Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Η Διαχείριση Κίνδυνων και η Εκτίμηση Αντικτύπου ως προς την Προστασία Προσωπικών Δεδομένων στην Πράξη

Ελένη Δάρρα

Επιβλέπων Καθηγητής
Δρ. Κωνσταντίνος Λιμνιώτης

Νοέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Η Διαχείριση Κίνδυνων και η Εκτίμηση Αντικτύπου ως προς την Προστασία Προσωπικών Δεδομένων στην Πράξη

Ελένη Δάρρα

Επιβλέπων Καθηγητής
Δρ. Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Νοέμβριος 2019

Περίληψη

Στη σημερινή εποχή και κυρίως λαμβάνοντας υπόψιν τη χρήση των νέων τεχνολογιών καθώς και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και το πεδίο εφαρμογής ενός είδους επεξεργασίας, θα λέγαμε ότι υπάρχει σοβαρός κίνδυνος απώλειας προσωπικών δεδομένων αλλά και καταπάτηση των δικαιωμάτων και των ελευθεριών του ατόμου. Για το λόγο αυτό ο όρος εκτίμηση αντικτύπου έχει βρει εφαρμογή, πριν από κάθε πράξη επεξεργασίας, στα προσωπικά δεδομένα προσωπικού χαρακτήρα. Συνήθως εκτιμάται ότι μια εκτίμηση αντικτύπου μπορεί να βοηθήσει τον εκάστοτε οργανισμό να εντοπίσει και να μετριάσει τους κινδύνους που προκύπτουν από διάφορες δραστηριότητες που μπορεί να προκύψουν.

Λαμβάνοντας υπόψιν τα ανωτέρω, η ανάγκη για μελέτη της εκπόνησης Εκτίμησης Αντικτύπου ως προς την προστασία Προσωπικών Δεδομένων (ΕΑΠΔ), κρίνεται επιτακτική ανάγκη στα πλαίσια εφαρμογής της σε πραγματικό περιβάλλον, επιλέγοντας συγκεκριμένη επεξεργασία δεδομένων, για ερευνητικούς σκοπούς, που πραγματοποιεί ένας οργανισμός. Ένας οργανισμός μπορεί να βοηθηθεί από μια τέτοιου είδους ΕΑΠΔ αξιοποιώντας τη διαχείριση κινδύνων που συνήθως πραγματοποιείται εφαρμόζοντας μια γνωστή μεθοδολογία (πχ. κατά ISO). Η ΕΑΠΔ από την άλλη πλευρά, αποτελεί μία διαδικασία, καθώς δεν εξετάζει μόνο θέματα ασφάλειας προσωπικών δεδομένων αλλά και θέματα που άπτονται, του πώς ικανοποιούνται τα δικαιώματα των προσώπων των οποίων τα δεδομένα υφίστανται επεξεργασία ή του αν συλλέγονται υπέρμετρα προσωπικά δεδομένα σε σχέση με τους επιδιωκόμενους σκοπούς. Η εκπόνηση μιας ΕΑΠΔ μπορεί επιπλέον να θεωρηθεί μια σημαντική διαδικασία που θα αποτελεί συνέχεια για τον κάθε οργανισμό.

Πιο συγκεκριμένα, η ΕΑΠΔ εμπεριέχει την πλήρωση της υποχρέωσης λογοδοσίας, η οποία επίσης εισάγεται με τον Γενικό Κανονισμό Προσωπικών Δεδομένων (ΓΚΠΔ), καθώς υποχρεώνει τους υπεύθυνους επεξεργασίας να συμμορφώνονται με τις προδιαγραφές του ΓΚΠΔ, αλλά και να αποδεικνύουν ότι έχουν λάβει τα απαραίτητα μέτρα για τη διασφάλιση της συμμόρφωσης με τον Κανονισμό. Τέλος, η μη συμμόρφωση με τις απαιτήσεις ΕΑΠΔ μπορεί να οδηγήσει στην επιβολή κυρώσεων – συμπεριλαμβανομένων των προστίμων - από την εκάστοτε αρμόδια εποπτική αρχή.

Summary

Nowadays, taking into consideration the use of new technologies as well as the nature, the scope, the context as well as the scope of processing, it is worth mentioning that there is an important risk of loss of personal data and violation of individual rights and freedoms. For this reason, impact assessment applies, before any processing act, to the personal data. It is usually estimated that the impact assessment can help the organization identify and mitigate the risks arising from various activities that may occur.

Bearing in mind the above, the need for a Data Protection Impact Assessment (DPIA) is necessary in the context of its implementation in a real-world environment, by selecting specific data processing procedure for research purposes carried out by an organization. An organization can assist such a type of DPIA by taking advantage of the management risk that is usually performed by applying a known method (e.g. ISO). The DPIA, on the other hand, is a process that addresses not only matters related to the security of personal data but also states the importance of how the persons rights are being processed or excessive personal data are being collected in relation to the aims pursued. Preparing an DPIA can additionally be considered an important process that will be a continuum for any organization.

More specifically, the DPIA includes the fulfillment of the accountability obligation, which is also introduced by the General Data Protection Regulation (GDPR), as it obliges processors to comply with the requirements of the GDPR, and to demonstrate that they have taken the necessary measures to ensure the compliance with the Regulation. Finally, any possible failure to comply with the GDPR requirements can lead to sanctions by the competent supervisory authority.

Ευχαριστίες

Η παρούσα μεταπτυχιακή διατριβή πραγματοποιήθηκε στα πλαίσια του μεταπτυχιακού Προγράμματος Σπουδών Ασφάλειας Υπολογιστών και Δικτύων της Σχολής Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου. Ως ελάχιστη δυνατή μνεία, οφείλω να ευχαριστήσω όλους όσους συνέβαλαν στην εκπόνησή της και ιδιαίτερα τον επιβλέποντα καθηγητή μου, κο. Κωνσταντίνο Λιμνιώτη για την εμπιστοσύνη που μου έδειξε, την επιστημονική του καθοδήγηση, τις υποδείξεις του, τη συνεχή υποστήριξη του καθώς η συνεργασία μαζί του έπαιξε πολύ σημαντικό ρόλο στην πραγματοποίησή της.

Τις ευχαριστίες μου θα ήθελα να εκφράζω επίσης στους γονείς μου Κωνσταντίνο και Κερασία, καθώς και τον αδερφό μου Άρη, που με υπομονή και κουράγιο πρόσφεραν την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της μεταπτυχιακής μου διατριβής. Τέλος θα ήθελα να ευχαριστήσω τον σύζυγο μου Κωνσταντίνο που με την αμέριστη συμπαράσταση που έδειξε καθ' όλη τη διάρκεια της μεταπτυχιακής διατριβής, μπόρεσα με ζήλο να ολοκληρώσω τη μεταπτυχιακή μου διατριβή.

Αθήνα, Νοέμβριος 2019

Ελένη Δάρρα

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Ο νέος Κανονισμός 2016/679[1] (Γενικός Κανονισμός για την Προστασία Δεδομένων – ΓΚΠΔ) έχει τεθεί σε εφαρμογή από την 25η Μαΐου 2018. Στον Κανονισμό αυτό περιλαμβάνεται το άρθρο 35 το οποίο εισάγει την έννοια της εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων – ΕΑΠΔ (Data Protection Impact Assessment – DPIA). Αντίστοιχα και η οδηγία 2016/680 έχει εισάγει την έννοια της εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων και ειδικότερα στο άρθρο 27 της οδηγίας, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, ορίζει ότι η εκτίμηση των επιπτώσεων στην ιδιωτική ζωή είναι αναγκαία όταν «[ο] τύπος [της] επεξεργασίας [...] είναι πιθανόν να προκαλέσει μεγάλο κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».

1.1 Αντικείμενο Μελέτης

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 είναι υποχρεωμένος να διενεργεί, πριν από κάθε επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων είναι μια διαδικασία που βοηθά τους οργανισμούς να εντοπίζουν και να μετριάζουν τους κινδύνους προστασίας δεδομένων διαφόρων δραστηριοτήτων μέσα στον ίδιο τον οργανισμό. Ο υπεύθυνος επεξεργασίας πρέπει να συμβουλεύεται τον υπεύθυνο προστασίας δεδομένων (αν έχει οριστεί)

[1] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

και, κατά περίπτωση, τα υποκείμενα των δεδομένων και ειδικούς εμπειρογνώμονες. Οι εκτελούντες την επεξεργασία μπορεί επίσης να συμβάλουν.

Πιο συγκεκριμένα, η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων είναι μια διαδικασία που έχει σκοπό να προσδιορίσει και να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητά της και να βοηθήσει στη διαχείριση των κινδύνων που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Αυτό μπορεί να πραγματοποιηθεί με την αξιολόγηση και τον καθορισμό των μέτρων για την αντιμετώπιση των κινδύνων. Η ΕΑΠΔ εμπεριέχει την πλήρωση της υποχρέωσης λογοδοσίας, η οποία επίσης εισάγεται με το ΓΚΠΔ, καθώς υποχρεώνει τους υπεύθυνους επεξεργασίας να συμμορφώνονται με τις προδιαγραφές του ΓΚΠΔ, αλλά και να αποδεικνύουν ότι έχουν λάβει τα απαραίτητα μέτρα για τη διασφάλιση της συμμόρφωσης με τον Κανονισμό. Θα λέγαμε λοιπόν ότι η ΕΑΠΔ είναι μια διαδικασία εμπέδωσης και απόδειξης της συμμόρφωσης. Βάσει του κανονισμού, η μη συμμόρφωση με τις απαιτήσεις ΕΑΠΔ μπορεί να οδηγήσει στην επιβολή κυρώσεων – συμπεριλαμβανομένων των προστίμων - από την εκάστοτε αρμόδια εποπτική αρχή.

1.1.1 Ερευνητικά ερωτήματα

Η αποτελεσματική εκπόνηση μιας εκτίμησης αντικτύπου, στο πλαίσιο όχι μόνο της συμμόρφωσης με τις επιταγές της νομοθεσίας αλλά και για την αποτελεσματική προστασία του θεμελιώδους δικαιώματος των προσωπικών δεδομένων, εμφανίζει διάφορες ερευνητικές προκλήσεις λόγω του ότι αποτελεί μία καινούρια έννοια που υπεισέρχεται πλέον ως νομική υποχρέωση. Παρόλο που ανέκαθεν αποτελούσε ένα σημαντικό εργαλείο ενίσχυσης της ιδιωτικότητας, δεν είχαν υιοθετηθεί συγκεκριμένες μεθοδολογίες και πρακτικές για την εκπόνησή της: παρόλο που υπάρχουν σχετικές μεθοδολογίες για τη διαχείριση κινδύνων ασφάλειας πληροφοριών, η ΕΑΠΔ αποτελεί μία ευρύτερη διαδικασία, υπό την έννοια ότι δεν εξετάζει μόνο θέματα ασφάλειας προσωπικών δεδομένων αλλά και θέματα που άπτονται, π.χ., του πώς ικανοποιούνται τα δικαιώματα των προσώπων των οποίων τα δεδομένα υφίστανται επεξεργασία ή του αν συλλέγονται υπέρμετρα προσωπικά δεδομένα σε σχέση με τους επιδιωκόμενους σκοπούς.

Βάσει των ανωτέρω, η παρούσα μεταπτυχιακή εργασία θα μελετήσει το θέμα εκπόνησης ΕΑΠΔ σε πραγματικό περιβάλλον, επιλέγοντας συγκεκριμένη επεξεργασία δεδομένων, για ερευνητικούς σκοπούς, που πραγματοποιεί ένας οργανισμός. Δεδομένου ότι η επεξεργασία για ερευνητικούς σκοπούς είναι μία συνήθης επεξεργασία, η εκπόνηση μίας τέτοιου τύπου εκτίμησης αντικτύπου μπορεί να αποτελέσει οδηγό για πολλούς οργανισμούς οι οποίοι δραστηριοποιούνται στο χώρο της έρευνας. Στο πλαίσιο αυτό, σκοπός είναι να αναγνωριστούν οι κίνδυνοι όχι μόνο της

ασφάλειας αλλά και της προσβολής της ιδιωτικότητας αναπτύσσοντας μια μεθοδολογία εκπόνησης ΕΑΠΔ, βάσει γνωστών τεχνικών από τη βιβλιογραφία, η οποία και θα πραγματοποιηθεί για τη συγκεκριμένη επεξεργασία. Παράλληλα σκοπός είναι να αξιοποιηθεί, στο πλαίσιο μίας συστηματικής εκπόνησης ΕΑΠΔ, κάποια γνωστή μεθοδολογία διαχείρισης κινδύνων ασφάλειας: για το σκοπό αυτό, εστιάζουμε στη γνωστή μεθοδολογία ISO 27005 προκειμένου να μελετηθεί ο βαθμός στον οποίο μια τέτοια μεθοδολογία μπορεί να ενσωματωθεί σε μια ΕΑΠΔ συνεισφέροντας σε αυτή ως προς το τμήμα των κινδύνων ασφάλειας. Είναι σημαντικό να αναφερθεί ότι καθώς πολλοί οργανισμοί χρησιμοποιούν την μεθοδολογία κατά ISO για να πραγματοποιήσουν εξονυχιστικά διαχείριση κινδύνων, η εκπόνηση μιας ΕΑΠΔ μπορεί από τη μια πλευρά να θεωρηθεί μια σημαντική διαδικασία που θα αποτελεί συνέχεια για τον κάθε οργανισμό.

Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων θα περιγραφεί αναφορικά με τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, αξιολογώντας την αναγκαιότητα, την αναλογικότητα και τα μέτρα συμμόρφωσης, με σκοπό να εντοπίσει και να αξιολογήσει τους κινδύνους και να προσδιορίσει τυχόν πρόσθετα μέτρα για τον μετριασμό των εν λόγω κινδύνων. Για να αξιολογηθεί το επίπεδο κινδύνου, θα εξεταστεί τόσο η πιθανότητα όσο και η σοβαρότητα των επιπτώσεων.

1.2 Οργάνωση Μεταπτυχιακής Διατριβής

Η ανάπτυξη της παρούσας μεταπτυχιακής διατριβής γίνεται σε 6 κεφάλαια, όπου στο 1ο κεφάλαιο γίνεται αναφορά στο σκοπό και το αντικείμενο της παρούσας μελέτης. Στο 2ο Κεφάλαιο παρουσιάζεται το θεωρητικό υπόβαθρο που σχετίζεται με τον ΓΚΠΔ και τα νομικά πλαίσια που σχετίζονται με τον ορισμό, τη θέση και τα καθήκοντα του υπεύθυνου προστασίας δεδομένων αλλά και τη νομιμότητα της επεξεργασίας και τις αρχές που διέπουν την επεξεργασία. Στο 3ο κεφάλαιο διατυπώνεται μια γενική προσέγγιση μεθοδολογίας η οποία αποτελείται από κατάλληλες δραστηριότητες, ώστε η εκτίμηση των επιπτώσεων σχετικά με τη προστασία των δεδομένων να εκτελείται με όσον το δυνατόν περισσότερη σαφήνεια και μεθοδικότητα. Στη συνέχεια αναφέρεται ρητώς το κόστος εφαρμογής, τα οφέλη η μεθοδολογία διενέργειας ΕΑΠΔ αλλά και τα βήματα και τα κριτήρια που απαιτούνται για διενέργεια ΕΑΠΔ. Στο 4ο κεφάλαιο περιγράφεται η μελέτη περίπτωσης ενός οργανισμού αποτυπώνοντας τα υπό εξέταση αγαθά, συστήματα, υπηρεσίες και δεδομένα, η κατηγοριοποίηση, η περιγραφή και η μελέτη των εκάστοτε προαναφερθέντων αγαθών, ως προς τις απαιτήσεις εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, καθώς και ως προς τις απαιτήσεις ιδιωτικότητας για την υπό μελέτη περίπτωση. Επιπλέον γίνεται αποτίμηση επιπτώσεων ασφάλειας καθώς και απειλών-αδυναμιών για κάθε

αγαθό, καταγραφή των μέτρων ασφάλειας που μπορούν να ληφθούν. Στο 5ο κεφάλαιο μελετάται και αναπτύσσεται μια μεθοδολογία DPIA στο περιβάλλον του υπό μελέτη οργανισμού η οποία ενσωματώνεται στα προαναφερόμενα βήματα που αφορούν την διαχείριση κινδύνων. Στο 6ο και τελευταίο κεφάλαιο συνοψίζονται τα αποτελέσματα της μεταπτυχιακής διατριβής και περιγράφονται τα συμπεράσματα από την εκπόνηση της.

Κεφάλαιο 2
Θεωρητικό Υπόβαθρο

Στο παρόν κεφάλαιο παρουσιάζεται το θεωρητικό υπόβαθρο που σχετίζεται με τον ΓΚΠΔ και τα υπόλοιπα κανονιστικά πλαίσια για την αλλά και τις μεθοδολογίες που ακολουθούνται για να μπορέσει να λειτουργήσει η ΕΑΠΔ ως ακρογωνιαίος λίθος για την ενσωμάτωσή της σε μια κλασική μεθοδολογία διαχείρισης κινδύνων.

2.1 Νομικό Πλαίσιο

Στην ενότητα αυτή παρουσιάζεται το Νομικό πλαίσιο όπως διαμορφώνεται από τον Γενικό Κανονισμό Προσωπικών Δεδομένων και αναφέρεται στην εκτίμηση αντικτύπου, στην επεξεργασία δεδομένων, στους υπεύθυνους επεξεργασίας και στους εκτελούντες την επεξεργασία και τα καθήκοντα τους.

