλυτική περιγραφή της εφαρμογή του μέτρου** |
| Ψευδωνυμοποίηση δεδομένων |  |
| Κρυπτογράφηση δεδομένων |  |
| ….. |  |

**Βήμα 3: Περιγραφή των επεξεργασιών**

*[Σχεδιάστε και οργανώστε τις διακριτές διαδικασίες ή και τις πράξεις που υλοποιούν επεξεργασίες προσωπικών δεδομένων και δώστε ένα τίτλο ή εναλλακτικά ένα πολύ σύντομο προσδιορισμό. Επειδή κάθε είδος επεξεργασίας μπορεί να εκτελείτε με ενιαίο ή διαφορετικό τρόπο για κάθε διαδικασία ή πράξη, περιγράψτε αναλυτικά την εξειδίκευση του κάθε είδους επεξεργασίας που αντιστοιχεί στη συγκεκριμένη ή στις συγκεκριμένες διαδικασίες/πράξεις. Μπορεί να σας φανεί χρήσιμο να ανατρέξετε σε ένα διάγραμμα ροής ή σε άλλο τρόπο περιγραφής των ροών δεδομένων. Να αναφέρετε στη περιγραφή ποια είδη επεξεργασίας χαρακτηρίζονται ως πιθανώς υψηλοί κίνδυνοι.*

*Υπόδειξη: χρησιμοποιήστε τεχνικές λογικού ή τεχνικού (split) διαχωρισμού κάθε γραμμής για να αντιστοιχίσετε καλύτερα την διαδικασία/πράξη με την περιγραφή και να μην επαναλαμβάνετε τις περιγραφές]*

|  |  |  |
| --- | --- | --- |
| **Είδος επεξεργασίας**  | **Τίτλος διαδικασίας/πράξης** |  **Περιγραφή της επεξεργασίας ανά διαδικασία/πράξη** |
| Πώς θα χρησιμοποιήσετε τα δεδομένα; |  |  |
| Πώς θα αποθηκεύσετε τα δεδομένα; |  |  |
| Για πόσο καιρό θα διατηρήσετε τα δεδομένα; |  |  |
| Πώς θα διαγραφούν τα δεδομένα; |  |  |
| Πώς θα διακινείτε τα δεδομένα; |  |  |

**Βήμα 4. Περιγραφή των σκοπών**

*[προσδιοριστές ακριβώς τους διακριτούς σκοπούς για τους οποίους επεξεργάζεστε τα προσωπικά δεδομένα και περιγράψτε τους αναλυτικά. Απαντήστε με ακρίβεια και στα επόμενα ερωτήματα ώστε να αποσαφηνίζονται περισσότερο οι σκοποί]*

|  |  |
| --- | --- |
| **Στοιχεία ανάλυσης των σκοπών** | **Περιγραφή**  |
| Για ποιους σκοπούς/ ειδικούς λόγους θα επεξεργαστείτε τα δεδομένα; |  |
| Τι θέλετε να επιτύχετε; |  |
| Ποιο είναι το επιδιωκόμενο αποτέλεσμα για τα άτομα; |  |
| Ποια είναι τα οφέλη της επεξεργασίας για εσάς αλλά και γενικότερα; |  |

**Βήμα 5. Αξιολόγηση της αντικειμενικότητας του σκοπού**

*[Για κάθε παραπάνω σκοπό και λαμβάνοντας υπόψη τις επιδιώξεις σας, να αξιολογήσετε την αντικειμενικότητα του σκοπού που περιλαμβάνει μεταξύ άλλων* *την αναγνώριση των θεμιτών προσδοκιών των υποκειμένων των δεδομένων όσον αφορά πιθανές αρνητικές συνέπειες που ενδέχεται να επιφέρει η επεξεργασία σε αυτούς και την εξέταση της σχέσης και των πιθανών επιπτώσεων της ανισότητας μεταξύ αυτών και του υπεύθυνου επεξεργασίας]*

|  |  |  |
| --- | --- | --- |
| **Σκοπός**  | **Αιτιολόγηση της αντικειμενικότητας του σκοπού**  | **Είναι αποδεκτός ο σκοπός / μπορεί να βελτιωθεί** |
|  |  |  |
|  |  |  |

