****

Ερωτηματολόγιο συλλογής πληροφοριών για την Εκτίμηση Αντικτύπου σχετικά με

την προστασία των προσωπικών δεδομένων

|  |  |
| --- | --- |
| **Διαβάθμιση Εγγράφου:** | **Εμπιστευτικό** |
| **Έκδοση:** | **1** |
| **Ημερομηνία:** | **October 2020** |
| **Συντάκτης Εγγράφου:** | **Ομάδα Υλοποίησης Συμμόρφωσης με το ΓΚΠΔ** |
| **Ιδιοκτήτης Εγγράφου:** | **ΑΠΘ** |

**Ιστορικό Ανασκόπησης**

|  |  |  |  |
| --- | --- | --- | --- |
| **Έκδοση** | **Ημερομηνία** | **Συντάκτης Ανασκόπησης**  | **Περίληψη Αλλαγών** |
|  |  |  |  |
|  |  |  |  |

**Διανομή**

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

**Έγκριση**

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

Ερωτηματολόγιο συλλογής πληροφοριών για την Εκτίμηση Αντικτύπου σχετικά με

την προστασία των προσωπικών δεδομένων

Αυτή η φόρμα αποτελεί ένα εργαλείο συλλογής πληροφοριών για μια κρίσιμη πράξη επεξεργασίας προσωπικών δεδομένων η οποία μπορεί να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες του φυσικού προσώπου στο οποίο ανήκουν τα προσωπικά δεδομένα. Επεξεργασία δηλαδή που αφορά ευαίσθητα προσωπικά δεδομένα (υγεία, εθνικότητα, βιομετρικά , εθνικότητα κ.α.), μεγάλης κλίμακας επεξεργασία ( > 1000 άτομα), χρήση νέας τεχνολογίας, δημιουργία προφίλ κλπ.

Οι απαντήσεις θα αξιοποιηθούν στην εκτίμηση αντικτύπου που θα έχει συνολικά η επεξεργασία στο έργο ως προς προστασία των προσωπικών δεδομένων και κατ’ επέκταση την προστασία των φυσικών προσώπων.

Για κάθε πράξη θα πρέπει να συμπληρωθεί ξεχωριστό ερωτηματολόγιο.

Γενικές πληροφορίες για την πράξη επεξεργασίας

|  |  |
| --- | --- |
| **Όνομα του έργου που αφορά η επεξεργασία** |  |
| **Σκοπός του έργου που αφορά η επεξεργασία:** |  |
| **Υπεύθυνος έργου (Owner):** |  |
| **Επιχειρησιακή Διαδικασία ή Υπηρεσία που εμπλέκεται στην συγκεκριμένη επεξεργασία****(Operational Process):** |  |
| **Τίτλος ή όνομα που θα μπορούσε να δοθεί στην επεξεργασία** |  |

# ΑΝΑΛΥΣΗ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

## Περιγραφή της πράξης επεξεργασίας

|  |
| --- |
| *[να περιγράψετε την πράξη επεξεργασίας με όρους:** *γεωγραφικής τοποθεσίας π.χ. χώρες, γραφεία, κέντρα δεδομένων*
* *οργανωτικές μονάδες π.χ. συγκεκριμένα τμήματα που μετέχουν*
* *άλλες διαδικασία (-ες) του Πανεπιστημίου που εμπλέκονται άμεσα με αυτή ( πχ διαδικασίες από όπου αναμένονται ή και που πρόκειται να διαβιβαστούν δεδομένα*
* *Αν αφορά φοιτητές ή εργαζόμενους ή άλλης κατηγορίας φυσικά πρόσωπα*
* *Συστήματα που θα χρησιμοποιηθούν για την συγκεκριμένη επεξεργασία (υποδομές και εργαλεία τεχνολογιών πληροφορικής και δικτύων , άλλος εξοπλισμός που θα χρησιμοποιηθεί)*

*]* |

## Προσωπικά δεδομένα που περιλαμβάνονται

|  |
| --- |
| *[Περιγράψτε τις κατηγορίες των προσωπικών δεδομένων που θα χρησιμοποιήσετε αρχικά για την πράξη επεξεργασίας ( π.χ όνομα, διεύθυνση, τηλέφωνα, ημερομηνία πρόσληψης, κλπ). Να αναφέρετε ξεχωριστά σε άλλη παράγραφο τα ευαίσθητα προσωπικά δεδομένα αν υπάρχουν ( δεδομένα υγείας, εθνικότητα, βιομετρικά, ποινικές καταδίκες, θρήσκευμα) ]*  |

## 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;

|  |
| --- |
| *[Που θα χρησιμοποιηθούν τα δεδομένα που επεξεργάζεστε και για ποιο σκοπό; 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;

|  |
| --- |
| *[Για πόσο καιρό πρέπει να διατηρηθούν τα δεδομένα και γιατί; Για παράδειγμα υπάρχει συγκεκριμένο νομικό πλαίσιο που καθορίζει τον χρόνο διατήρησης ή υπάρχει εσωτερικός κανονισμός ή απόφαση της διοίκησης]* |

## Πως γίνεται η διαγραφή / καταστροφή των δεδομένων;

|  |
| --- |
| *[Σε περίπτωση που ο οργανισμός δε χρειάζεται πλέον τα δεδομένα ή έχει περάσει ο χρόνος διατήρισης, 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 προστασία τους π.χ. κρυπτογράφηση ή ανωνυμοποίηση των αποθηκευμένων δεδομένων, ή ντουλάπα που κλειδώνει ή κάποια άλλα μέτρα για τη προστασία τους;]* |