2.1.1 Άρθρο 4 – Βασικοί Ορισμοί στα πλαίσια του ΓΚΠΔ

Το άρθρο 4 του ΓΚΠΔ [1] περιλαμβάνει ένα κατάλογο με ορισμούς που χρησιμοποιούνται στον Κανονισμό. Στα πλαίσια της παρούσας μεταπτυχιακής διατριβής διατυπώνονται οι παρακάτω ορισμοί διότι θα αναφέρονται εκτενώς στη συνέχεια και θα πρέπει να υπάρχει εξοικείωση με αυτούς:

1. **Δεδομένα προσωπικού χαρακτήρα**: 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

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

3. **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.

4. **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.

2.1.2 Άρθρο 5 – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Το άρθρο 5 του ΓΚΠΔ [1] αναφέρεται σε κάποιες αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και αυτές αναφέρονται ως:

1. Τα δεδομένα προσωπικού χαρακτήρα:

   α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»),

   β) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»),

γ) είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»),

δ) 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»),

ε) 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»),

στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

2. Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»).

2.1.3 Άρθρο 6 – Νομιμότητα της επεξεργασίας

Στο άρθρο 6 αναφέρονται τα παρακάτω που αφορούν τη νομιμότητα της επεξεργασίας:

1. Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

   α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί. Πρέπει να αναφερθεί ότι δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

2. Τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν πιο ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού όσον αφορά την επεξεργασία για τη συμμόρφωση με την παράγραφο 1 στοιχεία γ) και ε), καθορίζοντας ακριβέστερα ειδικές απαιτήσεις για την επεξεργασία και άλλα μέτρα προς εξασφάλιση σύννομης και θεμιτής επεξεργασίας, μεταξύ άλλων για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX του ΓΚΠΔ.

3. Η βάση για την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχεία γ) και ε) ορίζεται σύμφωνα με:

α) το δίκαιο της Ένωσης, ή

β) το δίκαιο του κράτους μέλος στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας.

Ο σκοπός της επεξεργασίας καθορίζεται στην εν λόγω νομική βάση ή, όσον αφορά την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχείο ε), είναι η αναγκαιότητα της επεξεργασίας για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Η εν λόγω νομική βάση μπορεί να περιλαμβάνει ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού, μεταξύ άλλων: τις γενικές προϋποθέσεις που διέπουν τη σύννομη επεξεργασία από τον υπεύθυνο επεξεργασίας· τα είδη των δεδομένων που υποβάλλονται σε επεξεργασία· τα οικεία υποκείμενα των δεδομένων· τις οντότητες στις οποίες μπορούν να κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα και τους σκοπούς αυτής της κοινοποίησης· τον περιορισμό του σκοπού· τις περιόδους αποθήκευσης· και τις πράξεις επεξεργασίας και τις διαδικασίες επεξεργασίας, συμπεριλαμβανομένων των μέτρων για τη διασφάλιση σύννομης και θεμιτής επεξεργασίας, όπως εκείνα για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX. Το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους ανταποκρίνεται σε σκοπό δημόσιου συμφέροντος και είναι ανάλογο προς τον επιδιωκόμενο νόμιμο σκοπό.

4. Όταν η επεξεργασία για σκοπό άλλο από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των σκοπών που αναφέρονται στο άρθρο 23 παράγραφος 1, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων:

   α) τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας,

   β) το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας,

   γ) τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 9, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με

ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10,

δ) τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων,

ε) την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.

2.1.4 Άρθρο 9 – Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα

Στα πλαίσια της παρούσας μεταπτυχιακής διατριβής θα πρέπει εκτός των άλλων να αναφερθούν τα δεδομένα ειδικών κατηγοριών του ΓΚΠΔ και πιο συγκεκριμένα η παράγραφος 1 του άρθρου 9 [1] αναφορικά με την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα:

Απαγορεύεται η 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.

2.1.5 Άρθρο 35 – Εκτίμηση αντικτύπου σχετικά με την Προστασία Δεδομένων

Σύμφωνα με το άρθρο 35 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ) [1] στο οποίο αναφέρεται η εκτίμηση αντικτύπου προστασίας δεδομένων, περιγράφονται τα παρακάτω:

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. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

1. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων (όπως αυτός περιγράφεται στη συνέχεια), εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

2. Η ανωτέρω αναφερόμενη εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

   α) συστηματικής και εκτενούς αξιολόγησης 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,

   β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 του ΓΚΔΠ (δηλαδή για τα λεγόμενα «ευαίσθητα» προσωπικά δεδομένα) ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 του ΓΚΠΔ ή

   γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

3. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68 του ΓΚΠΔ.

4. Η εκτίμηση αντικτύπου περιέχει τουλάχιστον:

   α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

   β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

   γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και

δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα Κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

5. Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας που αναφέρονται στο άρθρο 40 του ΓΚΠΔ από τους σχετικούς υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας που εκτελούνται από τους εν λόγω υπευθύνους ή εκτελούντες την επεξεργασία, ιδίως για τους σκοπούς εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

6. Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας.

7. Όταν η επεξεργασία δυνάμει του άρθρου 6 παράγραφος 1 στοιχείο γ) ή ε) του ΓΚΠΔ (δηλαδή περιπτώσεις στις οποίες η επεξεργασία πραγματοποιείται γιατί υπάρχει κάποια σχετική νομική πρόβλεψη) έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το εν λόγω δίκαιο ρυθμίζει την εκάστοτε συγκεκριμένη πράξη επεξεργασίας ή σειρά πράξεων και έχει διενεργηθεί ήδη εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο της έγκρισης της εν λόγω νομικής βάσης, οι παράγραφοι 1 έως 7 δεν εφαρμόζονται, εκτός εάν τα κράτη μέλη κρίνουν απαραίτητη τη διενέργεια της εν λόγω εκτίμησης πριν από τις δραστηριότητες επεξεργασίας.

8. Όπου απαιτείται, ο υπεύθυνος επεξεργασίας προβαίνει σε επανεξέταση για να εκτιμήσει εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διενεργείται σύμφωνα με την εκτίμηση αντικτύπου στην προστασία δεδομένων τουλάχιστον όταν μεταβάλλεται ο κίνδυνος που θέτουν οι πράξεις επεξεργασίας.

Συνοψίζοντας, ο ΓΚΠΔ περιγράφει ότι δεν απαιτείται η διενέργεια ΕΑΠΔ σε κάθε πράξη επεξεργασίας αλλά απαιτείται μόνον όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (άρθρο 35 παράγραφος

1). Αυτό όμως δεν σημαίνει ότι ο υπεύθυνος επεξεργασίας δεν μπορεί, ακόμα και στις περιπτώσεις όπου δεν προκύπτει ρητή υποχρέωση, να διενεργήσει ΕΑΠΔ εφαρμόζοντας μέτρα για την ενδεδειγμένη διαχείριση κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Επιπλέον ο υπεύθυνος επεξεργασίας πρέπει να αξιολογεί συνεχώς τους κινδύνους που απορρέουν από τις δραστηριότητες επεξεργασίας του, για να εξακριβώνει πότε ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο.

Σε κάθε περίπτωση, εάν ο υπεύθυνος επεξεργασίας εκπονήσει μία ΕΑΠΔ και κρίνει ότι κάποιοι κίνδυνοι για τα θεμελιώδη δικαιώματα των φυσικών προσώπων τα οποία αφορά η επεξεργασία δεν έχουν αντιμετωπιστεί επαρκώς, θα πρέπει να επικοινωνήσει με την αρμόδια εποπτική αρχή (ήτοι την οικεία ανεξάρτητη Αρχή Προστασίας Προσωπικών Δεδομένων), ζητώντας τη γνώμη της: η διαδικασία αυτή λέγεται «προηγούμενη διαβούλευση» με την εποπτική αρχή και προβλέπεται στο άρ. 36 του ΓΚΠΔ.

2.1.6 Άρθρο 37 – Ορισμός του υπευθύνου προστασίας δεδομένων

1. Όπως αναφέρθηκε και προηγουμένως, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν Υπεύθυνο Προστασίας Δεδομένων (DPO) [1] σε κάθε περίπτωση στην οποία:

   α) Η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας.

   β) Οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα.

   γ) Οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

2. Όμιλος επιχειρήσεων μπορεί να διορίσει **ένα μόνο υπεύθυνο προστασίας δεδομένων**, υπό την προϋπόθεση ότι κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων.

3. Εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσια αρχή ή δημόσιος φορέας, ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές τέτοιες αρχές ή πολλούς τέτοιους φορείς, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους.

4. Σε περιπτώσεις πλην των αναφερόμενων παραπάνω, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να ορίζουν υπεύθυνο προστασίας δεδομένων ή, όπου απαιτείται από το δίκαιο της Ένωσης ή του κράτους μέλους, ορίζουν υπεύθυνο προστασίας δεδομένων. Ο υπεύθυνος προστασίας δεδομένων μπορεί να ενεργεί για τις εν λόγω ενώσεις και τους άλλους φορείς που εκπροσωπούν υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία.

5. Ο υπεύθυνος προστασίας δεδομένων διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39.

6. Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών.

7. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δημοσιεύουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και τα ανακοινώνουν στην εποπτική αρχή.

2.1.7 Άρθρο 38 – Θέση του υπευθύνου προστασίας δεδομένων

Η θέση του υπεύθυνου προστασίας δεδομένων είναι η παρακάτω [1]:

1. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.

2. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία στηρίζουν τον υπεύθυνο προστασίας δεδομένων στην άσκηση των καθηκόντων που αναφέρονται στο άρθρο 39 του

ΓΚΠΔ παρέχοντας απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του.

3. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζει ότι ο υπεύθυνος προστασίας δεδομένων δεν λαμβάνει εντολές για την άσκηση των εν λόγω καθηκόντων. Δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του. Ο υπεύθυνος προστασίας δεδομένων λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

4. Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους δυνάμει του παρόντος κανονισμού.

5. Ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους.

6. Ο υπεύθυνος επεξεργασίας μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζουν ότι τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων.

2.1.8 Άρθρο 39 – Καθήκοντα του υπευθύνου προστασίας δεδομένων

Ο υπεύθυνος προστασίας δεδομένων έχει τα ακόλουθα καθήκοντα που πρέπει να πληροί [1]:

1. Ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα Κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων.

2. Παρακολουθεί τη συμμόρφωση με τον παρόντα Κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της

ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων.

3. Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35.

4. Συνεργάζεται με την εποπτική αρχή.

5. Ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

Κατά την εκτέλεση των καθηκόντων του, ο υπεύθυνος προστασίας δεδομένων λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

Κεφάλαιο 3

Εκτίμηση αντικτύπου ως προς την προστασία προσωπικών δεδομένων – ΕΑΠΔ

Στο κεφάλαιο αυτό διατυπώνεται μια γενική προσέγγιση μεθοδολογίας η οποία αποτελείται από κατάλληλες δραστηριότητες, ώστε η εκτίμηση των επιπτώσεων σχετικά με τη προστασία των δεδομένων να εκτελείται με όσον το δυνατόν περισσότερη σαφήνεια και μεθοδικότητα. Στη συνέχεια αναφέρεται ρητώς το περιεχόμενο της υποχρέωσης διενέργειας ΕΑΠΔ αλλά και της απόφασης διενέργειας ΕΑΠΔ. Επιπλέον, αναφέρονται οι βέλτιστες πρακτικές που μπορούν να ακολουθηθούν, ώστε να επιτευχθεί ο σκοπός μιας ΕΑΠΔ.

2.1 Πράξεις επεξεργασίας που υπόκεινται σε απαίτηση ΕΑΠΔ

Ο κατάλογος ομαδοποιεί και εξειδικεύει περαιτέρω τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια ΕΑΠΔ με παράθεση και ενδεικτικών παραδειγμάτων. Τα κριτήρια για την διενέργεια ΕΑΠΔ, σύμφωνα με την ελληνική Αρχή Προστασίας Δεδομένων[3], ομαδοποιούνται στις παρακάτω τρεις κατηγορίες :

1. **1η κατηγορία:** με βάση τα είδη και τους σκοπούς επεξεργασίας.

α) Συστηματική αξιολόγηση, βαθμολόγηση, πρόβλεψη, πρόγνωση και κατάρτιση προφίλ, ιδίως πτυχών που αφορούν την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή τις κινήσεις ή την πιστοληπτική ικανότητα των υποκειμένων των δεδομένων.

β) Συστηματική επεξεργασία δεδομένων που αποσκοπεί στη λήψη αυτοματοποιημένων αποφάσεων, οι οποίες παράγουν έννομα αποτελέσματα σχετικά με τα υποκείμενα των δεδομένων ή επηρεάζουν σημαντικά τα υποκείμενα των δεδομένων κατά ανάλογο τρόπο και μπορούν να οδηγήσουν σε αποκλεισμό ή διακρίσεις σε βάρος του φυσικού προσώπου.

γ) Συστηματική επεξεργασία δεδομένων που ενδέχεται να εμποδίζει το υποκείμενο να ασκήσει τα δικαιώματά του ή να χρησιμοποιήσει μια υπηρεσία ή σύμβαση, ιδίως όταν λαμβάνονται υπόψη δεδομένα που συλλέγονται από τρίτους.

δ) Συστηματική επεξεργασία δεδομένων που αφορά την κατάρτιση προφίλ για το σκοπό της προώθησης προϊόντων και υπηρεσιών εφόσον τα δεδομένα συνδυάζονται με δεδομένα που συλλέγονται από τρίτους.

ε) Συστηματική και σε μεγάλη κλίμακα επεξεργασία για την παρακολούθηση, την παρατήρηση ή τον έλεγχο των φυσικών προσώπων με χρήση δεδομένων που συλλέγονται μέσω συστημάτων βιντεοεπιτήρησης ή μέσω δικτύων ή με οποιοδήποτε άλλο μέσο σε δημόσιο χώρο, δημοσίως προσβάσιμο χώρο ή ιδιωτικό χώρο προσιτό σε απεριόριστο αριθμό προσώπων. Περιλαμβάνει την παρακολούθηση των κινήσεων ή της τοποθεσίας/γεωγραφικής θέσης σε πραγματικό ή μη χρόνο ταυτοποιημένων ή ταυτοποιήσιμων φυσικών προσώπων.

στ) Μεγάλης κλίμακας συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία και τη δημόσια υγεία για σκοπούς δημοσίου συμφέροντος, όπως η εισαγωγή και χρήση συστημάτων ηλεκτρονικής συνταγογράφησης και η εισαγωγή και χρήση ηλεκτρονικού φακέλου ή ηλεκτρονικής κάρτας υγείας.

ζ) Μεγάλης κλίμακας συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό την εισαγωγή, οργάνωση, παροχή και έλεγχο της χρήσης υπηρεσιών ηλεκτρονικής διακυβέρνησης, όπως ορίζονται στο άρθρο 3 του ν.3979/2011 όπως ισχύει.

2. **2η κατηγορία**: με βάση το είδος των δεδομένων και/ή τις κατηγορίες των υποκειμένων.

α) Μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων (περιλαμβανομένων των γενετικών και των βιομετρικών με σκοπό την αδιαμφισβήτητη ταυτοποίηση

προσώπου) που αναφέρονται στο άρθρο 9 παρ. 1 και των δεδομένων που αναφέρονται στο άρθρο 10 του ΓΚΠΔ.

β) Συστηματική και σε μεγάλη κλίμακα επεξεργασία δεδομένων ιδιαίτερης σημασίας ή εξαιρετικού χαρακτήρα όπως

i. δεδομένα κοινωνικής πρόνοιας (δεδομένα σχετικά με τη φτώχεια, την ανεργία, την κοινωνική εργασία κλπ.),

ii. δεδομένα ηλεκτρονικών επικοινωνιών, περιλαμβανομένων των δεδομένων περιεχομένου όπως του ηλεκτρονικού ταχυδρομείου, μεταδεδομένων και των δεδομένων γεωγραφικής θέσης/τοποθεσίας, με εξαίρεση την καταγραφή τηλεφωνικών συνδιαλέξεων σύμφωνα με το άρθρο 4 παρ. 3 του ν.3471/2006,

iii. δεδομένα που αφορούν εθνικό αριθμό ταυτότητας ή άλλο αναγνωριστικό στοιχείο ταυτότητας γενικής εφαρμογής ή αλλαγή των προϋποθέσεων και όρων επεξεργασίας και χρήσης αυτών και των συναφών με αυτά δεδομένων προσωπικού χαρακτήρα,

iv. δεδομένα που περιλαμβάνονται σε προσωπικά έγγραφα, ημερολόγια, σημειώσεις από ηλεκτρονικό αναγνώστη (e-reader) και σε εφαρμογές καταγραφής βίου (life logging), που προσφέρουν δυνατότητες τήρησης σημειώσεων και πολύ προσωπικών πληροφοριών,

v. δεδομένα που συλλέγονται ή παράγονται από συσκευές (όπως αυτές με αισθητήρες) ιδίως μέσω των εφαρμογών του 'διαδικτύου των πραγμάτων - IoT (όπως έξυπνες τηλεοράσεις, έξυπνες οικιακές συσκευές, συνδεδεμένα παιχνίδια, έξυπνες πόλεις, έξυπνοι μετρητές ενέργειας κλπ.) και/ή με τη χρήση άλλων μέσων.

γ) Συστηματική παρακολούθηση – εφόσον είναι επιτρεπτή – της θέσης/τοποθεσίας καθώς και του περιεχομένου και των μεταδεδομένων των επικοινωνιών των εργαζομένων με εξαίρεση τα αρχεία καταγραφής για λόγους ασφάλειας εφόσον η επεξεργασία περιορίζεται στα απολύτως απαραίτητα δεδομένα και είναι ειδικά τεκμηριωμένη. Σχετικό παράδειγμα που εμπίπτει στην υποχρέωση διενέργειας ΕΑΠΔ αποτελεί η χρήση συστημάτων DLP. Συστηματική επεξεργασία βιομετρικών δεδομένων των εργαζομένων με σκοπό την

αδιαμφισβήτητη ταυτοποίηση προσώπου καθώς και γενετικών δεδομένων των εργαζομένων.