**Επεξήγηση και αιτιολόγηση της νομιμότητας**

*[Στα κριτήρια νομιμότητας αναφέρατε τις προϋποθέσεις του άρθρου 6(1) του GDPR που μπορεί να δικαιολογήσει την επεξεργασία για κάθε παραπάνω σκοπό. Αν στα δεδομένα περιλαμβάνονται και ειδικής κατηγορίας ( ή ευαίσθητα) δεδομένα, τότε θα πρέπει να αναφέρετε* ***και*** *τις προϋποθέσεις του άρθρου 9(2) του GDPR που συντρέχουν. Η αξιολόγηση των κριτηρίων νομιμότητας έγκειται στο κατά πόσο εφαρμόζονται ή όχι οι προϋποθέσεις που ορίζει ο GDPR ή και ο ν.4624/2019. Σε κάθε περίπτωση στην αιτιολόγηση θα πρέπει να τεκμηριώνεται η απάντηση ΝΑΙ/ΟΧΙ στην εφαρμογή και με ποιο τρόπο τελικά οι προϋποθέσεις θα εφαρμόζονται. Η αξιολόγηση θα πρέπει να αποτυπώνει την τρέχουσα κατάσταση κατά την εκπόνηση της DPIA και όχι μια μελλοντική κατάσταση[[8]](#footnote-8)].*

|  |  |  |
| --- | --- | --- |
| **Κριτήρια νομιμότητας** | **Εφαρμόζεται** | **Αιτιολόγηση** |
| *[Παράδειγμα 1: περίπτωση 6(1)(α) και ειδική περίπτωση 9(2)(α): Η επεξεργασία των προσωπικών δεδομένων βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων που θα δώσει ή έχει δώσει για συγκεκριμένους σκοπούς]*  |  |  |
| *[Παράδειγμα 2: περίπτωση 6(1)(γ): Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με νομική υποχρέωση την οποία υπόκειται ο υπεύθυνος επεξεργασίας]*  |  |  |
| *[Παράδειγμα 3: περίπτωση 6(1)(στ): Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας και τα οποία υπερισχύουν του συμφέροντος ή των θεμελιωδών δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα]*  |  |  |
| *[Παράδειγμα 4: πρόσθετη περίπτωση 9(2)(η) : Η επεξεργασία είναι απαραίτητη για τους σκοπούς της προληπτικής ή επαγγελματικής ιατρικής, για την ιατρική διάγνωση και υπό τους όρους και τις εγγυήσεις που αναφέρονται στην παράγραφο 3 του άρθρου 9 του GDPR]* |  |  |
| *[Παράδειγμα 5: πρόσθετη περίπτωση 9(2)(θ) : Η επεξεργασία είναι απαραίτητη για λόγους δημόσιου ενδιαφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία από σοβαρές διασυνοριακές απειλές κατά της υγείας, με βάση του δικαίου του κράτους μέλους το οποίο προβλέπει κατάλληλα και ειδικά μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, και ιδίως του επαγγελματικού απορρήτου ]·* |  |  |
| *[Παράδειγμα 6: περίπτωση για απλά ή και ευαίσθητα ( 9(2)(ι) ) δεδομένα: Η επεξεργασία είναι απαραίτητη για σκοπούς επιστημονικής έρευνας[[9]](#footnote-9) που υπόκεινται σε κατάλληλες εγγυήσεις του άρθρου 89(1). Για τα ευαίσθητα προσωπικά δεδομένα ισχύει και το άρθρο 30 του ν. 4624/2019]* |  |  |

**Επεξήγηση και αιτιολόγηση της ελαχιστοποίησης των δεδομένων**

*[για να τεκμηριώσετε ότι εφαρμόζετε την αρχή της ελαχιστοποίησης (άρθρο 5(1)(γ))[[10]](#footnote-10) θα πρέπει να περιγράψετε του ελέγχους που εφαρμόζετε για να πετύχετε την ελάχιστη ποσότητα προσωπικών δεδομένων που χρειάζεστε για να εκπληρώσετε τον σκοπό σας. Θα πρέπει να έχετε τόσα πολλά δεδομένα (κατάλληλα, επαρκή), αλλά όχι περισσότερα (τα αναγκαία) και μόνο αυτά που εξυπηρετούν (συναφή) τον σκοπό σας]*

|  |  |
| --- | --- |
| **Λεπτομέρειες σχετικά με τα δεδομένα που επεξεργαζόμαστε** | **Έλεγχοι για την ελαχιστοποίηση των δεδομένων** |
|  |  |

**Επεξήγηση και αιτιολόγηση της ποιότητας των δεδομένων**

*[για να τεκμηριώσετε ότι εφαρμόζετε την αρχή της ακρίβειας (άρθρο 5(1)(δ))[[11]](#footnote-11) θα πρέπει να περιγράψετε του ελέγχους που εφαρμόζετε για να βεβαιωθείτε ότι τα προσωπικά δεδομένα που συλλέγεται και στη συνέχεια χρησιμοποιείτε είναι τα ακριβή (τα ορθά, σωστά) σε σχέση πάντα με τον επιδιωκόμενο σκοπό. Δηλαδή τα δεδομένα δεν είναι λανθασμένα ή παραπλανητικά ως προς οποιοδήποτε πραγματικό ζήτημα αφορά το υποκείμενο των δεδομένων σε σχέση με τον σκοπό.[[12]](#footnote-12)]*

|  |  |
| --- | --- |
| **Λεπτομέρειες σχετικά με τα δεδομένα που επεξεργαζόμαστε** | **Έλεγχοι για την ποιότητα των δεδομένων** |
|  |  |
|  |  |