## 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, τι 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 Πανεπιστημίου 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 κινδύνους που αντιλαμβάνεστε ότι υπάρχουν και αντιμετωπίζετε κατά την εκτέλεση της ζητούμενης επεξεργασίας. Αυτές οι απειλές και αυτοί οι κίνδυνοι μπορεί να υπάρχουν ήδη και για άλλες επεξεργασίες που εκτελείτε]*

## Απειλές

## Κίνδυνοι

# ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ

Συμπληρώστε τους παρακάτω πίνακες επιπτώσεων, με βάση τις ακόλουθες κατηγορίες για τους κινδύνους όπως τους έχετε περιγράψει παραπάνω και για ποιες κατηγορίες προσωπικών δεδομένων ισχύουν αυτοί. Ακόμη 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 :

|  |
| --- |
| ***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. |

##  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) που μπορεί να υπάρξει για τον οργανισμό σε περίπτωση παραβίαση της διαθεσιμότητας για κάθε κατηγορία δεδομένων που επεξεργάζεστε στα παρακάτω χρονικά όρια.

|  |
| --- |
| ***Απώλεια Διαθεσιμότητας Δεδομένων (μη δυνατότητα ανάκτησης από αντίγραφα ασφαλείας)*** |
| **Πληροφορίες/****Δεδομένα** | 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 |
|  |  |  |  |  |  |

Αν η παραβίαση της διαθεσιμότητας πληροφοριών ανήκει στις κατηγορίες **Υψηλός ή Μεσαίος,** περιγράψτε παρακάτω τις επιπτώσεις που μπορεί να έχει αυτήσε κάθε μια από τις 3 παρακάτω περιοχές *(εξετάστε μόνο την περίπτωση με τον υψηλότερο κίνδυνο και την συχνότερη επεξεργασία προσωπικών δεδομένων )*

1. Νομική και συμβατική συμμόρφωση:
2. Επιχειρησιακή Λειτουργία:
3. Εμπιστοσύνη Φοιτητών /προμηθευτών/ προσωπικού, Φήμη Πανεπιστημίου:

##  Ακεραιότητα Δεδομένων

Η προστασία των δεδομένων από εσφαλμένη τροποποίηση των δεδομένων η οποία μπορεί να γίνει εσκεμμένα ή ακούσια. Εκτιμήστε τον κίνδυνο ( Υψηλός, Μεσαίος, Χαμηλός ) που μπορεί να υπάρξει για τον οργανισμό σε περίπτωση παραβίαση της ακεραιότητας για κάθε κατηγορία δεδομένων που επεξεργάζεστε.

|  |
| --- |
| ***Απώλεια Ακεραιότητας Δεδομένων (εσκεμμένη ή μη)*** |
| **Πληροφορίες/****Δεδομένα** | Χαμηλός | Μεσαίος | Υψηλός | Σχόλια/Παρατηρήσεις |
|  |  |  |  |  |

Αν η παραβίαση της ακεραιότητας ανήκει στις κατηγορίες **Υψηλός ή Μεσαίος,** περιγράψτε παρακάτω τις επιπτώσεις που μπορεί να έχει αυτήσε κάθε μια από τις 3 παρακάτω περιοχές *(εξετάστε μόνο την περίπτωση με τον υψηλότερο κίνδυνο και την συχνότερη επεξεργασία προσωπικών δεδομένων )*

1. Νομική και συμβατική συμμόρφωση:
2. Επιχειρησιακή Λειτουργία:
3. Εμπιστοσύνη Φοιτητών /προμηθευτών/ προσωπικού, Φήμη Πανεπιστημίου:

##  Εμπιστευτικότητα Δεδομένων

Η προστασία από την αποκάλυψη προσωπικών δεδομένων εσκεμμένα ή μη σε άτομα που δεν είναι ανάγκη να γνωρίζουν. Εκτιμήστε τον κίνδυνο ( High, Medium, Low) που μπορεί να υπάρξει για τον οργανισμό σε περίπτωση παραβίαση της εμπιστευτικότητας για κάθε κατηγορία δεδομένων που επεξεργάζεστε θεωρώντας ότι η αποκάλυψη γίνεται σε άτομα εκτός οργανισμού ή ακόμη και εντός οργανισμού στην περίπτωσή, που κατά την άποψή σας, θα καθιστούσε τον κίνδυνο υψηλότερο

|  |
| --- |
| ***Απώλεια Εμπιστευτικότητας Δεδομένων (εσκεμμένη ή μη)*** |
| **Πληροφορίες/****Δεδομένα** | Χαμηλός | Μεσαίος | Υψηλός | Σχόλια/Παρατηρήσεις |
|  |  |  |  |  |

Αν η παραβίαση της εμπιστευτικότητας ανήκει στις κατηγορίες **Υψηλός ή Μεσαίος,** περιγράψτε παρακάτω τις επιπτώσεις που μπορεί να έχει αυτήσε κάθε μια από τις 3 παρακάτω περιοχές *(εξετάστε μόνο την περίπτωση με τον υψηλότερο κίνδυνο και την συχνότερη επεξεργασία προσωπικών δεδομένων )*

1. Νομική και συμβατική συμμόρφωση:
2. Επιχειρησιακή Λειτουργία:
3. Εμπιστοσύνη Φοιτητών /προμηθευτών/ προσωπικού, Φήμη Πανεπιστημίου:

# Γενικά σχόλια / παρατηρήσεις:

**Στοιχεία του υπεύθυνου συμπλήρωσης του ερωτηματολογίου**

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

**Στοιχεία του υπεύθυνου αξιολόγησης**

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