3. **3η κατηγορία**: με βάση τα πρόσθετα χαρακτηριστικά και/ή τα χρησιμοποιούμενα μέσα της επεξεργασίας.

α) Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογιών ή οργανωτικών λύσεων, οι οποίες μπορεί να περιλαμβάνουν νέες μορφές συλλογής και χρήσης δεδομένων, με ενδεχόμενο υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων όπως η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης, ή εφαρμογές mhealth ή άλλες «έξυπνες» εφαρμογές, από τις οποίες δημιουργείται προφίλ των χρηστών (π.χ. καθημερινές συνήθειες), ή εφαρμογές τεχνητής νοημοσύνης ή τεχνολογίες δημόσια προσπελάσιμων blockchain που περιλαμβάνουν προσωπικά δεδομένα.

β) Συνδυασμό και/ή συσχέτιση προσωπικών δεδομένων από πολλαπλές πηγές ή τρίτους, από δύο ή περισσότερες πράξεις επεξεργασίας που υλοποιούνται για διαφορετικούς σκοπούς ή/και από διαφορετικούς υπευθύνους επεξεργασίας με τρόπο που θα μπορούσε να υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων.

γ) Σε περίπτωση που η επεξεργασία αφορά δεδομένα, τα οποία δεν έχουν συλλεγεί από το υποκείμενο και η ενημέρωση των υποκειμένων σύμφωνα με το άρθρο 14 ΓΚΠΔ αποδεικνύεται αδύνατη ή θα προϋπέθετε δυσανάλογη προσπάθεια ή είναι πιθανό να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της επεξεργασίας.

Η διενέργεια ΕΑΠΔ κρίνεται υποχρεωτική όταν πληρούται τουλάχιστον ένα από τα κριτήρια της 1ης ή της 2ης κατηγορίας. Είναι επίσης υποχρεωτική όταν συντρέχει ένα τουλάχιστον κριτήριο ως προς την 3η κατηγορία και η επεξεργασία αφορά είδη και σκοπούς επεξεργασίας της 1ης κατηγορίας, ή/και είδη δεδομένων ή/και κατηγορίες υποκειμένων της 2ης κατηγορίας.

2.2 Εκτέλεση της εκτίμησης των επιπτώσεων σχετικά με την προστασία των δεδομένων

Για να μπορέσει να εφαρμοστεί η ΕΑΠΔ σε ένα πληροφοριακό σύστημα, θα πρέπει να ακολουθείται μια μεθοδολογία η οποία αποτελείται από κατάλληλες δραστηριότητες, ώστε η εκτίμηση των επιπτώσεων σχετικά με τη προστασία των δεδομένων να εκτελείται με όσον το δυνατόν περισσότερη σαφήνεια και μεθοδικότητα. Τα βήματα που πρέπει να ακολουθούνται είναι τα παρακάτω:

1. καθορισμός της ανάγκης για την διενέργεια της ΕΑΠΔ

2. προσδιορισμός της ομάδας που θα εκτελέσει την ΕΑΠΔ

3. αναγνώριση και περιγραφή του σχεδιασμού της εφαρμογής και των διαδικασιών που ακολουθούνται μεταξύ των εμπλεκόμενων χρηστών

4. συνεργασία με τους τους εμπλεκόμενους φορείς εντός και εκτός οργανισμού αναφέροντας τους πιθανούς κινδύνους

5. αναγνώριση των πιθανών κινδύνων αναφορικά με τα προσωπικά δεδομένα των χρηστών

6. διαχείριση των κινδύνων αλλά και λήψη μέτρων αντιμετώπισης και ασφάλειας

7. έλεγχος συμμόρφωσης με το νόμο

8. διατύπωση συστάσεων

9. προετοιμασία και δημοσίευση της έκθεσης

10. Εφαρμογή των συστάσεων

11. Εξωτερική επισκόπηση και έλεγχος

Κάθε επεξεργασία δεδομένων εντός μιας εταιρείας ή οποιοδήποτε οργανισμού θα πρέπει να συμμορφώνεται με τις απαιτήσεις προστασίας δεδομένων. Σύμφωνα με τον ΓΚΠΔ η εκτίμηση των επιπτώσεων για την προστασία δεδομένων αποτελεί σημαντικό στοιχείο και πιο συγκεκριμένα διευκρινίζεται η ασφάλεια στην επεξεργασία αλλά και η αξιολόγηση των επιπτώσεων στην προστασία δεδομένων. Σε πολλές εταιρείες, τα μέτρα που πρέπει να εφαρμοστούν έχουν ήδη αξιολογηθεί όσον αφορά τις πτυχές που σχετίζονται με τον κίνδυνο - συχνά σε συμφωνία με την

ασφάλεια των πληροφοριών σύστημα διαχείρισης (ISMS). Όπως έχει ήδη καθιερωθεί σε πολλές εταιρείες, μπορεί να γίνει διάκριση μεταξύ βασικής ασφάλειας πληροφοριών, η οποία βασικά ισχύει για όλες τις διαδικασίες και εισαγωγή ειδικών μέτρων για την διαδικασία επεξεργασίας πληροφοριών. Εδώ θα πρέπει να αναφέρουμε ότι η αξιολόγηση αντίκτυπου για την προστασία των δεδομένων (άρθρο 35 του ΓΚΠΔ) είναι το αντίστοιχο της προηγούμενης οδηγίας (άρθρο 20 της οδηγίας 95/46 / ΕΚ).

Μια σημαντική καινοτομία που επιφέρει ο ΓΚΠΔ [4], συνίσταται στην καταρχήν κατάργηση της γενικής υποχρέωσης γνωστοποίησης προς την αρχή ελέγχου (εκάστοτε αρμόδια ΑΠΔΠΧ) της επεξεργασίας, που προέβλεπε η Οδηγία 95/46/ΕΚ5 και η οποία βάρυνε τους υπευθύνους επεξεργασίας, και στην αντικατάστασή της από άλλες υποχρεώσεις, όπως:

1. αφενός, από την υποχρέωση για τους υπευθύνους επεξεργασίας να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας, για τις οποίες είναι υπεύθυνοι, καθώς και την υποχρέωση για τους εκτελούντες την επεξεργασία να τηρούν αρχεία όλων των κατηγοριών δραστηριοτήτων επεξεργασίας, που διεξάγονται για λογαριασμό υπευθύνου επεξεργασίας,

2. αφετέρου, από την υποχρέωση για τους υπευθύνους επεξεργασίας να διενεργούν ΕΑΠΔ σχετικά με την προστασία δεδομένων σε συγκεκριμένες κατηγορίες επεξεργασιών.

Η κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προς τις ΑΠΔΠΧ δικαιολογήθηκε από τη διαπίστωση ότι η υποχρέωση αυτή -παρά το ότι επιφέρει στις αρχές ελέγχου και, ιδίως, στους υπευθύνους επεξεργασίας διοικητικό και οικονομικό φόρτο- δεν συνέβαλε σε όλες τις περιπτώσεις στη βελτίωση της προστασίας των δεδομένων προσωπικού χαρακτήρα. Προκρίθηκε, συνεπώς, η αντικατάσταση αυτής της γενικής υποχρέωσης γνωστοποίησης από «αποτελεσματικές διαδικασίες και μηχανισμούς που επικεντρώνονται σε εκείνους τους τύπους πράξεων επεξεργασίας που ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους». Ως «τύποι πράξεων» επεξεργασίας, από τους οποίους ενδέχεται να προκύψουν κίνδυνοι για τα υποκείμενα των δεδομένων, χαρακτηρίζονται, ιδίως, εκείνοι που περιλαμβάνουν τη χρήση νέων τεχνολογιών ή είναι νέου τύπου και δεν έχει διενεργηθεί προηγούμενη εκτίμηση αντικτύπου ως προς την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας ή παρίσταται αναγκαία η αξιολόγησή τους, λόγω του χρόνου που έχει παρέλθει από την αρχική επεξεργασία. Στο πλαίσιο

αυτό, η ρητή θέσπιση υποχρέωσης διενέργειας ΕΑΠΔ παρίσταται, καταρχάς, ως ένα αντιστάθμισμα στην κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας, με σκοπό την αντιμετώπιση των υψηλών κινδύνων, που ενδέχεται να προκύψουν για τα υποκείμενα των δεδομένων από συγκεκριμένες κατηγορίες επεξεργασιών, λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους. Ωστόσο, η υποχρέωση διενέργειας ΕΑΠΔ θεσπίζεται -κατά τρόπο γενικότερο και σαφώς ουσιαστικότερο- στο ΓΚΔΠ κυρίως ως ένα μέτρο ενίσχυσης της συμμόρφωσης προς τις διατάξεις του, λαμβανομένης πάντοτε υπόψη της ανάγκης αντιμετώπισης των υψηλών κινδύνων, που ενδέχεται να προκύψουν για τα υποκείμενα των δεδομένων από συγκεκριμένες κατηγορίες επεξεργασιών, λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους. Υπό την έννοια αυτή η υποχρέωση διενέργειας ΕΑΠΔ σημαίνει ότι ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να αξιολογήσει όλες τις παραμέτρους των κρίσιμων πράξεων επεξεργασίας πριν από την έναρξή τους, προκειμένου να διασφαλίσει την αποτελεσματική προστασία των υποκειμένων. Επιπλέον, εάν απαιτείται από τις περιστάσεις, ο υπεύθυνος επεξεργασίας υποχρεούται να πραγματοποιεί σχετικά διαβούλευση με την αρμόδια ΑΠΔΠΧ, πριν από την έναρξη της επεξεργασίας. Συνακόλουθα, η υποχρέωση διενέργειας ΕΑΠΔ σημαίνει, επίσης, ότι πρόκειται για ένα μέτρο, το οποίο είναι πλήρως ενταγμένο στην ανάγκη προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ' ορισμού (data protection by design / data protection by default), σύμφωνα με τα οριζόμενα στις διατάξεις του άρθρου 25 του ΓΚΠΔ.

2.3 Το κόστος εφαρμογής της ΕΑΠΔ

Η υποχρέωση των εκτελούντων της επεξεργασίας προσωπικών δεδομένων να διενεργούν εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων, όπου η επεξεργασία φαίνεται να παρουσιάζει κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων, επιφέρει ένα επιπλέον κόστος για τον εκάστοτε οργανισμό, με την έννοια ότι χρειάζεται πόρους για να εκτελέσει την εν λόγω εκτίμηση. Η εκτίμηση του πιθανού κόστους της ΕΑΠΔ εξαρτάται από έναν σημαντικό αριθμό παραγόντων. Το μέγεθος και η αυστηρότητα της ΕΑΠΔ θα εξαρτηθούν κυρίως από το πώς ο οργανισμός αντιλαμβάνεται τους κινδύνους αλλά και τη σοβαρότητα με την οποία τους αντιμετωπίζει. Η εκτίμηση του πιθανού κόστους της ΕΑΠΔ εξαρτάται από τους ενδεικτικά κάτωθι συναφείς παράγοντες [6]:

α) μέγεθος της εκτίμησης,

β) αυστηρότητα της νομοθεσίας,

γ) συμμετοχή των εμπλεκόμενων μερών,

δ) πρόσληψη ειδικού στελέχους για την εκτέλεση της εκτίμησης.

Προσθέτοντας όλες τις παραπάνω πιθανές δαπάνες γίνεται κατανοητό πως η ΕΑΠΔ αποτελεί μια διαδικασία που ενδεχομένως να κοστίζει αρκετά. Το ζήτημα που εγείρεται είναι αν το όφελος από την ΕΑΠΔ όντως καλύπτει το κόστος της, κάτι που μπορεί να εξακριβωθεί από μια ανάλυση κόστους-οφέλους, λαμβάνοντας όμως υπόψη και επιπλέον ποιοτικούς παράγοντες. Σε κάθε περίπτωση όμως, εάν η εκπόνησή της είναι υποχρεωτική, τυχόν μη εκπόνησή της δεν μπορεί να δικαιολογηθεί ούτε για λόγους κόστους.

2.4 Οφέλη από την εκτέλεση της ΕΑΠΔ

Από την εκτέλεση και την ολοκλήρωση της εκτίμησης των επιπτώσεων σχετικά με την προστασία των προσωπικών δεδομένων προκύπτουν σημαντικά πλεονεκτήματα ουσιαστικής σημασίας για τον οργανισμό. Αυτά τα πλεονεκτήματα αφορούν το εσωτερικό και εξωτερικό περιβάλλον του οργανισμού και θα μπορούσαν να καταγραφούν ως εξής [6]:

Εσωτερικά:

α) διαχείριση του κινδύνου (αναγνώριση και περιορισμός),

β) αποφυγή κοστοβόρων επαναπροσδιορισμών της διαδικασίας επεξεργασίας αλλά και της ίδιας της εφαρμογής εάν από την αρχή έχουν προσδιοριστεί οι ενδεχόμενοι κίνδυνοι και απειλές,

γ) αποφυγή επιβολής κυρώσεων αλλά και αποφυγή της διακοπής ή απαγόρευσης του εγχειρήματος από την αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων λόγω μη συμμόρφωσης στους υφιστάμενους κανονισμούς και στη νομοθεσία της Ε.Ε,

δ) βελτίωση της προστασίας των προσωπικών δεδομένων και της αποδοτικότητας της συγκεκριμένης υπηρεσίας,

ε) βελτίωση του τρόπου διαχείρισης των δεδομένων γνωρίζοντας τις πιθανές απειλές και αστοχίες,

στ) αύξηση της ασφάλειας του συστήματος όσον αφορά την προστασία των δεδομένων και των γενικότερων λειτουργιών του οργανισμού που βασίζονται σε αυτό,

ζ) βελτίωση της τεχνογνωσίας σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριακών συστημάτων.

Εξωτερικά:

α) ενίσχυση της αξιοπιστίας του οργανισμού από την πλευρά των εμπλεκόμενων μερών

β) υπόδειξη συμμόρφωσης με την νομοθεσία περί προστασίας προσωπικών δεδομένων και επιβεβαίωση ότι η ασφάλεια λαμβάνεται σοβαρά υπόψη.

2.5 Μεθοδολογία διενέργειας ΕΑΠΔ

Ο Κανονισμός δεν υποδεικνύει συγκεκριμένη μεθοδολογία για την διενέργεια μιας ΕΑΠΔ. Ωστόσο, σαφώς και υπάρχουν δοκιμασμένες βέλτιστες πρακτικές της οποίες μπορούμε να ακολουθήσουμε, ώστε να πετύχουμε τον σκοπό της ΕΑΠΔ. Αυτό φυσικά δίνει τη δυνατότητα σε αυτόν που διενεργεί την ΕΑΠΔ να επιλέξει μεταξύ πληθώρας και δοκιμασμένων τεχνικών που θα του δώσουν την δυνατότητα να επιτύχει ένα σωστό αποτέλεσμα. Μπορεί ο Κανονισμός να μην προτείνει συγκεκριμένη μεθοδολογία όπως προαναφέρθηκε όμως είναι σαφής ως προς τα κριτήρια και τα χαρακτηριστικά τα οποία θα πρέπει να περιλαμβάνονται σε μία σωστή ΕΑΠΔ [2].

Ο Κανονισμός ορίζει το ελάχιστο περιεχόμενο της ΕΑΠΔ:

1. περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας

2. εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας

3. εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων

4. τα προβλεπόμενα μέτρα:

    α) αντιμετώπισης των κινδύνων

    β) απόδειξης της συμμόρφωσης με τον παρόντα Κανονισμό

Το ακόλουθο γράφημα απεικονίζει τη γενική επαναλαμβανόμενη διαδικασία που πρέπει να ακολουθείται για τη διενέργεια ΕΑΠΔ.

Κατά την εκτίμηση του αντικτύπου μιας πράξης επεξεργασίας δεδομένων πρέπει να λαμβάνεται υπόψη (άρθρο 35 παράγραφος 8) ή τυχόν συμμόρφωση με έναν κώδικα δεοντολογίας (άρθρο 40). Τούτο μπορεί επίσης να χρησιμεύσει στην απόδειξη ότι έχουν επιλεγεί ή ληφθεί τα κατάλληλα μέτρα, με τον όρο ότι ο κώδικας δεοντολογίας ενδείκνυται για την πράξη επεξεργασίας. Θα πρέπει επίσης να λαμβάνονται υπόψη οι πιστοποιήσεις, οι σφραγίδες και τα σήματα [προστασίας των δεδομένων] για τον σκοπό της απόδειξης της συμμόρφωσης των πράξεων επεξεργασίας των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία (άρθρο 42) με τον Κανονισμό, καθώς και οι δεσμευτικοί εταιρικοί κανόνες . Όλες οι συναφείς απαιτήσεις που περιέχει ο Κανονισμός παρέχουν ένα ευρύ, γενικό πλαίσιο για τον σχεδιασμό και την υλοποίηση ΕΑΠΔ. Η πρακτική υλοποίηση μιας ΕΑΠΔ θα εξαρτηθεί από την πλήρωση των απαιτήσεων του κανονισμού, οι οποίες μπορεί να συμπληρωθούν με πιο αναλυτικές πρακτικές οδηγίες. Ως εκ τούτου, η υλοποίηση ΕΑΠΔ είναι κλιμακώσιμη. Αυτό σημαίνει ότι ακόμη και ένας μικρής εμβέλειας υπεύθυνος επεξεργασίας μπορεί να σχεδιάσει και να διενεργήσει DPIA πρόσφορη για τις πράξεις επεξεργασίας του [2].