**Επεξήγηση και αιτιολόγηση του χρόνου αποθήκευσης**

*[Σύμφωνα με την αρχή περιορισμού της περιόδου αποθήκευσης (άρθρο 5(1)(ε))[[13]](#footnote-13) δεν μπορείτε να τα διατηρήσετε τα προσωπικά δεδομένα για περισσότερο από όσο πραγματικά τα χρειάζεστε σε σχέση πάντα με τον επιδιωκόμενο σκοπό. Διαφορετικοί χρόνοι διατήρησης μπορούν να οριστούν για υποσύνολα των προσωπικών δεδομένων χρησιμοποιώντας απόλυτους (πχ έως το 2030) ή σχετικούς χρόνους (6 μήνες από την τελευταία επίσκεψη) ή άλλα σαφή κριτήρια. Σε κάθε περίπτωση πρέπει να αιτιολογήσετε τη επιλογή σας με σαφήνεια λαμβάνοντας υπόψη πχ νομικές και κανονιστικές απαιτήσεις, πραγματικές ανάγκες, πρότυπα ή οδηγίες του κλάδου κλπ. Είναι επίσης σημαντικό να αναφερθείτε στον τρόπο διαγραφής]*

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορίες δεδομένων** | **Χρόνος Διατήρησης**  | **Αιτιολόγηση του χρόνου διατήρησης** | **Μηχανισμός διαγραφής στο τέλος της διάρκειας αποθήκευσης** |
|  |  |  |  |

**Αξιολόγηση των ελέγχων για την διαφανή ενημέρωση των υποκειμένων των δεδομένων**

*[Ελέγξετε κατά πόσο τηρείτε την αρχή της διαφάνειας, αξιολογώντας την εφαρμογή των στοιχείων ενημέρωσης των υποκειμένων των δεδομένων σύμφωνα με τις υποχρεώσεις των άρθρων 13 και 14 του GDPR.]*

|  |  |
| --- | --- |
| **Έλεγχοι για το δικαίωμα στην ενημέρωση**  | **Πως εφαρμόζονται;** |
| Ποια είναι η φύση της σχέσης σας με τα φυσικά πρόσωπα; Συλλέγετε τα δεδομένα από τους ίδιους ή από τρίτους; |  |
| Τα φυσικά πρόσωπα θα έχουν άμεσο έλεγχο στα προσωπικά τους δεδομένα (πχ μέσω χρήσης εφαρμογών) ή όχι;. Περιγράψτε τον τρόπο.  |  |
| Θα το θεωρούσαν λογικό να χρησιμοποιήσετε τα δεδομένα τους με αυτόν τον τρόπο; |  |
| Γνωρίζουν τους σκοπούς για τους οποίους συλλέγετε τα δεδομένα τους και ποια είναι αυτά τα δεδομένα;  |  |
| Γνωρίζουν τον χρόνο που θα διατηρήσετε τα προσωπικά τους δεδομένα για κάθε σκοπό; |  |
| Γνωρίζουν ποια δικαιώματα έχουν τα φυσικά πρόσωπα (απόσυρση συγκατάθεσης, διαγραφή δεδομένων κλπ.) και πως να τα ασκούν ; |  |
| Γνωρίζουν εάν υπάρχει μεταφορά των δεδομένων τους σε τρίτους και σε ποιους (ή ποιες κατηγορίες παραληπτών) ή αν υπάρχει διεθνή διαβίβαση (εκτός ΕΟΧ); |  |
| Γνωρίζουν τα στοιχεία επικοινωνίας με τον υπεύθυνο επεξεργασίας και τον υπεύθυνο προστασίας δεδομένων αν υπάρχει. |  |