Η αιτιολογική σκέψη 90 του κανονισμού παραθέτει μια σειρά στοιχείων της ΕΑΠΔ που αλληλεπικαλύπτονται με τα πλήρως καθορισμένα στοιχεία της διαχείρισης κινδύνων. Με όρους

διαχείρισης κινδύνου, μια ΕΑΠΔ αποσκοπεί στη «διαχείριση των κινδύνων» για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, με χρήση των ακόλουθων διαδικασιών, μέσω:

α) του καθορισμού του πλαισίου: «λαμβάνοντας υπόψη τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας και τις πηγές του κινδύνου»

β) της εκτίμησης των κινδύνων: «ώστε να εκτιμήσει την ιδιαίτερη πιθανότητα και τη σοβαρότητα του υψηλού κινδύνου»

γ) της αντιμετώπισης των κινδύνων: «που μετριάζουν αυτόν τον κίνδυνο» και «διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα» και «αποδεικνύουν τη συμμόρφωση προς τον παρόντα Κανονισμό».

Η ΕΑΠΔ κατά τον Κανονισμό αποτελεί εργαλείο διαχείρισης των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, επομένως, υιοθετεί τη δική τους οπτική, όπως ισχύει σε ορισμένους τομείς (π.χ. κοινωνική ασφάλεια). Αντιθέτως, σε άλλους τομείς η διαχείριση των κινδύνων (π.χ. ασφάλεια πληροφοριών) επικεντρώνεται στην οργανωτική διάρθρωση.

Ο Κανονισμός παρέχει ευελιξία στους υπεύθυνους επεξεργασίας για τον καθορισμό της ακριβούς δομής και της μορφής της ΕΑΠΔ, προκειμένου αυτή να εξυπηρετεί τις υφιστάμενες πρακτικές εργασίας. Υπάρχουν πολυάριθμες καθιερωμένες διαδικασίες, εντός της ΕΕ και παγκοσμίως, που λαμβάνουν υπόψη τα στοιχεία που περιγράφονται στην αιτιολογική σκέψη 90. Ωστόσο, ανεξαρτήτως της μορφής που θα λάβει, η ΕΑΠΔ θα πρέπει να αποτελεί μια πραγματική αξιολόγηση των κινδύνων, που θα παρέχει στους υπεύθυνους επεξεργασίας τη δυνατότητα να λάβουν μέτρα για την αντιμετώπισή τους.

Διαφορετικές μεθοδολογίες θα μπορούσαν να χρησιμοποιηθούν για να συνδράμουν στην υλοποίηση των βασικών απαιτήσεων που θέτει ο Κανονισμός. Έχουν προσδιοριστεί ορισμένα κοινά κριτήρια ώστε να επιτρέπεται στους υπεύθυνους επεξεργασίας να υιοθετούν διαφορετικές προσεγγίσεις, συμμορφούμενοι παράλληλα με τον Κανονισμό. Τα εν λόγω κριτήρια αποσαφηνίζουν τις βασικές απαιτήσεις του κανονισμού και παρέχουν επαρκές έδαφος για τη χρήση διαφορετικών μορφών υλοποίησης. Τα εν λόγω κριτήρια μπορούν να χρησιμοποιηθούν για την απόδειξη ότι μια συγκεκριμένη μεθοδολογία ΕΑΠΔ πληροί τα απαιτούμενα πρότυπα που θέτει ο Κανονισμός.

2.6 Βήματα εκτέλεσης ΕΑΠΔ

Στο σημείο αυτό θα πρέπει να αναφέρουμε ότι σε ποια και σε πόσα βήματα χωρίζεται μια διαδικασία ΕΑΠΔ είναι κυρίως θέμα προτίμησης. Περισσότερο σημαντική είναι η κατανόηση της δομής και η επεξεργασία της διαδικασίας, η οποία λαμβάνει ιδίως υπόψη τις απαιτήσεις του άρθρου 35 (7) του ΓΚΠΔ και τις συστάσεις της Ομάδας Εργασίας του άρθρου 29 [2], [7].

Το μοντέλο ΕΑΠΔ για έξυπνα δίκτυα και συστήματα έξυπνης μέτρησης, το οποίο αναφέρεται ρητώς στη σύσταση 2014/724/ΕΕ της Ευρωπαϊκής Επιτροπής, προβλέπει τα ακόλουθα βήματα:

1. **Προ-αξιολόγηση και κριτήρια που καθορίζουν την ανάγκη διενέργειας μιας ΕΑΠΔ**: Ο στόχος του πρώτου βήματος είναι να παρέχει καθοδήγηση στον ιδιοκτήτη του συστήματος ή της υπηρεσίας - ο οποίος έχει ουσιώδη ρόλο στη συγκεκριμένη διαδικασία - να διαπιστώσει εάν είναι απαραίτητη μια ΕΑΠΔ και ποιος θα πρέπει να διεξάγει αυτή την ΕΑΠΔ (τούτο βέβαια δεν αίρει το γεγονός ότι, τελικά, η ευθύνη για τη λήψη απόφασης εκπόνησης ΕΑΠΔ βαρύνει αποκλειστικά τον υπεύθυνο επεξεργασίας – δηλαδή τον οργανισμό ως νομικό πρόσωπο: αυτό συνεπάγεται υποχρεώσεις της Διοίκησης στο να κάνει κατάλληλη ανάθεση ρόλων και αρμοδιοτήτων). Προτείνεται συνεπώς στον ιδιοκτήτη του συστήματος να πραγματοποιήσει μια αρχική ανάλυση της υπό εξέταση αίτησης και να αποφασίσει εάν θα προχωρήσει στα επόμενα βήματα της ΕΑΠΔ ή θα σταματήσει τη διαδικασία. Κατά τη διάρκεια αυτού του βήματος θα πρέπει να απαντηθούν βασικά ερωτήματα:

    α) Γίνεται επεξεργασία προσωπικών δεδομένων; Υπάρχει αντίκτυπο στα δικαιώματα και τις ελευθερίες του ατόμου;

    β) Σε ποιο στάδιο της ανάπτυξης θα πρέπει να διενεργηθεί η ΕΑΠΔ;

    γ) Ποιος είναι ο σκοπός της υπηρεσίας ή του συστήματος που επεξεργάζεται προσωπικά δεδομένα;

2. **Έναρξη:** Κατά την εκκίνηση μιας ΕΑΠΔ πρέπει να λαμβάνονται υπόψη και να αποτυπώνονται τα παρακάτω:

    α) Καταγραφή ομάδας έργου

β) Καταγραφή ρόλου ομάδας ή ατόμου

γ) Καταγραφή αρμοδιοτήτων ομάδας έργου

δ) Καταγραφή συνεντευξιαζόμενων και εγγράφων που παρέχονται

3. **Προσδιορισμός, χαρακτηρισμός και περιγραφή των συστημάτων / εφαρμογών που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα:** Στο σημείο αυτό θα πρέπει να αποδοθεί η πλήρης εικόνα ενός οργανισμού, ο σχεδιασμός της εφαρμογής, του περιβάλλοντος, των επεξεργασμένων δεδομένων, οι ροές πληροφοριών, των ορίων του συστήματος. Για να επιτευχθεί η σωστή απεικόνιση, απαιτείται να συμπληρωθεί ένα σύνολο πινάκων. Κάθε πίνακας συνοδεύεται από μια σειρά οδηγιών σχετικά με τον τρόπο με τον οποίο θα πρέπει να συμπληρωθεί προκειμένου να παρέχεται καθοδήγηση μέσω αυτού του μέρους της διαδικασίας.

4. **Προσδιορισμός των πιθανών κινδύνων:** Ο στόχος αυτού του βήματος είναι να προσδιοριστούν οι συνθήκες και οι δυνητικοί κίνδυνοι που ενδέχεται να απειλήσουν τα προσωπικά δεδομένα του υποκειμένου των δεδομένων και να επηρεάσουν την ιδιωτική του ζωή με βάση κανονισμό. Μια διαδικασία εκτίμησης κινδύνου θα πρέπει συνήθως να εξετάζει τους κινδύνους από την άποψη της πιθανότητας εμφάνισης (likelihood) και τον αντίκτυπο των συνεπειών τους (impact). Αυτοί οι κίνδυνοι απορρήτου αποτελούνται κυρίως από ένα ακραίο γεγονός και τις απειλές που θα μπορούσαν να πυροδοτήσουν αυτό το γεγονός (πολλές απειλές μπορούν να προκαλέσουν το ίδιο γεγονός). Ο υπεύθυνος προστασίας θα πρέπει να συμμετέχει στην ανάλυση αυτή, όπως έχει ήδη προταθεί.

5. **Αξιολόγηση κινδύνου προστασίας δεδομένων**: οι απειλές αξιολογούνται και μετρούνται με βάση τη σοβαρότητα των επιπτώσεων στα άτομα και την πιθανότητα εμφάνισης. Για να ταξινομηθούν οι επιπτώσεις και η πιθανότητα, μπορούν να χρησιμοποιηθούν αρκετά ευρέως διαθέσιμα μοντέλα. Είναι αποδεκτή η χρήση εναλλακτικών μεθοδολογιών και εφόσον οι κίνδυνοι για την προστασία της ιδιωτικής ζωής μπορούν να επηρεάσουν το υποκείμενο των δεδομένων τότε προσδιορίζονται και ποσοτικοποιούνται κατάλληλα.

6. **Προσδιορισμός, σύσταση ελέγχων και υπολειπόμενοι κίνδυνοι:** Στόχος είναι να εξεταστούν οι κίνδυνοι που εντοπίστηκαν και αξιολογήθηκαν στο προηγούμενο στάδιο

και να παρουσιαστούν οι έλεγχοι που έχουν εφαρμοστεί ή πρόκειται να εφαρμοστούν προκειμένου να μειωθεί ο κίνδυνος σε κατάλληλα επίπεδα. Κάθε προσδιορισμένος κίνδυνος πρέπει να μετριαστεί κατάλληλα με έναν ή περισσότερους ελέγχους, λαμβάνοντας υπόψη την πιθανότητα και τον αντίκτυπό τους.

7. **Τεκμηρίωση και σύνταξη της έκθεσης ΕΑΠΔ**: Η έκθεση ΕΑΠΔ μπορεί να δομηθεί γύρω από τα βήματα που προσδιορίστηκαν προηγουμένως, παρουσιάζοντας τα αποτελέσματα κάθε βήματος και αξιολογώντας το κάθε τι.. Η ΕΑΠΔ περιλαμβάνει εσωτερικές διαδικασίες και μπορεί να χειρίζονται ιδιόκτητες διαβαθμισμένων πληροφορίων του οργανισμού που σχετίζονται με προϊόντα και διαδικασίες, με ειδικές απαιτήσεις εμπιστευτικότητας. Η υπογεγραμμένη έκθεση ΕΑΠΔ, η οποία περιέχει εγκεκριμένη απόφαση, θα πρέπει να δίδεται στον υπεύθυνο προστασίας δεδομένων του εκάστοτε οργανισμού (εάν υπάρχει) σύμφωνα με τις εσωτερικές διαδικασίες του ιδιοκτήτη του συστήματος.

8. **Αναθεώρηση και συντήρηση**: Σε αυτό το σημείο διασφαλίζεται ότι η ανάληψη υποχρέωσης που απορρέει από την διεξαχθείσα ΕΑΠΔ διεξάγεται στο υπάρχον σύστημα ή στο έργο που υλοποιείται.

Το πρότυπο ISO/IEC 29134 παρέχει κατευθυντήριες γραμμές για μια διαδικασία διενέργειας αντικτύπου σχετικά με την ιδιωτικότητα και για τη δομή και το περιεχόμενο μιας έκθεσης PIA. Η διαδικασία χωρίζεται στις ακόλουθες τέσσερις υπο-κατηγορίες:

1. Πρωταρχική ανάλυση

2. Προετοιμασία της PIA

3. Εκτέλεση του PIA

4. Επικαιροποίηση της PIA

2.7 Κριτήρια για μια αποδεκτή ΕΑΠΔ

Η ομάδα εργασίας του άρθρου 29[2] (η οποία είναι μία ομάδα εργασίας που είχε συσταθεί με το άρθρο 29 της προηγούμενης Οδηγίας 95/46/ΕΚ και αποτελούνταν από εκπροσώπους των Αρχών Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης) προτείνει τα ακόλουθα κριτήρια, τα οποία οι υπεύθυνοι επεξεργασίας μπορούν να χρησιμοποιούν για να αξιολογούν κατά πόσο μια ΕΑΠΔ ή μια μεθοδολογία διενέργειας ΕΑΠΔ είναι επαρκώς περιεκτική προκειμένου να συμμορφώνεται με τον Κανονισμό:

1. παρέχεται συστηματική περιγραφή των πράξεων επεξεργασίας [άρθρο 35 παράγραφος 7 στοιχείο α)]:

    α) λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90)

    β) καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα

    γ) παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας

    δ) προσδιορίζονται τα μέσα στα οποία υφίστανται επεξεργασίαι τα δεδομένα (υλισμικό, λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων)

    ε) λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας, εφόσον υπάρχουν (άρθρο 35 παράγραφος 8)

2. εκτιμώνται η αναγκαιότητα και η αναλογικότητα [άρθρο 35 παράγραφος 7 στοιχείο β)]

    α) καθορίζονται τα προβλεπόμενα μέτρα συμμόρφωσης με τον Κανονισμό [άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90], λαμβάνοντας υπόψη:

        i. τα μέτρα που κατατείνουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας βάσει:

[2] Η ομάδα εργασίας του άρθρου 29 είναι η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως τις 25 Μαΐου 2018 (έναρξη ισχύος του ΓΚΠΔ).

ii. καθορισμένων, ρητών και νόμιμων σκοπών [άρθρο 5 παράγραφος 1 στοιχείο β)]

iii. της νομιμότητας της επεξεργασίας (άρθρο 6)

iv. κατάλληλων, συναφών και περιορισμένων στα αναγκαία δεδομένων [άρθρο 5 παράγραφος 1 στοιχείο γ)]

v. της περιορισμένης διάρκειας αποθήκευσης [άρθρο 5 παράγραφος 1 στοιχείο ε)]

β) μέτρα που συμβάλλουν στη διαφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων:

i. πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρθρα 12, 13 και 14)

ii. δικαίωμα πρόσβασης και δικαίωμα στη φορητότητα των δεδομένων (άρθρα 15 και 20)

iii. δικαίωμα διόρθωσης και διαγραφής (άρθρα 16, 17 και 19)

iv. δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρθρα 18, 19 και 21)

v. σχέσεις με τους εκτελούντες την επεξεργασία (άρθρο 28)

vi. διασφαλίζονται οι περιστάσεις που περιβάλλουν τη διεθνή διαβίβαση ή τις διεθνείς διαβιβάσεις (Κεφάλαιο V)

vii. προηγούμενη διαβούλευση (άρθρο 36)

3. τελούν υπό διαχείριση οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων [άρθρο 35 παράγραφος 7 στοιχείο γ)]:

α) έχουν αξιολογηθεί η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (πρβλ. αιτιολογική σκέψη 84) ή ειδικότερα κάθε κίνδυνος (αθέμιτη

πρόσβαση, ανεπιθύμητη τροποποίηση, και εξαφάνιση δεδομένων) από την οπτική των υποκειμένων των δεδομένων

i. έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτιολογική σκέψη 90)

ii. εξακριβώνονται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περιπτώσεις συμβάντων που περιλαμβάνουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων

Κεφάλαιο 4
Μελέτη Περίπτωσης Οργανισμού

Στο κεφάλαιο αυτό περιγράφεται η μελέτη περίπτωσης αποτυπώνοντας τα υπό εξέταση αγαθά, συστήματα, υπηρεσίες και δεδομένα, η κατηγοριοποίηση, η περιγραφή και η μελέτη των εκάστοτε προαναφερθέντων αγαθών, ως προς τις απαιτήσεις εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, καθώς και ως προς τις απαιτήσεις ιδιωτικότητας για την υπό μελέτη περίπτωση. Επιπλέον γίνεται αποτίμηση επιπτώσεων ασφάλειας καθώς και απειλών-αδυναμιών για κάθε αγαθό, καταγραφή των μέτρων ασφάλειας που μπορούν να ληφθούν Στα πλαίσια της παρούσας μεταπτυχιακής διατριβής, αναλύεται ο τρόπος με τον οποίο η μεθοδολογία κατά ISO 27005 μπορεί να βοηθήσει για να πραγματοποιηθεί η ΕΑΠΔ, καθώς και να προσδιοριστεί μια μεθοδολογία και κατευθυντήριες γραμμές που μπορούν να βοηθήσουν τον εν λόγω οργανισμό να πραγματοποιήσει μια αποτελεσματική ΕΑΠΔ κατά τη διαχείριση δραστηριοτήτων που εμπεριέχουν προσωπικά δεδομένα. Θα πρέπει να σημειωθεί ότι τα δεδομένα που αναφέρονται στο κεφάλαιο αυτό είναι κατά προσέγγιση πραγματικά διότι δεν θα μπορούσαν αν αποτυπωθούν τα πλήρη και πραγματικά δεδομένα του εν λόγω οργανισμού.