**Αξιολόγηση των ελέγχων για τη λήψη της συγκατάθεσης**

*[Οι παρακάτω έλεγχοι έχουν στόχο να διαπιστωθεί ότι εφόσον η συγκατάθεση είναι η νομική βάση επεξεργασίας των δεδομένων, τότε αυτή καλύπτει τις προϋποθέσεις του άρθρου 7 και στην περίπτωση παιδιών του άρθρου 8 του GDPR]*

|  |  |
| --- | --- |
| **Έλεγχοι για τη λήψη της συγκατάθεσης**  | **Πως εφαρμόζονται;** |
| Όταν η επεξεργασία βασίζεται σε συγκατάθεση, είστε σε θέση να αποδείξετε ότι το υποκείμενο των δεδομένων συγκατατέθηκε; |  |
| Έχετε εξασφαλίσει ότι η συγκατάθεση δίνεται ελεύθερα; |  |
| Το υποκείμενο τω δεδομένων έχει ενημερωθεί εκ των προτέρων ότι έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή; |  |
| Το υποκείμενο τω δεδομένων έχει ενημερωθεί ότι ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της;  |  |
| Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα; |  |
| Όταν επεξεργάζεστε δεδομένα για διακριτούς σκοπούς, λαμβάνετε συγκατάθεση για κάθε διακριτό σκοπό;  |  |
| Η συγκατάθεση παρουσιάζεται σε κατανοητή και ευανάγνωστη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα προσαρμοσμένη στον χρήστη-στόχο (ιδιαίτερα για τα παιδιά); |  |
| Υπάρχει συγκατάθεση των γονέων/κηδεμόνων για ανηλίκους κάτω των 18 ετών; Εάν αφορά υπηρεσίες τη κοινωνίας της πληροφορίας (πχ χρήση διαδικτυακών υπηρεσιών) η συγκατάθεση των γονέων/κηδεμόνων είναι για ανηλίκους κάτω των 15 ετών; |  |
| Το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των προσωπικών δεδομένων του που ανήκουν στις ειδικές κατηγορίες (ή ευαίσθητα δεδομένα) ; |  |

**Αξιολόγηση των ελέγχων για τα δικαιώματα των φυσικών προσώπων**

*[Για όσα δικαιώματα των φυσικών προσώπων ισχύουν, με βάση τους σκοπούς της επεξεργασίας, ελέγξετε το πως τα εφαρμόζετε, λαμβάνοντας υπόψη τα σχετικά άρθρα του GDPR.]*

|  |  |
| --- | --- |
| **Δικαιώματα** | **Πως εφαρμόζονται;** |
| Έλεγχοι για το δικαίωμα στην πρόσβασης στα δεδομένα ( άρθρο 15) |   |
| Έλεγχοι για το δικαίωμα διόρθωσης των δεδομένων ( άρθρο 16) |  |
| Έλεγχοι για το δικαίωμα διαγραφής των δεδομένων ( άρθρο 17) |  |
| Έλεγχοι για το δικαίωμα περιορισμού της επεξεργασίας των δεδομένων ( άρθρο 18) |  |
| Έλεγχοι για το δικαίωμα στη φορητότητα των δεδομένων ( άρθρο 20) |  |
| Έλεγχοι για το δικαίωμα εναντίωσης στην επεξεργασία των προσωπικών δεδομένων ( άρθρο 21) |  |
| Έλεγχοι για το δικαίωμα του φυσικού προσώπου να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο. ( άρθρο 22) |  |

**Περιγραφή των ελέγχων για τους εκτελούντες την επεξεργασία**

*[για κάθε εκτελούντα την επεξεργασία περιγράψτε σύντομα αλλά περιεκτικά την εμπλοκή του στην επεξεργασία και κυρίως να είναι σαφές αν υπάρχει σύμβαση, αν περιλαμβάνονται όροι για την προστασία των προσωπικών δεδομένων και αν αυτοί καλύπτουν τις απαιτήσεις του άρθρου 28 (πχ χρήση τυποποιημένων συμβατικών ρητρών (ΕΕ) 2021/915 της ευρωπαϊκή επιτροπής[[14]](#footnote-14)), περιλαμβανομένων και των τυχών υπεργολάβων του]*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Εκτελών την Επεξεργασία**  | **Υπεργολάβοι του Εκτελούντα την Επεξεργασία**  | **Αντικείμενο της επεξεργασίας** | **Αναφορά σε σύμβαση**  | **Συμμόρφωση με το Άρθρο 28 του GDPR** |
|  |  |  |  |  |

**Προσδιορισμός και περιγραφή των ελέγχων σχετικά με τη διαβίβαση δεδομένων εκτός του ΕΟΧ ( Ευρωπαϊκού Οικονομικού Χώρου)**