4.1 Περιγραφή Μεθοδολογίας

Στο πλαίσιο της μεταπτυχιακής διατριβής χρησιμοποιήθηκε η μεθοδολογία κατά ISO/IEC 27005. Τα στάδια για την ολοκληρωμένη ανάλυση του εν λόγω οργανισμού αποτυπώνονται παρακάτω:

1. Καταγραφή των υπό εξέταση services, data & systems και κατ'επέκταση των αγαθών που θα μελετηθούν

2. Κατανομή αυτών σε κατηγορίες (Asset categories) και περιγραφή του ιδιοκτήτη και της τοποθεσίας του κάθε αγαθού

3. Μελέτη του εκάστοτε αγαθού ως προς την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας

4. Αποτίμηση των επιπτώσεων ασφάλειας λαμβάνοντας υπόψη τον μέγιστο βαθμό αποτίμησης όλων των κατηγοριών (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα)

5. Αποτίμηση απειλών – αδυναμιών για κάθε αγαθό και καταγραφή σε σχετικούς πίνακες

6. Καταγραφή των μέτρων ασφάλειας που μπορούν να ληφθούν, καθώς και την επιλεχθείσα στρατηγική, τον υπεύθυνο και τον χρόνο υλοποίησης της στρατηγικής αυτής και τέλος τον εναπομείναντα κίνδυνο

4.2 Περιγραφή Οργανισμού

Ο υπό μελέτη οργανισμός είναι επιστημονικός, ερευνητικός και συμβουλευτικός φορέας που σκοπός του είναι η διεξαγωγή θεωρητικής και εφαρμοσμένης έρευνας και η εκπόνηση μελετών, ιδίως σε στρατηγικό επίπεδο, για θέματα που αφορούν την Πολιτική Ασφάλειας, καθώς και η παροχή υπηρεσιών, γνωμοδοτικού και συμβουλευτικού χαρακτήρα, σε θέματα ασφάλειας γενικότερα. Η ανάδειξη και καταξίωση του οργανισμού σε σημαντικό σημείο αναφοράς για όλες τις δράσεις σχετικές με την αποστολή του τόσο στην Ελλάδα όσο και στο εξωτερικό αποτελεί τον βασικό στόχο του οργανισμού.

4.2.1 Τμήματα Οργανισμού

Τμήμα Έρευνας και Ανάπτυξης

Το τμήμα Έρευνας & Ανάπτυξης περιλαμβάνει τις παρακάτω δραστηριότητες:

1. διεξάγει ερευνητικά προγράμματα και μελέτες για θέματα εσωτερικής ασφάλειας

2. εκπονεί και εκτελεί ερευνητικά προγράμματα για λογαριασμό ή σε συνεργασία με αντίστοιχους φορείς της Ευρωπαϊκής Ένωσης, άλλων κρατών ή διεθνών οργανισμών σύμφωνα με τους αντίστοιχους κανόνες και διαδικασίες

3. οργανώνει και διεξάγει συνέδρια

4. δημοσιεύει ερευνητικά και γενικότερα επιστημονικά πορίσματα και συναφή έργα

Τμήμα Νομικών Συμβούλων

Το τμήμα Νομικών Συμβούλων περιλαμβάνει τις παρακάτω δραστηριότητες:

1. Συμβουλεύουν τα υπόλοιπα τμήματα σε θέματα νομικής φύσεως

2. Συμμετέχουν στην δημιουργία και αναθεώρηση των πολιτικών ασφάλειας

3. Παρέχουν νομική υποστήριξη για τον οργανισμό (π.χ δικαστικές διαμάχες)

Τμήμα Πιστοποιήσεων

Το τμήμα Πιστοποιήσεων περιλαμβάνει τις παρακάτω δραστηριότητες:

1. πραγματοποιεί εκπαιδευτικά σεμινάρια και παρέχει πιστοποιημένες εκπαιδεύσεις σε θέματα ασφάλειας

2. εκπονεί πιστοποιημένες μελέτες σε θέματα ασφάλειας

3. οργανώνει και διεξάγει συνέδρια και δράσεις

Τομέας Υπηρεσιών & Υποστήριξης

Ο τομέας Υπηρεσιών & Υποστήριξης περιλαμβάνει τα παρακάτω υποτμήματα:

1. Τμήμα Γραμματείας

2. Τμήμα Λογιστηρίου

3. Τμήμα Μηχανογράφησης

4. Τμήμα Προμηθειών

5. Τμήμα Τεχνικής Υποστήριξης

Τμήμα Οικονομικών Συναλλαγών

Το τμήμα Οικονομικών Συναλλαγών αφορά τις οικονομικές δραστηριότητες (π.χ. ευρωπαϊκά κονδύλια από ΕΕ) των παραπάνω τμημάτων.

4.2.2 Αλληλεξαρτήσεις με άλλα συστήματα – φορείς

Ο οργανισμός στο πλαίσιο υλοποίησης των ευρωπαϊκών προγραμμάτων συνεργάζεται με αρκετούς ευρωπαϊκούς & εθνικούς φορείς ή/και εταιρείες εθνικού ή ευρωπαϊκού βεληνεκούς κατά περίσταση στο πλαίσιο υλοποίησης των στόχων του εκάστοτε έργου. Επί παραδείγματι και πέραν της συνεργασίας με σκοπό την υλοποίηση των ευρωπαϊκών προγραμμάτων, υπάρχουν συνεργασίες με εταιρείες που προσφέρουν Domains, Web hosting, etc. καθώς και συνεργασίες για την παροχή υπηρεσιών email, κτλ.

4.2.3 Συστήματα ή τμήματα εκτός πεδίου εφαρμογής της μεταπτυχιακής διατριβής

Στα πλαίσια της παρούσας μεταπτυχιακής διατριβής θα εφαρμοστεί η μελέτη για το τμήμα έρευνας & ανάπτυξης. Από το πεδίο εφαρμογής μελέτης εξαιρούνται τα παρακάτω τμήματα:

1. Τμήμα Νομικών Συμβούλων
2. Τμήμα Πιστοποιήσεων
3. Τομέας Υπηρεσιών & Υποστήριξης
4. Τμήμα Οικονομικών Συναλλαγών

4.3 Καταγραφή αγαθών του Οργανισμού

Ο διαχωρισμός των αγαθών για το τμήμα Έρευνας & Ανάπτυξης πραγματοποιήθηκε σύμφωνα με τις παρακάτω κατηγορίες:

1. H/W (Hardware)
2. S/W (Software)

Τα δεδομένα χωρίστηκαν στις εξής κατηγορίες:

1. Προσωπικά
2. Διαβαθμισμένα
3. Δεδομένα Αυθεντικοποίησης
4. Δεδομένα Παραμετροποίησης
5. Δεδομένα back-up

Οι κατηγορίες των συστημάτων είναι δύο: Computer Systems, Network. Οι υποκατηγορίες των S/W & H/W αγαθών είναι οι ακόλουθες:

1. Operating system
2. Stand-alone application
3. Database SW
4. Web Server SW
5. Server Computer
6. Client Computer
7. Router
8. Switch
9. Storage Equipment
10. Firewall

4.3.1 Καταγραφή υπηρεσιών

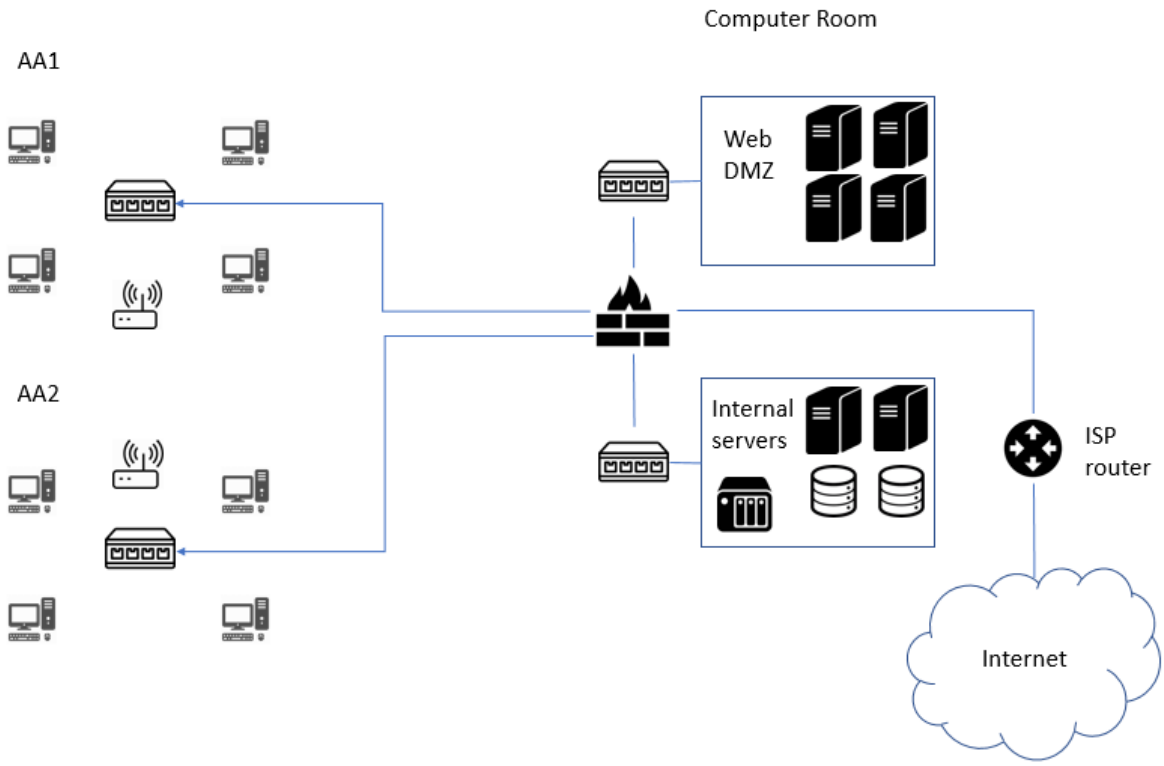
Οι υπηρεσίες οι οποίες έγιναν αντικείμενο μελέτης στην παρούσα εργασία, για το τμήμα Έρευνας και Ανάπτυξης είναι οι παρακάτω:

1. **Website:** Η συγκεκριμένη υπηρεσία αφορά τον ιστότοπο ο οποίος παρέχει πληροφορίες και χρήσιμο υλικό για ένα ερευνητικό πρόγραμμα. Ο κύριος στόχος αυτής της υπηρεσίας είναι η διάδοση των αποτελεσμάτων του προγράμματος

2. **Moodle – e learning platform:** Η υπηρεσία Moodle έχει δημιουργηθεί για να παρέχει OnLine το απαραίτητο εκπαιδευτικό υλικό στους ενδιαφερόμενους. Για την πρόσβαση στην συγκεκριμένη υπηρεσία απαιτείται η αυθεντικοποίηση των εκπαιδευόμενων (username, password).

3. **Network Attached Storage (NAS):** Πρόκειται για την υπηρεσία που προσφέρεται για την αποθήκευση και σε ορισμένες περιπτώσεις την κοινή χρήση αρχείων του οργανισμού.

4.3.2 Διάγραμμα δικτύου



Εικόνα 1: Διάγραμμα δικτύου οργανισμού

Στο παραπάνω διάγραμμα δικτύου αποτυπώνεται η ακριβής διάταξη του δικτύου που αφορά τις προς μελέτη υπηρεσίες. Τα AA1 και AA2 μπορούν να θεωρηθούν χώροι εργασίας με πεπερασμένο αριθμό θέσεων. Καθένας από τους προαναφερθέντες χώρους, διαθέτουν patch panel & switch για την σύνδεσή τους στο εσωτερικό δίκτυο του οργανισμού. Επιπροσθέτως, διαθέτουν από ένα

Wireless Access Point, το οποίο βρίσκεται όμως «εξωτερικά» του δικτύου (ξεχωριστό VLAN), όπως αποτυπώνεται και στο σχήμα. Στο computer room, υπάρχουν ένα firewall, από το οποίο περνάει όλη η κίνηση του δικτύου (και πριν εισέλθει/εξέλθει data στο Internet), αφού στην συνέχεια περάσει από το router του ISP. Το computer room είναι χωρισμένο σε 2 περιοχές, την web DMZ που περιέχει κάθε «service» το οποίο έχει επαφή με το Internet και την περιοχή των Internal servers, που περιέχει κάθε service που δεν βγαίνει στο Internet και βρίσκεται στο εσωτερικό VLAN του οργανισμού.

4.3.3 Χαρτογράφηση Πληροφοριακού Συστήματος– Asset Model

#	**SERVICE**	Name:	**WebSite**
1	**DESCRIPTION**	Πρόκειται για τον διαδικτυακό τόπο όπου παρουσιάζονται όλες οι απαπαίτητες πληροφορίες (περίληψη, νέα, εταίροι, υλικό διάδοσης, κτλ.) για το ευρωπαϊκό πρόγραμμα	

#	**DATA**			
1	**Name**	Πηγαίος κώδικας της ιστοσελίδας	**Category**	Δεδομένα παραμετροποίησης
2	**Name**	Configuration Αρχεία της ιστοσελίδας	**Category**	Δεδομένα παραμετροποίησης
3	**Name**	Πληροφορίες ευρωπαϊκού προγράμματος	**Category**	-
4	**Name**	Προσωπικά στοιχεία συνδρομητών (subscriber, registration forms)	**Category**	Προσωπικά

SYSTEM					
#	**SYSTEM NAME:**	**Web Server**	**CATEGORY:**	Computer System	
1	**DESCRIPTION**	web server responsible for the provision of the project's website			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A1	DELL PowerEdge T670	**H/W**	**Server Computer**	Computer Room
	A2	Ubuntu 16.04	**S/W**	**Operating System**	
	A3	Apache / php 7	**S/W**	**Web Server SW**	
SYSTEM					
#	SYSTEM NAME:	**DB Server**	**CATEGORY:**	Computer System	

2	**DESCRIPTION**	Είναι ο DB server του web site			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A4	DELL PowerEdge T670	**H/W**	**Server Computer**	Computer Room
	A5	Ubuntu 16.04	**S/W**	**Operating System**	
	A6	MySQL	**S/W**	**Database SW**	
SYSTEM					
#	SYSTEM NAME:	**Workstation 1**	**CATEGORY:**	**Computer System**	
3	**DESCRIPTION**	Πρόκειται για το Workstation του διαχειριστή του website			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A7	DELL Workstation PC Precision 3430	**H/W**	**Client Computer**	Room AA1
	A8	Windows 10	**S/W**	**Operating System**	
	A9	OFFICE 365	**S/W**	**stand-alone Application**	
SYSTEM					
#	SYSTEM NAME:	**Main network**	**CATEGORY:**	**Network**	
4	**DESCRIPTION**	Το βασικό δίκτυο των servers όπου φιλοξενείται το website			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A10	FortiGate 200f	**H/W**	**Firewall / Router**	Computer Room
	A11	FortiSwitch 124D-POE	**H/W**	**Switch**	Computer Room

Πίνακας 1: Service no 1

#	**SERVICE**	**NAME:**	**Moodle - e learning platfrom**	
2	**DESCRIPTION**	Πρόκειται για την διαδικτυακή εφαρμογή όπου καταχωρείται το εκπαιδευτικό υλικού και υποβάλλονται τα τεστ αξιολόγησης		
#	**DATA**			
1	**NAME:**	Πηγαίος κώδικας της ιστοσελίδας του moodle	**CATEGORY:**	Δεδομένα παραμετροποίησης
2	**NAME:**	Configuration Αρχεία της ιστοσελίδας/του MOODLE	**CATEGORY:**	Δεδομένα παραμετροποίησης
3	**NAME:**	Προσωπικά στοιχεία εκπαιδευόμενων	**CATEGORY:**	Προσωπικά δεδομένα

4	**NAME:**	Στοιχεία αυθεντικοποίησης εκπαιδευόμενων	**CATEGORY:**	Δεδομένα Αυθεντικοποίησης	
	SYSTEM				
#	**SYSTEM NAME:**	**Web Server**	**CATEGORY:**	**Computer System**	
1	**DESCRIPTION**	Web server responsible for the provision of the project's e-learning platform			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A12	DELL PowerEdge T420	**H/W**	**Server Computer**	Computer Room
	A13	Windows Server 2012 R2	**S/W**	**Operating System**	
	A14	Apache /php	**S/W**	**Web Server SW**	
	SYSTEM				
#	**SYSTEM NAME:**	**DB Server**	**CATEGORY:**	**Computer System**	
2	**DESCRIPTION**	Είναι ο DB server του moodle			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A15	DELL PowerEdge T420	**H/W**	**Server Computer**	Computer Room
	A16	Windows Server 2012 R2	**S/W**	**Operating System**	
	A17	MariaDB	**S/W**	**Database SW**	
	SYSTEM				
#	**SYSTEM NAME:**	**PC**	**CATEGORY:**	**Computer System**	
3	**DESCRIPTION**	Πρόκειται για το PC του διαχειριστή της πλατφόρμας MOODLE			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A18	DELL XPS Tower	**H/W**	**Client Computer**	Room AA1

	A19	Windows 10	**S/W**	**Operating System**	
	A20	OFFICE 365	**S/W**	**stand-alone Application**	
	SYSTEM				
#	**SYSTEM NAME:**	**main network**	**CATEGORY:**	**Network**	
4	**DESCRIPTION**	Το βασικό δίκτυο των servers όπου φιλοξενείται η πλατφόρμα			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A10	FortiGate 200f	**H/W**	**Firewall / Router**	Computer Room
	A11	FortiSwitch 124D-POE	**H/W**	**Switch**	Computer Room

Πίνακας 2: Service no 2

#	**SERVICE**	**NAME:**	**Network Attached Storage (NAS)**		
3	**DESCRIPTION**	Πρόκειται για την δικτυακό σύστημα κοινόχρηστης αποθήκευσης (ερωτηματολογίων και αρχείων κοινού ενδιαφέροντος μέσω κοινόχρηστων φακέλων). Ακόμα χρησιμοποιείται για back-up αρχείων (& disaster recovery)			
#	**DATA**				
1	**NAME:**	Προσωπικά δεδομένα συνεργατών	**CATEGORY:**	Προσωπικά	Επώνυμο, Όνομα, Οργανισμό, Mail, κλπ.
2	**NAME:**	Δεδομένα για έρευνα & ανάλυση	**CATEGORY:**	Διαβαθμισμένα	Απαντήσεις ερωτηματολογίων
3	**NAME:**	Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)	**CATEGORY:**	Προσωπικά / Διαβαθμισμένα	Κοινόχρηστοι φάκελοι μεταξύ συγκεκριμέν

					ων συνεργατών
	NAME:	Δεδομένα back-up συστήματος	**CATEGORY:**	Δεδομένα back-up	

	SYSTEMS				
#	**SYSTEM NAME:**	**Network Attached Storage (Data storage server)**	**CATEGORY:**	Computer System	
1	**DESCRIPTION**	Πρόκειται για το Σύστημα κοινόχρηστου αποθηκευτικού χώρου (αρχείων)			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	21	QNAP	**H/W**	Storage Equipment	Computer Room
	22	Debian-based	**S/W**	Operating System	
	SYSTEM				
#	**SYSTEM NAME:**	**Admin Laptop**	**CATEGORY:**	**Computer System**	
2	**DESCRIPTION**	Πρόκειται για τον υπολογιστή του administrator που έχει πρόσβαση και στο NAS			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	23	DELL XPS	**H/W**	Client Computer	Room AA2
	24	Windows 10	**S/W**	Operating System	
	SYSTEM				
#	**SYSTEM NAME:**	**Main network**	**CATEGORY:**	**Network**	
3	**DESCRIPTION**	Το βασικό δίκτυο με το οποίο επικοινωνεί το NAS			

	ASSET	NAME	Category	Subcategory	LOCATION
	A10	FortiGate 200f	**H/W**	**Firewall / Router**	Computer Room
	A11	FortiSwitch 124D-POE	**H/W**	**Switch**	Computer Room

Πίνακας 3: Service No 3

4.1.1 Λίστα Αγαθών

Για να οριστούν οι ιδιοκτήτες των παρακάτω αγαθών χρησιμοποιήθηκαν οι ακόλουθες ονοματοδοσίες. Οι συγκεκριμένες ονομοταδοσίες εμπεριέχουν διάφορους ρόλους που θα αποτυπώνονται αργότερα.