*[Η διαβίβαση και αποθήκευση δεδομένων σε χώρα εκτός ΕΟΧ θεωρείται διεθνής διαβίβαση και πρέπει να διενεργείται με τις προϋποθέσεις του Κεφαλαίου V του GDPR ( άρθρα 44-49). Σε περίπτωση που χρησιμοποιείτε υπηρεσίες cloud, βεβαιωθείτε αν τα δεδομένα αποθηκεύονται εντός ΕΟΧ ή όχι. Οι διαβιβάσεις σε τρίτες χώρες είναι εφικτές βάσει απόφασης επάρκειας της ευρωπαϊκής επιτροπής[[15]](#footnote-15) ή τις προϋποθέσεις του άρθρου 46[[16]](#footnote-16) ή τις παρεκκλίσεις το του άρθρου 49 του GDPR ]*

|  |  |  |  |
| --- | --- | --- | --- |
| **Τα σύνολα δεδομένων**  | **Η χώρα διαβίβασης για την οποία υπάρχει απόφαση επάρκειας**  | **Άλλη χώρα διαβίβασης**  | **Προϋποθέσεις για την διαβίβαση (τυποποιημένες συμβατικές ρήτρες, εσωτερικοί εταιρικοί κανονισμοί κλπ)** |
|  |  |  |  |

**Αξιολόγηση των μέτρων προστασίας των προσωπικών δεδομένων**

*[Αναφέρετε με σαφή τρόπο τα μέτρα ασφαλείας που εφαρμόζετε για όλες τις επεξεργασία των προσωπικών δεδομένων και αξιολογείστε με σαφήνεια τον τρόπο που τα εφαρμόζετε αναφέροντας τις δικές σας εκτιμήσεις ή των ειδικών τις ευπάθειες που είναι αντιληπτές, τον βαθμό προστασίας που προσφέρουν ή και προτάσεις βελτίωσης. Ο στόχος των μέτρων που λαμβάνονται θα πρέπει να είναι η προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των προσωπικών δεδομένων[[17]](#footnote-17), αλλά και η τήρηση των υποχρεώσεων του GDPR.]*

|  |  |
| --- | --- |
| **Μέτρα προστασίας** | **Αξιολογήστε το πως εφαρμόζονται**  |
| [ενδεικτικό παράδειγμα: Αποθήκευση προσωπικών δεδομένων σε πλατφόρμα πολλαπλών χώρων XXXX (multi tenant platform)] | Οι χρήστες που έχουν πρόσβαση στην πλατφόρμα XXXX, εκχωρούνται σε διαφορετικά επίπεδα εξουσιοδότησης κατά την εγγραφή τους (π.χ. διαχειριστής, απλοί χρήστες) με διαφορετικά δικαιώματα και δικαιώματα πρόσβασης. Ως γενικός εμπειρικός κανόνας, οι συμμετέχοντες στο προσωπικό έχουν πρόσβαση για προβολή ή αλλαγή πληροφοριών μόνο των υποκειμένων των δεδομένων του μητρώου, οι οποίοι σχετίζονται με τη δική τους χωρική τοποθεσία. Αυτό έχει ως αποτέλεσμα την αποτροπή μη εξουσιοδοτημένης πρόσβασης |
| [Ενδεικτικό παράδειγμα:Δέσμευση εμπιστευτικότηταςα/ οι υπάλληλοι ορισμένου χρόνου που εργάζονται στον οργανισμό δεσμεύονται με τη δεσμεύονται γραπτά με όρους εμπιστευτικότητας (παρατήρηση: για το Δημόσιο οι μόνιμοι δεσμεύονται με την τήρηση του απορρήτου από τον κώδικα δημοσίων υπαλλήλων)β/ υπάλληλοι εργολάβων και προμηθευτών (πχ καθαρίστριες, προσωπικό φύλαξης) που έχουν πρόσβαση στους χώρους φύλαξης των φακέλων προσωπικού δεσμεύονται γραπτά με όρους εμπιστευτικότητας] | Δεν υπάρχουν σχετικές δεσμεύσεις σε καμία από τις κατηγορίες αυτές των εργαζομένων στον οργανισμό. Δεν υπάρχουν επίσης και οι σχετικές διαδικασίες αλλά και ούτε οι ανάλογες προβλέψεις στις προκηρύξεις υπηρεσιών καθαριότητας που να δεσμεύουν τον εργολάβο ώστε να δεσμεύει τους εργαζόμενους του με όρους εμπιστευτικότητας.  |
| [Ενδεικτικό παράδειγμα:Εφαρμογή πολιτικής ασφάλειας δεδομένων] | Η πολιτική ασφάλειας δεδομένων εφαρμόζεται μερικώς στον βαθμό που υλοποιείται μέσω του Active Directory του οργανισμού και περιλαμβάνει μόνο την διαχείριση του κωδικού, τα δικαιώματα πρόσβασης στους κοινόχρηστους πόρους και τον χρόνο άεργου κλειδώματος του υπολογιστή. Θα πρέπει να εφαρμοστεί η πολιτική στο σύνολό της εκπαιδεύοντας το προσωπικό.  |
|  |  |

**Βήμα 6: Προσδιορισμός και εκτίμηση των κινδύνων**

*[Σε κάθε επεξεργασία οι πιθανές ευπάθειες και ο μη ικανοποιητικός βαθμός προστασίας των μέτρων που έχετε αξιολογήσει στον παραπάνω πίνακα, αποτελούν πηγές κινδύνων που μπορεί να οδηγήσουν στη παραβίαση των δεδομένων. Αποτυπώστε τον κάθε τύπο της ενδεχόμενης παραβίασης ( εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας) ή ομάδα τύπων παραβίασης που έχουν τον ίδιο βαθμό επιπτώσεων και περιγράψτε τη πηγή του κινδύνου καθώς και τη φύση των δυνητικών επιπτώσεων στα άτομα. Για την εκτίμηση της πιθανότητας να συμβεί η παραβίαση (να υλοποιηθεί ο κίνδυνος) και τον βαθμό των επιπτώσεων στα φυσικά πρόσωπα, θα πρέπει να μελετήσετε το* [*ΠΑΡΑΡΤΗΜΑ*](#_ΠΑΡΑΡΤΗΜΑ)*. Ακολουθούν διάφορα παραδείγματα αποτύπωσης και εκτίμησης]*

|  |  |  |  |
| --- | --- | --- | --- |
| **Περιγράψτε για κάθε επεξεργασία τους ενδεχόμενους τύπους της παραβίασης από πηγή κινδύνου και τη φύση των δυνητικών επιπτώσεων στα άτομα.** | **Πιθανότητα παραβίασης** **Μικρή, Μεσαία, Μεγάλη** | **Βαθμός επιπτώσεων****Μικρός, Σημαντικός ή Σοβαρός** | **Συνολικός κίνδυνος****Χαμηλός, Μεσαίος ή Υψηλός** |
| [ενδεικτικό παράδειγμα 1: Παραβίαση εμπιστευτικότητας από αθέμιτη πρόσβαση στα δεδομένα λόγω πρόσβασης στις ηχογραφημένες συνεντεύξεις από πιθανή απώλεια του μαγνητοφώνου ηχογράφησης. Η πιθανότητά είναι μικρή όμως οι επιπτώσεις για τα φυσικά πρόσωπα είναι σοβαρή δεδομένου ότι στη συνέντευξη καλύπτονται θέματα ψυχικής υγείας που μπορεί να επηρεάσει την κοινωνική και επαγγελματική ζωή του…………..] | Μικρή | Σοβαρός | Μεσαίος |
| [ενδεικτικό παράδειγμα 2: Κίνδυνος αποκάλυψης προσωπικών δεδομένων λόγω έλλειψης δέσμευσης εμπιστευτικότητας του προσωπικού που δεν υποχρεώνεται με άλλον τρόπο. Παραβίαση εμπιστευτικότηταςΤυχών αποκάλυψη των προσωπικών δεδομένων των υποκείμενων των δεδομένων θα είχε σημαντικές επιπτώσεις στη κοινωνική συμπεριφορά των συναδέλφων τους και στην επαγγελματική τους ζωή….] | Μικρή | Σημαντικός | Χαμηλός |
| [ενδεικτικό παράδειγμα 3: Ανεπιθύμητη αλλαγή στα δεδομένα από ακούσια αλλαγή ή μη εξουσιοδοτημένη πρόσβαση και παραβίαση της ακεραιότητας των δεδομένων λόγω κοινόχρηστης χρήσης του αρχείου με τα οικονομικά στοιχεία. Παραβίαση ακεραιότητας.Σε περίπτωση που γίνει ανεπιθύμητη αλλαγή δεν είναι εύκολο να ανιχνευτεί η πηγή της αλλαγής ώστε να ληφθούν άμεσα τα κατάλληλα μέτρα.Παρόλα αυτά για την παραπάνω παραβίαση υπάρχουν οι διαδικασίες υπομνήματος και ενστάσεων που αντιμετωπίζουν τον κίνδυνο, όμως οι υπόχρεοι μπορεί να έχουν σημαντική οικονομική ζημιά ή να καταβάλουν σημαντική προσπάθεια για την υπεράσπισή τους)Η αλλαγή αυτή μπορεί να έχει οικονομικές επιπτώσεις στον υπόχρεο από τον λάθος προσδιορισμό της οφειλής ή την μη έγκαιρη ενημέρωση του από λάθος στα στοιχεία επικοινωνίας.] | Μικρή | Σημαντικός | Χαμηλός |
| **[**ενδεικτικό παράδειγμα 4: Μη εξουσιοδοτημένη πρόσβαση ή και μη διαθεσιμότητα προσωπικών δεδομένων λόγω εξωτερικής δικτυακής κακόβουλης επίθεσης (hacking). Παραβίαση εμπιστευτικότητας και διαθεσιμότητας.Οι κακόβουλες επιθέσεις γενικά στους υπολογιστές της Διεύθυνσης …. του οργανισμού (π.χ. ransomware) μπορεί να έχουν μεγάλες επιπτώσεις στη λειτουργία της Διεύθυνσης με την διαγραφή ή την ομηρία δεδομένων να είναι πιο εκτεταμένη και να οδηγήσει σε μη διαθεσιμότητα δεδομένων (όπως ιατρικές γνωματεύσεις κ.λπ.), με σοβαρό αντίκτυπο στα υποκείμενα των δεδομένων. Ενίοτε ο στόχος της επίθεσης να είναι η κλοπή δεδομένων που έχει εξίσου σοβαρές επιπτώσεις.] | Μεσαία | Σοβαρός | Υψηλή |
|  |  |  |  |