1. Admin 1: Διαχειριστής των Server, NAS και ολόκληρου του δικτύου,
2. Admin 2: Διαχειριστής ιστοσελίδας ευρωπαϊκού προγράμματος
3. Admin 3: Διαχειριστής e-learning πλατφόρμας
4. Admin 4: Μέλος Τεχνικής ομάδας (ΣΕΣ) και Ομάδας διαχείρισης πληροφοριών
5. Admin 5: Μέλος Τεχνικής ομάδας (ΣΕΣ) και Ομάδας διαχείρισης πληροφοριών
6. Developer 1: Website/application developer, Μέλος Τεχνικής ομάδας (ΣΕΣ) και Ομάδας δειχείρισης πληροφοριών

Όνομα	Περιγραφή	Κατηγορία Αγαθού	Χώρος	Ιδιοκτήτης
Πηγαίος κώδικας της ιστοσελίδας/Πληροφορίες ευρωπαϊκού προγράμματος	Δεδομένα παραμετροποίησης ιστοσελίδας	Data Asset		Developer 1/ Admin 2

Όνομα	Περιγραφή	Κατηγορία Αγαθού	Χώρος	Ιδιοκτήτης
Configuration Αρχεία της ιστοσελίδας	Δεδομένα παραμετροποίησης ιστοσελίδας	Data Asset		Developer 1
Προσωπικά στοιχεία συνδρομητών(subscriber, registration forms) μέσω website	Προσωπικά δεδομένα & συνεργατών	Data Asset		Admin 2
Πηγαίος κώδικας Moodle	Δεδομένα παραμετροποίησης ιστοσελίδας	Data Asset		Developer 1
Configuration Αρχεία του Moodle	Δεδομένα παραμετροποίησης ιστοσελίδας	Data Asset		Developer 1
Στοιχεία εκπαιδευόμενων μέσω Moodle	Δεδομένα αυθεντικοποίησης	Data Asset		Admin 3
DELL PowerEdge T670	Εξυπηρετητής για τον διαδικτυακό ιστότοπο σχετικά με το ευρωπαϊκό πρόγραμμα Περιλαμβάνει: • Two Intel Xeon processors • 24 DDR4 IMMs • Massive internal storage capacity with hard drives • Four hot-plug SSDs • Four GPUs	H/W Server Computer	Computer Room	Admin 1
Ubuntu 16.04		S/W Operating System		

Όνομα	Περιγραφή	Κατηγορία Αγαθού	Χώρος	Ιδιοκτήτης
Apache / php 7		S/W Web Server SW		
DELL Workstation PC Precision 3470	Workstation διαχείρισης website Περιλαμβάνει: • Intel® Core™ and Processors • Memory 64GB • AMD Radeon™ and NVIDIA® • SSD	H/W Client Computer	AA1	Admin 2
MySQL		S/W Database		
Windows 10		S/W Operating System		
OFFICE 365		stand-alone application		
FortiGate 200f		H/W Firewall/Router	Computer Room	Admin 1
FortiSwitch 124D-POE		H/W Switches	Computer Room	Admin 1
DELL PowerEdge T420	Εξυπηρετητής που αφορά το e-learning platform Περιλαμβάνει: • 2x Intel Xeon series processors. • Memory: 128 GB DDR3 • Hard Drives: SAS/SATA hard drives.	H/W Server Computer	Computer Room	Admin 1

Όνομα	Περιγραφή	Κατηγορία Αγαθού	Χώρος	Ιδιοκτήτης
Windows Server 2012 R2	Λειτουργικό σύστημα του server	S/W Operating System		
MariaDB	Λογισμικό με το οποίο γίνεται η αποθήκευση των δεδομένων των χρηστών μέσω του Moodle e-learning platform	S/W Database		
DELL XPS Tower	Workstation διαχείρισης website Περιλαμβάνει: • Intel® Core™ Processor • 2TB M.2 PCIe NVMe SSD • 24GB, DDR4, 2666MHz • NVIDIA® GeForce® 8GB	H/W Client Computer	AA2	Admin 3
Προσωπικά δεδομένα συνεργατών στο QNAP	Προσωπικά δεδομένα συνεργατών	Data Asset		Admin 1
Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)	Κοινόχρηστα αρχεία (word, excel κλπ.)	Data Asset		Admin 1
Δεδομένα back-up συστήματος	Δεδομένα back-up συστήματος	Data Asset		Admin 1
Δεδομένα για έρευνα & ανάλυση	Διαβαθμισμένα	Data Asset		Admin 1
QNAP	Σύστημα αποθήκευσης και διαμοίρασης δεδομένων συνδεδεμένο στο δίκτυο	H/W Storage Equipment	Computer Room	Admin 1

Όνομα	Περιγραφή	Κατηγορία Αγαθού	Χώρος	Ιδιοκτήτης
Debian-based	Λειτουργικό σύστημα του NAS	S/W Operating System		
Dell XPS	Laptop διαχειριστή (Admin 1)	H/W Client Computer	AA1	Admin 1

Σύμφωνα με τον παραπάνω πίνακα καταλήγουμε στην ομαδοποίηση μερικών αγαθών καθώς ο κίνδυνος ως προς την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα κυμαίνεται στα ίδια επίπεδα. Η ομαδοποίηση έγινε με βάση την κατηγορία στην οποία ανήκει το κάθε αγαθό. Για παράδειγμα, το λειτουργικό σύστημα του ενός server (Windows Server 2012 R2) και το λειτουργικό σύστημα του άλλου (Ubuntu 16.04) ομαδοποιήθηκαν σε ένα αγαθό στο πλαίσιο των ορίων της συγκεκριμένης εργασίας, θεωρώντας αμελητέες τις διαφορές των ευπαθειών που έχει το κάθε λειτουργικό. Η καταγραφή των τελικών ομαδοποιημένων αγαθών περιγράφεται στον πίνακα παρακάτω:

Αρ. Αγαθού	Όνομα Αγαθού
1	Προσωπικά δεδομένα & συνεργατών
2	Δεδομένα για έρευνα & ανάλυση
3	Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (Word, Excel κλπ.)
4	Δεδομένα back-up συστήματος
5	Δεδομένα παραμετροποίησης
6	Δεδομένα Αυθεντικοποίησης
7	Computer Room
8	AA1/AA2
9	QNAP
10	Debian-based SW
11	Dell XPS/ DELL Workstation PC Precision
12	Windows 10
13	FortiGate 200f
14	FortiSwitch 124D-POE
15	DELL PowerEdge T420/T630
16	Apache / php 7
17	Ubuntu 16.04/Windows Server 2012 R2
18	MySQL/MariaDB

4.4 Αποτίμηση Επιπτώσεων αγαθών

Στην συγκεκριμένη ενότητα παρουσιάζεται η αποτίμηση των αγαθών και η αιτιολόγησή τους. Αρχικά αναλύεται με παράδειγμα η αποτίμηση αγαθού δεδομένων και έπειτα εξηγείται πώς υλοποιήθηκε η αποτίμηση αγαθών λογισμικού, αγαθών υλικού και υποδομών. Τέλος, παρουσιάζεται σε πίνακα η συνοπτική αποτίμηση αξίας δεδομένων.

4.4.1 Αποτίμηση Αγαθών Δεδομένων

Παρακάτω περιλαμβάνεται η Αποτίμηση του αγαθού 1 (δεδομένων) ως προς την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Η εκτίμηση των υπολοίπων 5 αγαθών δεδομένων περιλαμβάνεται στο Παράρτημα Α.

#	1	**ΑΓΑΘΟ**	**Προσωπικά δεδομένα & συνεργατών**	
ΑΠΩΛΕΙΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ				
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** **0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ** **Σενάρια Απώλειας Εμπιστευτικότητας**			**Σχόλια**
	Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Εξωτερικό περιβάλλον				
Επιπτώσεις στις πολιτικές σχέσεις				
Διαταραχή πολιτικής απόφασης				
Ζημιές σε συνεργάτες του Οργανισμού	1	2	3	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	3			
Επιπτώσεις στις Διεθνείς σχέσεις		2	3	
Επιπτώσεις στη δημόσια τάξη	1			
Διαδικασίες και Συστήματα				
Διαταραχή ελέγχου διαχείρισης				
Υποβάθμιση υπηρεσιών				
Απρόβλεπτες ή πρόσθετες δαπάνες		3		

Απώλεια αγαθών	2			
Υπέρβαση προϋπολογισμού				
Επιπτώσεις σε πελάτες / υπαλλήλους				
Υγεία και ασφάλεια				
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	2			
Κατάχρηση προσωπικών δεδομένων		3		
Νομικές και κανονιστικές επιπτώσεις				
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών			1	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)			3	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων			2	
Νομική ευθύνη και κυρώσεις		1	2	
Summary of ratings	**Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας**	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	3	3	3	
Τελικός Βαθμός Αποτίμησης Αγαθού	**3**			Μέγιστος βαθμός αποτίμησης όλων των σεναρίων

Πίνακας 4: Αγαθό 1 - Απώλεια Εμπιστευτικότητας

#	1	ΑΓΑΘΟ	Προσωπικά δεδομένα & συνεργατών
ΑΠΩΛΕΙΑ ΑΚΕΡΑΙΟΤΗΤΑΣ			
	Επίπεδο Επίπτωσης (ISO 27005)		**Σχόλια**

Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ**				
	Σενάρια Απώλειας Ακεραιότητας				
	Μερική Καταστροφή των δεδομένων	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Εξωτερικό περιβάλλον					
Επιπτώσεις στις πολιτικές σχέσεις		2			
Διαταραχή πολιτικής απόφασης			2		
Ζημιές σε συνεργάτες του Οργανισμού			2	2	
Επιπτώσεις στις Διεθνείς σχέσεις	2	3			
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού			2	1	
Επιπτώσεις στη δημόσια τάξη					
Διαδικασίες και Συστήματα					
Διαταραχή ελέγχου διαχείρισης					
Υποβάθμιση υπηρεσιών					
Απρόβλεπτες ή πρόσθετες δαπάνες		2			
Απώλεια αγαθών					
Υπέρβαση προϋπολογισμού		1			
Επιπτώσεις σε πελάτες / υπαλλήλους					
Υγεία και ασφάλεια					
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	1	2	1		
Κατάχρηση προσωπικών δεδομένων					
Νομικές και κανονιστικές επιπτώσεις					

Παρεμπόδιση εφαρμογής νόμου ή κανονισμών					
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)			2		
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων			2	2	
Νομική ευθύνη και κυρώσεις		1			
Συνολικοί βαθμοί	**Μερική Καταστροφή των δεδομένων**	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**2**	**3**	**2**	**2**	
Τελικός Βαθμός Αποτίμησης Αγαθού	3				Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΥΨΗΛΟ**				

Πίνακας 5: Αγαθό 1 - Απώλεια Ακεραιότητας

#	1	**ΑΓΑΘΟ**	Προσωπικά δεδομένα & συνεργατών					
ΑΠΩΛΕΙΑ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ								
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**							**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ							
	Διάρκεια Διακοπής							
	15 Λεπτά	**1 ώρα**	**3 ώρες**	**12 ώρες**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	

Εξωτερικό περιβάλλον								
Επιπτώσεις στις πολιτικές σχέσεις				0	0	1	1	
Διαταραχή πολιτικής απόφασης								
Ζημιές σε συνεργάτες του Οργανισμού					1	1	1	
Επιπτώσεις στις Διεθνείς σχέσεις							2	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού				0	1	1	2	
Επιπτώσεις στη δημόσια τάξη								
Διαδικασίες και Συστήματα								
Διαταραχή ελέγχου διαχείρισης								
Υποβάθμιση υπηρεσιών				1	1	1	2	
Απρόβλεπτες ή πρόσθετες δαπάνες								
Απώλεια αγαθών							1	
Υπέρβαση προϋπολογισμού								
Επιπτώσεις σε πελάτες / υπαλλήλους								
Υγεία και ασφάλεια								
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού			1					
Κατάχρηση προσωπικών δεδομένων								
Νομικές και κανονιστικές επιπτώσεις								
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών								
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)								
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων								

Νομική ευθύνη και κυρώσεις								
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ	**15 Λεπτα**	**1 ώρα**	**3 ώρες**	**12 ώρε**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**0**	**1**	**1**	**1**	**1**	**2**	
Τελικός Βαθμός Αποτίμησης Αγαθού	**2**							Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	ΜΕΤΡΙΟ							

Πίνακας 6: Αγαθό 1 - Απώλεια Διαθεσιμότητας

4.4.2 Αποτίμηση αγαθών λογισμικού, αγαθών υλικού και υποδομών

Η αποτίμηση των δεδομένων των αγαθών λογισμικού, φυσικών αγαθών και υποδομών προκύπτει από την αποτίμηση των δεδομένων της υπηρεσίας που υποστηρίζουν. Για το λόγο αυτό η πρώτη φάση αναφέρεται στην αποτίμηση των επιπτώσεων των δεδομένων και με βάση αυτά πραγματοποιείται στη συνέχεια η αποτίμηση των υπόλοιπων αγαθών της υπηρεσίας.

4.4.3 Συνοπτική Αποτίμηση Αξίας Αγαθών

			ΒΑΘΜΟΣ ΕΠΙΠΤΩΣΗΣ			
#	**Όνομα Αγαθού**	**Περιγραφή**	C	I	A	MAX
1	Προσωπικά δεδομένα & συνεργατών		3	3	2	3

			ΒΑΘΜΟΣ ΕΠΙΠΤΩΣΗΣ			
#	Όνομα Αγαθού	Περιγραφή	C	I	A	MAX
2	Δεδομένα για έρευνα & ανάλυση		4	4	3	4
3	Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)		2	3	3	3
4	Δεδομένα back-up συστήματος		2	2	1	2
5	Δεδομένα παραμετροποίησης		3	2	2	3
6	Δεδομένα Αυθεντικοποίησης		4	2	3	4
7	Computer Room		4	4	3	4
	Computer Room		4	4	3	4

			ΒΑΘΜΟΣ ΕΠΙΠΤΩΣΗΣ			
#	Όνομα Αγαθού	Περιγραφή	C	I	A	MAX
	Computer Room		4	4	3	4
	Computer Room		4	4	3	4
	Computer Room		4	4	3	4
	Computer Room		4	4	3	4
8	AA1/AA2		2	3	3	3
	AA1/AA2		2	3	3	3
	AA1/AA2		2	3	3	3
	AA1/AA2		2	3	3	3
	AA1/AA2		2	3	3	3
9	QNAP	Storage Equipment	4	4	3	4
	QNAP	Storage Equipment	4	4	3	4
	QNAP	Storage Equipment	4	4	3	4
10	Debian-based SW	Operating System	4	4	3	4
	Debian-based SW	Operating System	4	4	3	4
	Debian-based SW	Operating System	4	4	3	4
	Debian-based SW	Operating System	4	4	3	4
	Debian-based SW	Operating System	4	4	3	4
11	Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Client Computer	4	4	3	4
	Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Client Computer	4	4	3	4
12	Windows 10	OS Client Computer	4	4	3	4

			ΒΑΘΜΟΣ ΕΠΙΠΤΩΣΗΣ			
#	Όνομα Αγαθού	Περιγραφή	C	I	A	MAX
	Windows 10	OS Client Computer	4	4	3	4
	Windows 10	OS Client Computer	4	4	3	4
	Windows 10	OS Client Computer	4	4	3	4
	Windows 10	OS Client Computer	4	4	3	4
13	FortiGate 200f	Firewall / Router	4	4	3	4
	FortiGate 200f	Firewall / Router	4	4	3	4
	FortiGate 200f	Firewall / Router	4	4	3	4
	FortiGate 200f	Firewall / Router	4	4	3	4
14	FortiSwitch 124D-POE	Switch	4	4	3	4
	FortiSwitch 124D-POE	Switch	4	4	3	0
	FortiSwitch 124D-POE	Switch	4	4	3	4
	FortiSwitch 124D-POE	Switch	4	4	3	4
	FortiSwitch 124D-POE	Switch	4	4	3	4
15	DELL PowerEdge T420/T630	Server Computer	4	2	3	4
	DELL PowerEdge T420/T630	Server Computer	4	2	3	4
	DELL PowerEdge T420/T630	Server Computer	4	2	3	4
16	Apache / php 7	Web Server SW	4	2	3	4

			ΒΑΘΜΟΣ ΕΠΙΠΤΩΣΗΣ			
#	Όνομα Αγαθού	Περιγραφή	C	I	A	MAX
	Apache / php 7	Web Server SW	4	2	3	4
	Apache / php 7	Web Server SW	4	2	3	4
17	Ubuntu 16.04/Windows Server 2012 R2	Operating System	4	2	3	4
	Ubuntu 16.04/Windows Server 2012 R2	Operating System	4	2	3	4
18	MySQL/MariaDB	Database SW	4	2	3	4
	MySQL/MariaDB	Database SW	4	2	3	4
	MySQL/MariaDB	Database SW	4	2	3	4

Πίνακας 7: Συνοπτική Αποτίμηση Αγαθών

4.5 Ανάλυση Επικινδυνότητας

Παρακάτω καθορίζεται το επίπεδο των απειλών και των αδυναμιών καθώς επίσης καθορίζονται οι απειλές και αδυναμίες ανά αγαθό.