**Βήμα 7: Προσδιορισμός μέτρων για τη μείωση του κινδύνου**

*[Προσδιορίστε τα πρόσθετα μέτρα που θα μπορούσατε να λάβετε για να εξαλείψετε ή να μειώσετε ή ακόμη και να αποδεχτείτε τους κινδύνους που εντοπίζονται ως μεσαίοι ή υψηλοί κίνδυνοι στο βήμα 6.]*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κίνδυνος | Επιλογές για τη μείωση ή την εξάλειψη του κινδύνου | Αντίδραση στον κίνδυνο: Εξάλειψη, Μείωση ή γίνεται Αποδεκτός | Υπολειπόμενος κίνδυνος Χαμηλός, μεσαίος ή υψηλός | Το μέτρο εγκρίθηκεΝαι όχι |
| [Ενδεικτικό παράδειγμα 1: Παραβίαση εμπιστευτικότητας από αθέμιτη πρόσβαση στα δεδομένα λόγω πρόσβασης στις ηχογραφημένες συνεντεύξεις από πιθανή απώλεια του μαγνητοφώνου ηχογράφησης] | Χρήση ψηφιακού μαγνητοφώνου με δυνατότητα κρυπτογράφησης και κρυπτογράφηση του αρχείου ηχογράφησης.Άμεση μεταφορά του κρυπτογραφημένου αρχείου σε ασφαλές σύστημα και διαγραφή από το φορητό μαγνητοφωνο | Μείωση | Χαμηλός |  |
| [ενδεικτικό παράδειγμα 4: Μη εξουσιοδοτημένη πρόσβαση ή μη διαθεσιμότητα προσωπικών δεδομένων λόγω εξωτερικής δικτυακής κακόβουλης επίθεσης (hacking). Παραβίαση εμπιστευτικότητας και διαθεσιμότητας.] | Προτείνεται η αγορά επαγγελματικού antivirus με αυτόματες ενημερώσεις και κεντρική διαχείριση αρχείων. Δημιουργία backup αποσυνδεμένο από το δίκτυο.Εφαρμογή των πολιτικών ασφάλειας πληροφοριών και αποδεκτής χρήσης | Μείωση | Χαμηλός |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Βήμα 8: Εγκρίσεις και καταγραφή αποτελεσμάτων**

[*να συμπληρωθεί από τον ΥΠΔ ή τον υπεύθυνο για την διαχείριση των δεδομένων του οργανισμού ]*

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/date** | **Notes** |
| Τα μέτρα εγκρίθηκαν από:  |  |  |
| Ο υπολειπόμενος κίνδυνος εγκρίθηκε από :  |  |  |
| Οι συμβουλές του ΥΠΔ παρέχονται από : |  |  |
| Περίληψη των συμβουλών του ΥΠΔ:  |
| Οι συμβουλές του ΥΠΔ που έγιναν δεκτές ή απορρίφθηκαν από: |  |  |
| Σχόλια: |
| Οι απαντήσεις εξετάστηκαν από: |  |  |
| Σχόλια: |
| Η παρούσα DPIA θα επανεξεταστεί από: |  |  |

## ΠΑΡΑΡΤΗΜΑ

## 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 στον οργανισμό 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** | **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.