4.5.1 Καθορισμός επιπέδου απειλών και αδυναμιών

Σ' αυτήν την ενότητα καταγράφονται οι κλίμακες που χρησιμοποιούνται σύμφωνα με την μεθοδολογία που έχει επιλεγεί, σχετικά με την αποτίμηση απειλών , αδυναμιών καθώς και την κλίμακα επικινδυνότητας.

Επίπεδο Απειλής	Βαθμός Απειλής	Περιγραφή
LOW (L)	**0**	**αναμένεται να συμβούν το πολύ μέχρι μία φορά κάθε 5χρόνια**
MEDIUM (M)	**1**	**αναμένεται να συμβούν κατά μέσο όρο μία φορά τα 3 χρόνια.**
HIGH (H)	**2**	**αναμένεται να συμβούν κατά μέσο όρο μία φορά το χρόνο**

Πίνακας 8: Κλίμακα Αποτίμησης Απειλών

Επίπεδο Αδυναμίας	Βαθμός Αδυναμίας	Περιγραφή
LOW (L)	**0**	**Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι < 33%**
MEDIUM (M)	**1**	**Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι 33% - 66%**
HIGH (H)	**2**	**Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι > 66%**

Πίνακας 9: Κλίμακα Αποτίμησης Αδυναμιών

Risk Level	Risk Value
Low	0 - 2
Medium	3 - 5
High	6 - 8

Πίνακας 10: Κλίμακα Επικινδυνότητας

4.5.2 Απειλές και Αδυναμίες ανά αγαθό

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
1	Προσωπικά δεδομένα & συνεργατών	Απώλεια δεδομένων	MEDIUM (M)	Μη διαθεσιμότητα αντιγράφων ασφαλείας	Medium (M)
				Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	Medium (M)
				Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	Medium (M)
				Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	Medium (M)
2	Δεδομένα για έρευνα & ανάλυση	Απώλεια δεδομένων	MEDIUM (M)	Μη διαθεσιμότητα αντιγράφων ασφαλείας	Medium (M)
				Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	Medium (M)
				Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	Medium (M)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
				Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	Medium (M)
3	Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)	Απώλεια δεδομένων	Low (L)	Μη διαθεσιμότητα αντιγράφων ασφαλείας	Low (L)
				Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	Low (L)
				Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	Low (L)
				Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	Low (L)
4	Δεδομένα back-up συστήματος	Απώλεια δεδομένων	Low (L)	Μη διαθεσιμότητα αντιγράφων ασφαλείας	Medium (M)
				Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	Medium (M)
				Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	Medium (M)
				Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	Medium (M)
5	Δεδομένα παραμετροποίησης	Απώλεια δεδομένων	Low (L)	Μη διαθεσιμότητα αντιγράφων ασφαλείας	Medium (M)
				Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	Medium (M)
				Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	Medium (M)
				Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	Medium (M)
6	Δεδομένα Αυθεντικοποίησης	Απώλεια δεδομένων	Low (L)	Μη διαθεσιμότητα αντιγράφων ασφαλείας	Medium (M)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
				Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	Medium (M)
				Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	Medium (M)
				Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	Medium (M)
7	Computer Room	Μη έγκαιρη αποκατάσταση πληροφοριακών συστημάτων	Low (L)	Έλλειψη σχεδίου Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan)	Medium (M)
				Έλλειψη εφεδρικού υπολογιστικού κέντρου ή σύμβασης με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών	Medium (M)
				Τα συστήματα που περιλαμβάνονται στο Σχέδιο Ανάκαμψης από Καταστροφή δεν καλύπτουν πλήρως τα κρίσιμα πληροφοριακά συστήματα, όπως προκύπτουν από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας	Medium (M)
				Το Σχέδιο Ανάκαμψης από Καταστροφή δεν δοκιμάζεται και δεν ανανεώνεται σε τακτά χρονικά διαστήματα	Low (L)
	Computer Room	Πυρκαγιά	Low (L)	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	Low (L)
				Ελλιπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	Low (L)
	Computer Room	Πλημμύρα	Low (L)	Κρίσιμος εξοπλισμός δεν είναι καλυμμένος με αδιάβροχα καλύμματα	Low (L)
	Computer Room	Καιρικά φαινόμενα /	Low (L)	Έλλειψη πολιτικών και διαδικασιών που αφορούν	Low (L)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
		Ακραίες συνθήκες		τον έλεγχο των περιβαλλοντολογικών κινδύνων και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ.);	
	Computer Room	Διακοπή ηλεκτροδότησης	Low (L)	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας	Medium (M)
	Computer Room	Δολιοφθορά (Sabotage)	Low (L)	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	Low (L)
8	AA1/AA2	Πυρκαγιά	Low (L)	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	Low (L)
				Ελλιπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	Low (L)
	AA1/AA2	Πλημμύρα	Low (L)	Κρίσιμος εξοπλισμός δεν είναι καλυμμένος με αδιάβροχα καλύμματα	Low (L)
	AA1/AA2	Καιρικά φαινόμενα / Ακραίες συνθήκες	Low (L)	Έλλειψη πολιτικών και διαδικασιών που αφορούν τον έλεγχο των περιβαλλοντολογικών κινδύνων και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ);	Low (L)
	AA1/AA2	Διακοπή ηλεκτροδότησης	Low (L)	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας	Medium (M)
	AA1/AA2	Δολιοφθορά (Sabotage)	Low (L)	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	Low (L)
9	QNAP	Τεχνικές Βλάβες και Αστοχίες	Medium (M)	Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	Low (L)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
				Ελλιπής συντήρηση των εξυπηρετητών	Medium (M)
	QNAP	Σφάλμα χειρισμού και διαχείρησης	Low (L)	Απουσία μηχανισμών ελέγχου	Low (L)
	QNAP	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Low (L)	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	Low (L)
10	Debian-based SW	Κακόβουλο Λογισμικό (Malicious Code)	Medium (M)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	Low (L)
				Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	Medium (M)
				Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	Medium (M)
	Debian-based SW	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	High (H)	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	Medium (M)
	Debian-based SW	Δικτυακή εισβολή (network intrusion)	Medium (M)	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	Medium (M)
	Debian-based SW	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος	Medium (M)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	Medium (M)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
		(Administration missuse)		Έλλειψη αντιγράφων επαναφοράς του συστήματος	Medium (M)
	Debian-based SW	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Medium (M)	Ελλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	Medium (M)
11	Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Τεχνικές Βλάβες και Αστοχίες	Low (L)	Ύπαρξη πεπαλαιωμένου εξοπλισμού	Low (L)
	Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Σφάλμα χειρισμού	Low (L)	Εργασία υπό πίεση	Low (L)
				Απουσία μηχανισμών ελέγχου	Low (L)
12	Windows 10	Κακόβουλο Λογισμικό (Malicious Code)	Medium (M)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	Low (L)
				Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	Medium (M)
				Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	Medium (M)
	Windows 10	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	High (H)	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	Medium (M)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
	Windows 10	Δικτυακή εισβολή (network intrusion)	Medium (M)	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	Medium (M)
	Windows 10	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration missuse)	Low (L)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	Medium (M)
				Έλλειψη αντιγράφων επαναφοράς του συστήματος	Medium (M)
	Windows 10	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Medium (M)	Έλλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	Medium (M)
13	FortiGate 200f	Τεχνικές Βλάβες και Αστοχίες	Medium (M)	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβών	Low (L)
	FortiGate 200f	Σφάλμα χειρισμού και συντήρησης	Medium (M)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	Low (L)
				Εργασία υπό πίεση	Medium (M)
	FortiGate 200f	Άρνηση Υπηρεσίας (Denial of Service)	Low (L)	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	Medium (M)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
	FortiGate 200f	Παρακολούθηση επικοινωνιών	Low (L)	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	Low (L)
14	FortiSwitch 124D-POE	Τεχνικές Βλάβες και Αστοχίες	Medium (M)	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβών	Low (L)
	FortiSwitch 124D-POE	Σφάλμα χειρισμού και συντήρησης	Medium (M)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	Low (L)
				Εργασία υπό πίεση	Medium (M)
	FortiSwitch 124D-POE	Άρνηση Υπηρεσίας (Denial of Service)	Low (L)	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	Medium (M)
	FortiSwitch 124D-POE	Παρακολούθηση επικοινωνιών	Low (L)	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	Low (L)
	FortiSwitch 124D-POE	Κλοπή	Low (L)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	Low (L)
15	DELL PowerEdge T420/T630	Τεχνικές Βλάβες και Αστοχίες	Medium (M)	Ύπαρξη πεπαλαιωμένων εξυπηρετητών	Medium (M)
				Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	Low (L)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
				Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	Medium (M)
				Ανεπαρκής εποπτεία της λειτουργίας των εξυπηρετητών	Low (L)
				Ελλιπής συντήρηση των εξυπηρετητών	Medium (M)
	DELL PowerEdge T420/T630	Σφάλμα χειρισμού και διαχείρησης	Low (L)	Έλλειψη αξιολόγησης διαχειριστών	Low (L)
				Εργασία υπό πίεση	Low (L)
				Απουσία μηχανισμών ελέγχου	Low (L)
	DELL PowerEdge T420/T630	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	High (H)	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	Medium (M)
				Χρήση εξυπηρετητή για περισσότερες από μία υπηρεσίες	Medium (M)
				Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές	Low (L)
16	Apache / php 7	Επίθεση XSS	Medium (M)	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation)	Medium (M)
				Μη χρήση συναρτήσεων μετατροπής ειδικών χαρακτήρων σε απλή html	Low (L)
				Μη χρήση τεχνικών αφαίρεσης μη έγκυρων ετικετών html	Medium (M)
				Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	Medium (M)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
	Apache / php 7	Επίθεση sql injection	Medium (M)	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ. και στη βάση να περνούν μόνο έγκυρα πεδία)	Medium (M)
				Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner	Medium (M)
	Apache / php 7	Εσφαλμένη διαχείριση εφαρμογής	Low (L)	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	Low (L)
				Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	Medium (M)
				Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	Medium (M)
17	Ubuntu 16.04/Windows Server 2012 R2	Κακόβουλο Λογισμικό (Malicious Code)	Low (L)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	Low (L)
				Ανεπαρκής έλεγχος και επισκόπηση των αρχείων καταγραφής.	Low (L)
				Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	Medium (M)
	Ubuntu 16.04/Windows Server 2012 R2	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration missuse)	Low (L)	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών	Medium (M)
				Έλλειψη αντιγράφων επαναφοράς του συστήματος	Medium (M)

#	Όνομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Όνομα Αδυναμίας	Επίπεδο Αδυναμίας
18	MySQL/MariaDB	Επίθεση κλοπής/ αλλοίωσης δεδομένων	Medium (M)	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	Medium (M)
				Μη χρήση μηχανισμών ελέγχου ακεραιότητας των ευαίσθητων δεδομένων	Medium (M)
	MySQL/MariaDB	Επίθεση sql injection	Medium (M)	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ. και στη βάση να περνούν μόνο έγκυρα πεδία….)	Medium (M)
				Έλλειψη ελέγχου ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.	Low (L)
	MySQL/MariaDB	Εσφαλμένη διαχείριση εφαρμογής	Low (L)	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	Low (L)
				Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	Medium (M)
				Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)	Medium (M)

Πίνακας 11: Απειλές και αδυναμίες ανά αγαθό

4.6 Εκτίμηση επικινδυνότητας

Στην συγκεκριμένη ενότητα παρουσιάζονται τα αγαθά για τα οποία υπολογίστηκε ο βαθμός επικινδυνότητας ανά απειλή.

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
1	Προσωπικά δεδομένα & συνεργατών	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	5
			Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	5

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
			Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	5
			Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	5
2	Δεδομένα για έρευνα & ανάλυση	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	6
			Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	6
			Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	6
			Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	6
3	Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	3
			Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	3
			Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	3
			Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	3
4	Δεδομένα back-up συστήματος	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	3
			Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	3
			Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	3
			Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	3
5	Δεδομένα παραμετροποίησης	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	4
			Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	4
			Μη διαθεσιμότητα αντιγράφων	4

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
			ασφαλείας για κρίσιμα δεδομένα	
			Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	4
6	Δεδομένα Αυθεντικοποίησης	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	5
			Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	5
			Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	5
			Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	5
7	Computer Room	Μη έγκαιρη αποκατάσταση πληροφοριακών συστημάτων	Έλλειψη σχεδίου Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan)	5
			Έλλειψη εφεδρικού υπολογιστικού κέντρου ή σύμβασης με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών	5
			Τα συστήματα που περιλαμβάνονται στο Σχέδιο Ανάκαμψης από Καταστροφή δεν καλύπτουν πλήρως τα κρίσιμα πληροφοριακά συστήματα, όπως προκύπτουν από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας	5
			Το Σχέδιο Ανάκαμψης από Καταστροφή δεν δοκιμάζεται και δεν ανανεώνεται σε τακτά χρονικά διαστήματα	4
	Computer Room	Πυρκαγιά	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	4
			Ελλιπής εκπαίδευση προσωπικού σε ζητήματα	4

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
			πυρόσβεσης και πυροπροστασίας	
	Computer Room	Πλημμύρα	Κρίσιμος εξοπλισμός δεν είναι καλυμμένος με αδιάβροχα καλύμματα	4
	Computer Room	Καιρικά φαινόμενα / Ακραίες συνθήκες	Έλλειψη πολιτικών και διαδικασιών που αφορούν τον έλεγχο των περιβαλλοντολογικών κινδύνων και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ.);	4
	Computer Room	Διακοπή ηλεκτροδότησης	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας	5
	Computer Room	Δολιοφθορά (Sabotage)	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	4
8	AA1/AA2	Πυρκαγιά	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	3
			Ελλιπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	3
	AA1/AA2	Πλημμύρα	Κρίσιμος εξοπλισμός δεν είναι καλυμμένος με αδιάβροχα καλύμματα	3
	AA1/AA2	Καιρικά φαινόμενα / Ακραίες συνθήκες	Έλλειψη πολιτικών και διαδικασιών που αφορούν τον έλεγχο των περιβαλλοντολογικών κινδύνων και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ.);	3
	AA1/AA2	Διακοπή ηλεκτροδότησης	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας	4
	AA1/AA2	Δολιοφθορά (Sabotage)	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	3

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
9	QNAP	Τεχνικές Βλάβες και Αστοχίες	Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	5
			Ελλιπής συντήρηση των εξυπηρετητών	6
	QNAP	Σφάλμα χειρισμού και διαχείρισης	Απουσία μηχανισμών ελέγχου	4
	QNAP	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	4
10	Debian-based SW	Κακόβουλο Λογισμικό (Malicious Code)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	5
			Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	6
			Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	6
	Debian-based SW	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	7
	Debian-based SW	Δικτυακή εισβολή (network intrusion)	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	6
	Debian-based SW	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration missuse)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	6
			Έλλειψη αντιγράφων επαναφοράς του συστήματος	6

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
	Debian-based SW	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Έλλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	6
11	Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένου εξοπλισμού	4
	Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Σφάλμα χειρισμού	Εργασία υπό πίεση	4
			Απουσία μηχανισμών ελέγχου	4
12	Windows 10	Κακόβουλο Λογισμικό (Malicious Code)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	5
			Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	6
			Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	6
	Windows 10	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	7
	Windows 10	Δικτυακή εισβολή (network intrusion)	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	6
	Windows 10	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration misuse)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	5
			Έλλειψη αντιγράφων επαναφοράς του συστήματος	5

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
	Windows 10	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Έλλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	6
13	FortiGate 200f	Τεχνικές Βλάβες και Αστοχίες	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβών	5
	FortiGate 200f	Σφάλμα χειρισμού και συντήρησης	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	5
			Εργασία υπό πίεση	6
	FortiGate 200f	Άρνηση Υπηρεσίας (Denial of Service)	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	5
	FortiGate 200f	Παρακολούθηση επικοινωνιών	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	4
14	FortiSwitch 124D-POE	Τεχνικές Βλάβες και Αστοχίες	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβών	5
	FortiSwitch 124D-POE	Σφάλμα χειρισμού και συντήρησης	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	1
			Εργασία υπό πίεση	2
	FortiSwitch 124D-POE	Άρνηση Υπηρεσίας (Denial of Service)	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	5
	FortiSwitch 124D-POE	Παρακολούθηση επικοινωνιών	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις	4

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
			εγκαταστάσεις του οργανισμού	
	FortiSwitch 124D-POE	Κλοπή	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	4
15	DELL PowerEdge T420/T630	Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένων εξυπηρετητών	6
			Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	5
			Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	6
			Ανεπαρκής εποπτεία της λειτουργίας των εξυπηρετητών	5
			Ελλιπής συντήρηση των εξυπηρετητών	6
	DELL PowerEdge T420/T630	Σφάλμα χειρισμού και διαχείρισης	Έλλειψη αξιολόγησης διαχειριστών	4
			Εργασία υπό πίεση	4
			Απουσία μηχανισμών ελέγχου	4
	DELL PowerEdge T420/T630	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	7
			Χρήση εξυπηρετητή για περισσότερες από μία υπηρεσίες	7
			Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές	6
16	Apache / php 7	Επίθεση XSS	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation)	6
			Μη χρήση συναρτήσεων μετατροπής ειδικών χαρακτήρων σε απλή html	5
			Μη χρήση τεχνικών αφαίρεσης μη	6

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
			έγκυρων ετικετών html	
			Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	6
	Apache / php 7	Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ και στη βάση να περνούν μόνο έγκυρα πεδία)	6
			Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner	6
	Apache / php 7	Εσφαλμένη διαχείριση εφαρμογής	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	4
			Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	5
			Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	5
17	Ubuntu 16.04/Windows Server 2012 R2	Κακόβουλο Λογισμικό (Malicious Code)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	4
			Ανεπαρκής έλεγχος και επισκόπηση των αρχείων καταγραφής.	4
			Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	5
	Ubuntu 16.04/Windows Server 2012 R2	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών	5

#	Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Βαθμός Επικινδυνότητας
		συστήματος (Administration misuse)	Έλλειψη αντιγράφων επαναφοράς του συστήματος	5
18	MySQL/MariaDB	Επίθεση κλοπής/ αλλοίωσης δεδομένων	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	6
			Μη χρήση μηχανισμών ελέγχου ακεραιότητας των ευαίσθητων δεδομένων	6
	MySQL/MariaDB	Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ. και στη βάση να περνούν μόνο έγκυρα πεδία….)	6
			Έλλειψη ελέγχου ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.	5
	MySQL/MariaDB	Εσφαλμένη διαχείριση εφαρμογής	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	4
			Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	5
			Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)	5

4.7 Διαχείριση Επικινδυνότητας

4.7.1 Στρατηγική αντιμετώπισης κινδύνου

Στην ενότητα αυτή ορίζεται η στρατηγική αντιμετώπισης κινδύνου σύμφωνα με τα αποτελέσματα.