## 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:

* Γενικές επιπτώσεις στο Υποκείμενο των δεδομένων
* Υγεία και ασφάλεια του Υποκειμένου των δεδομένων
* Οικονομικά του οργανισμού
* Φήμη του οργανισμού
* 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*

## 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.

## 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.

## Καθορισμός Σχεδίου Αντιμετώπισης Κινδύνων

Για τους κινδύνους που έχουν συμφωνηθεί ότι υπερβαίνουν το όριο αποδοχής από του οργανισμού 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. Ο οργανισμός 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. ***μειώστε τον κίνδυνο -*** εφαρμόστε τους κατάλληλους ελέγχους για να μειώσετε την πιθανότητα και / ή την επίδραση του κινδύνου.
2. ***Αποφύγετε/εξαλείψτε*** τον κίνδυνο με τη λήψη μέτρων που σημαίνει ότι δεν ισχύει πλέον
3. ***Μοιραστείτε /αποδεχτείτε*** 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 διαχείριση του κινδύνου, συμπεριλαμβανομένου του κατόχου του κινδύνου.

1. «**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-1)
2. «**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-2)
3. Άρθρο 3 του GDPR [↑](#footnote-ref-3)
4. Άρθρο 4(7) GDPR - «υπεύθυνος επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους [↑](#footnote-ref-4)
5. Άρθρο 4(8) GDPR - «εκτελών την επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας [↑](#footnote-ref-5)
6. Άρθρο 35 (8) GDPR: «*Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας που αναφέρονται στο άρθρο 40 από τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας»* [↑](#footnote-ref-6)
7. ή ειδικής κατηγορίας 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 ( άρθρο 9(1) GDPR) [↑](#footnote-ref-7)
8. Π.χ α) Αν τα υπάρχοντα έντυπα συγκατάθεσης δεν είναι τα τελικά ή αν η διαδικασία λήψης συγκατάθεσης έχει κενά ως προς την τεκμηρίωση της ενημέρωσης, τότε στην εφαρμογή απαντάμε ΟΧΙ και αιτιολογούμε το τι πρέπει να γίνει, β) για την έννομη υποχρέωση θα πρέπει να αναφέρουμε το εδάφιο του νόμου στην αιτιολογία, γ) πως υπερισχύουν τα έννομα συμφέροντα του υπεύθυνου επεξεργασίας ή τρίτου έναντι του υποκειμένου των δεδομένων κλπ [↑](#footnote-ref-8)
9. Επειδή η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται, σύμφωνα με το άρθρο 5(1)(β) του GDPR, ασύμβατη με τους αρχικούς σκοπούς συλλογής των δεδομένων, τα κριτήρια νομιμότητας για τους περαιτέρω σκοπούς παραμένουν αυτά της συλλογής. Θα πρέπει επομένως να αιτιολογηθούν οι προϋποθέσεις για την νομιμότητα επεξεργασίας των αρχικών σκοπών συλλογής των δεδομένων.

Επιπλέον αν περιλαμβάνονται και ευαίσθητα προσωπικά δεδομένα να εξεταστούν αν ενδεχομένως καλύπτονται οι προϋποθέσεις και οι κατάλληλες εγγυήσεις του άρθρου 30 του ν. 4624/2019 [↑](#footnote-ref-9)
10. Τα προσωπικά δεδομένα: *είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»)*, [↑](#footnote-ref-10)
11. Τα προσωπικά δεδομένα: *είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»),* [↑](#footnote-ref-11)
12. Για να διασφαλίσετε ότι τα δεδομένα σας δεν είναι ανακριβή ή παραπλανητικά θα πρέπει να καταγράψετε με ακρίβεια τις παρεχόμενες πληροφορίες και την πηγή των πληροφοριών, να λαμβάνετε εύλογα, υπό τις περιστάσεις, μέτρα για να διασφαλίσετε την ακρίβεια των πληροφοριών και να εξετάστε προσεκτικά τυχόν προκλήσεις σχετικά με την ακρίβεια των πληροφοριών . [↑](#footnote-ref-12)
13. Τα προσωπικά δεδομένα: *διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»),* [↑](#footnote-ref-13)
14. <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021D0915&from=EN> [↑](#footnote-ref-14)
15. <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_el> [↑](#footnote-ref-15)
16. Όπως οι [τυποποιημένες συμβατικές ρήτρες της απόφασης (ΕΕ) 2021/914 της 4/6/2021](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en) ή οι [Δεσμευτικοί Εταιρικοί Κανόνες- Binding Corporate Rules (BCR)](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_el) [↑](#footnote-ref-16)
17. Εμπιστευτικότητα (Confidentiality):*Όταν γνωρίζει μόνο αυτός/αυτή που είναι ανάγκη να γνωρίζει -* *δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα*, Ακεραιότητα (integrity): *Οι πληροφορίες/δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα*, Διαθεσιμότητα (availability): *Οι πληροφορίες/δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.*

*Η μη τήρηση τουλάχιστον μιας εκ των τριών συνιστά παραβίαση* [↑](#footnote-ref-17)