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
Προσωπικά δεδομένα & συνεργατών	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
Δεδομένα για έρευνα & ανάλυση	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	HIGH	ΜΕΤΑΦΟΡΑ
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΑΠΟΔΟΧΗ
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
Δεδομένα back-up συστήματος	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΑΦΟΡΑ
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΑΠΟΔΟΧΗ
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
Δεδομένα παραμετροποίησης	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΑΠΟΔΟΧΗ
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
Δεδομένα Αυθεντικοποίησης	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΑΠΟΔΟΧΗ
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
Computer Room	Μη έγκαιρη αποκατάσταση πληροφοριακών συστημάτων	Έλλειψη σχεδίου Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη εφεδρικού υπολογιστικού κέντρου ή σύμβασης με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών	MEDIUM	ΜΕΤΑΦΟΡΑ
		Τα συστήματα που περιλαμβάνονται στο Σχέδιο Ανάκαμψης από Καταστροφή δεν καλύπτουν πλήρως τα κρίσιμα πληροφοριακά συστήματα, όπως προκύπτουν από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Το Σχέδιο Ανάκαμψης από Καταστροφή δεν δοκιμάζεται και δεν ανανεώνεται σε τακτά χρονικά διαστήματα	MEDIUM	ΑΠΟΔΟΧΗ
Computer Room	Πυρκαγιά	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	MEDIUM	ΜΕΤΑΦΟΡΑ
		Ελλιπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	MEDIUM	ΜΕΤΑΦΟΡΑ
Computer Room	Πλημμύρα	Κρίσιμος εξοπλισμός δεν είναι καλυμμένος με αδιάβροχα καλύμματα	MEDIUM	ΜΕΤΑΦΟΡΑ

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
Computer Room	Καιρικά φαινόμενα / Ακραίες συνθήκες	Έλλειψη πολιτικών και διαδικασιών που αφορούν τον έλεγχο των περιβαλλοντολογικών κινδύνων και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ);	MEDIUM	ΑΠΟΔΟΧΗ
Computer Room	Διακοπή ηλεκτροδότησης	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας	MEDIUM	ΜΕΤΑΦΟΡΑ
Computer Room	Δολιοφθορά (Sabotage)	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
AA1/AA2	Πυρκαγιά	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	MEDIUM	ΑΠΟΔΟΧΗ
		Ελλειπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	MEDIUM	ΑΠΟΔΟΧΗ
AA1/AA2	Πλημμυρα	Κρίσιμος εξοπλισμός δεν είναι καλυμένος με αδιάβροχα καλύματα	MEDIUM	ΑΠΟΔΟΧΗ
AA1/AA2	Καιρικά φαινόμενα / Ακραίες συνθήκες	Έλλειψη πολιτικών και διαδικασιών που αφορούν τον έλεγχο των περιβαλοντολογικών κινδύνων και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ);	MEDIUM	ΑΠΟΔΟΧΗ
AA1/AA2	Διακοπή ηλεκτροδότησης	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας	MEDIUM	ΜΕΤΑΦΟΡΑ
AA1/AA2	Δολιοφθορά (Sabotage)	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	MEDIUM	ΑΠΟΔΟΧΗ
QNAP	Τεχνικές Βλάβες και Αστοχίες	Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Ελλιπής συντήρηση των εξυπηρετητών	HIGH	ΜΕΤΡΙΑΣΜΟΣ
QNAP	Σφάλμα χειρισμού και διαχείρησης	Απουσία μηχανισμών ελέγχου	MEDIUM	ΑΠΟΔΟΧΗ

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
QNAP	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	MEDIUM	ΑΠΟΔΟΧΗ
Debian-based SW	Κακόβουλο Λογισμικό (Malicious Code)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	HIGH	ΜΕΤΑΦΟΡΑ
Debian-based SW	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Debian-based SW	Δικτυακή εισβολή (network intrusion)	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Debian-based SW	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration misuse)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη αντιγράφων επαναφοράς του συστήματος	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Debian-based SW	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Έλλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	HIGH	ΑΠΟΔΟΧΗ
Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένου εξοπλισμού	MEDIUM	ΑΠΟΔΟΧΗ

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Σφάλμα χειρισμού	Εργασία υπό πίεση	MEDIUM	ΑΠΟΔΟΧΗ
		Απουσία μηχανισμών ελέγχου	MEDIUM	ΑΠΟΔΟΧΗ
Windows 10	Κακόβουλο Λογισμικό (Malicious Code)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
		Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	HIGH	ΜΕΤΑΦΟΡΑ
Windows 10	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Windows 10	Δικτυακή εισβολή (network intrusion)	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Windows 10	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration missuse)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη αντιγράφων επαναφοράς του συστήματος	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
Windows 10	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Ελλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	HIGH	ΑΠΟΔΟΧΗ
FortiGate 200f	Τεχνικές Βλάβες και Αστοχίες	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων	MEDIUM	ΑΠΟΔΟΧΗ
FortiGate 200f	Σφάλμα χειρισμού και συντήρησης	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ
		Εργασία υπό πίεση	HIGH	ΜΕΤΡΙΑΣΜΟΣ

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
FortiGate 200f	Άρνηση Υπηρεσίας (Denial of Service)	Ελλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
FortiGate 200f	Παρακολούθηση επικοινωνιών	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού	MEDIUM	ΑΠΟΔΟΧΗ
FortiSwitch 124D-POE	Τεχνικές Βλάβες και Αστοχίες	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
FortiSwitch 124D-POE	Σφάλμα χειρισμού και συντήρησης	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	LOW	ΑΠΟΔΟΧΗ
		Εργασία υπό πίεση	LOW	ΑΠΟΔΟΧΗ
FortiSwitch 124D-POE	Άρνηση Υπηρεσίας (Denial of Service)	Ελλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
FortiSwitch 124D-POE	Παρακολούθηση επικοινωνιών	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού	MEDIUM	ΑΠΟΔΟΧΗ
FortiSwitch 124D-POE	Κλοπή	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
DELL PowerEdge T420/T630	Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένων εξυπηρετητών	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Ανεπαρκής εποπτεία της λειτουργίας των εξυπηρετητών	MEDIUM	ΜΕΤΑΦΟΡΑ

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
		Ελλιπής συντήρηση των εξυπηρετητών	HIGH	ΜΕΤΑΦΟΡΑ
DELL PowerEdge T420/T630	Σφάλμα χειρισμού και διαχείρησης	Έλλειψη αξιολόγησης διαχειριστών	MEDIUM	ΑΠΟΔΟΧΗ
		Εργασία υπό πίεση	MEDIUM	ΑΠΟΔΟΧΗ
		Απουσία μηχανισμών ελέγχου	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
DELL PowerEdge T420/T630	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Ελλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Χρήση εξυπηρετητή για περισσότερες από μία υπηρεσίες	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Apache / php 7	Επίθεση XSS	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation)	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Μη χρήση συναρτήσεων μετατροπής ειδικών χαρακτήτων σε απλή html	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Μη χρήση τεχνικών αφαίρεσης μη έγκυρων ετικετών html	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Apache / php 7	Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ και στη βάση να περνούν μόνο έγκυρα πεδία)	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner	HIGH	ΜΕΤΡΙΑΣΜΟΣ
Apache / php 7	Εσφαλμένη διαχείριση εφαρμογής	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
Ubuntu 16.04/Windows Server 2012 R2	Κακόβουλο Λογισμικό (Malicious Code)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Ανεπαρκής έλεγχος και επισκόπιση των αρχείων καταγραφής.	MEDIUM	ΑΠΟΔΟΧΗ
		Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	MEDIUM	ΜΕΤΑΦΟΡΑ
Ubuntu 16.04/Windows Server 2012 R2	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration missuse)	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη αντιγράφων επαναφοράς του συστήματος	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
MySQL/MariaDB	Επίθεση κλοπής/ αλλοίωσης δεδομένων	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Μη χρήση μηχανισμών ελέγχου ακεραιότητας των ευαίσθητων δεδομένων	HIGH	ΜΕΤΡΙΑΣΜΟΣ
MySQL/MariaDB	Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ και στη βάση να περνούν μόνο έγκυρα πεδία….)	HIGH	ΜΕΤΡΙΑΣΜΟΣ
		Έλλειψη ελέγχου ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
MySQL/MariaDB	Εσφαλμένη διαχείριση εφαρμογής	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	MEDIUM	ΑΠΟΔΟΧΗ
		Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ
		Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική
		δημιουργήσουν νέο λογαριασμό χρήστη)		

4.7.2 Σχέδιο διαχείρισης κινδύνου

Παρακάτω ορίζονται τα προτεινόμενα μέτρα ασφάλειας και το σχέδιο διαχείρισης κινδύνου:

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
Προσωπικά δεδομένα & συνεργατών	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 2	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 2	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Δεδομένα για έρευνα & ανάλυση	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	HIGH	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΑΜΕΣΑ	LOW
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Δεδομένα back-up συστήματος	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Δεδομένα παραμετροποίησης	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 2	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Δεδομένα Αυθεντικοποίησης	Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
Computer Room	Μη έγκαιρη αποκατάσταση πληροφοριακών συστημάτων	Έλλειψη σχεδίου Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Έλλειψη εφεδρικού υπολογιστικού κέντρου ή σύμβασης με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΑΜΕΣΑ	LOW
		Τα συστήματα που περιλαμβάνονται στο Σχέδιο Ανάκαμψης από Καταστροφή δεν καλύπτουν πλήρως τα κρίσιμα πληροφοριακά συστήματα, όπως προκύπτουν από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Το Σχέδιο Ανάκαμψης από Καταστροφή δεν δοκιμάζεται και δεν ανανεώνεται σε τακτά χρονικά διαστήματα	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Computer Room	Πυρκαγιά	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Ελλιπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
Computer Room	Πλημμύρα	Κρίσιμος εξοπλισμός δεν είναι καλυμμένος με αδιάβροχα καλύμματα	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
Computer Room	Καιρικά φαινόμενα / Ακραίες συνθήκες	Έλλειψη πολιτικών και διαδικασιών που αφορούν τον έλεγχο των περιβαλλοντολογικών κινδύνων και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ);	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Computer Room	Διακοπή ηλεκτροδότησης	Έλλειψη εναλλακτικών μεθόδων	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΤΟΥΣ ΕΠΟΜΕΝΟ	LOW

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
		παροχής ηλεκτρικής ενέργειας				ΥΣ 6 ΜΗΝΕΣ	
Computer Room	Δολιοφθορά (Sabotage)	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
AA1/AA2	Πυρκαγιά	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Ελλιπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
AA1/AA2	Πλημμύρα	Κρίσιμος εξοπλισμός δεν είναι καλυμμένος με αδιάβροχα καλύμματα	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
AA1/AA2	Καιρικά φαινόμενα / Ακραίες συνθήκες	Έλλειψη πολιτικών και διαδικασιών που αφορούν τον έλεγχο των περιβαλλοντολογικών κινδύνων και την αντιμετώπιση τους (π.χ. καταιγίδες, παλιρροϊκό κύμα, ακραίες θερμοκρασίες κτλ);	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
AA1/AA2	Διακοπή ηλεκτροδότησης	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
AA1/AA2	Δολιοφθορά (Sabotage)	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
QNAP	Τεχνικές Βλάβες και Αστοχίες	Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW
		Ελλιπής συντήρηση των εξυπηρετητών	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW
QNAP	Σφάλμα χειρισμού και διαχείρισης	Απουσία μηχανισμών ελέγχου	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
QNAP	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Debian-based SW	Κακόβουλο Λογισμικό (Malicious Code)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
		Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW
		Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	HIGH	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΑΜΕΣΑ	MEDIUM
Debian-based SW	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	MEDIUM
Debian-based SW	Δικτυακή εισβολή (network intrusion)	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
Debian-based SW	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration misuse)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW
		Έλλειψη αντιγράφων επαναφοράς του συστήματος	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
Debian-based SW	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Έλλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	HIGH	ΑΠΟΔΟΧΗ			HIGH
Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένου εξοπλισμού	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Dell XPS/ DELL Workstation PC Precision 3430/DELL XPS Tower	Σφάλμα χειρισμού	Εργασία υπό πίεση	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Απουσία μηχανισμών ελέγχου	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
Windows 10	Κακόβουλο Λογισμικό (Malicious Code)	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΑΜΕΣΑ	LOW
		Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	HIGH	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΑΜΕΣΑ	MEDIUM
Windows 10	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΑΜΕΣΑ	MEDIUM
Windows 10	Δικτυακή εισβολή (network intrusion)	Έλλειψη διαδικασίας τακτικής ενημέρωσης των συστημάτων με τις πρόσφατες διορθώσεις αδυναμιών του κατασκευαστή (patch management)	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
Windows 10	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration misuse)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Έλλειψη αντιγράφων επαναφοράς του συστήματος	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
Windows 10	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Έλλειψη μηχανισμού πρόληψης διαρροής δεδομένων (Data Leak Prevention - DLPs)	HIGH	ΑΠΟΔΟΧΗ			HIGH
FortiGate 200f	Τεχνικές Βλάβες και Αστοχίες	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβών	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
FortiGate 200f	Σφάλμα χειρισμού και συντήρησης	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Εργασία υπό πίεση	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	MEDIUM
FortiGate 200f	Άρνηση Υπηρεσίας (Denial of Service)	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
FortiGate 200f	Παρακολούθηση επικοινωνιών	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
FortiSwitch 124D-POE	Τεχνικές Βλάβες και Αστοχίες	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβών	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
FortiSwitch 124D-POE	Σφάλμα χειρισμού και συντήρησης	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας	LOW	ΑΠΟΔΟΧΗ			LOW
		Εργασία υπό πίεση	LOW	ΑΠΟΔΟΧΗ			LOW

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
FortiSwitch 124D-POE	Άρνηση Υπηρεσίας (Denial of Service)	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
FortiSwitch 124D-POE	Παρακολούθηση επικοινωνιών	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
FortiSwitch 124D-POE	Κλοπή	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
DELL PowerEdge T420/T630	Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένων εξυπηρετητών	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	MEDIUM
		Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	MEDIUM
		Ανεπαρκής εποπτεία της λειτουργίας των εξυπηρετητών	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΑΜΕΣΑ	LOW
		Ελλιπής συντήρηση των εξυπηρετητών	HIGH	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΑΜΕΣΑ	LOW
DELL PowerEdge T420/T630	Σφάλμα χειρισμού και διαχείρησης	Έλλειψη αξιολόγησης διαχειριστών	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Εργασία υπό πίεση	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Απουσία μηχανισμών ελέγχου	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
DELL PowerEdge T420/T630	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Έλλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	MEDIUM
		Χρήση εξυπηρετητή για περισσότερες από μία υπηρεσίες	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	MEDIUM
		Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
Apache / php 7	Επίθεση XSS	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation)	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
		Μη χρήση συναρτήσεων μετατροπής ειδικών χαρακτήρων σε απλή html	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Μη χρήση τεχνικών αφαίρεσης μη έγκυρων ετικετών html	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
Apache / php 7	Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ. και στη βάση να περνούν μόνο έγκυρα πεδία)	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
Apache / php 7	Εσφαλμένη διαχείριση εφαρμογής	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
		Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW
Ubuntu 16.04/Windows Server 2012 R2	Κακόβουλο Λογισμικό (Malicious Code)	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 1	ΑΜΕΣΑ	LOW

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
		Ανεπαρκής έλεγχος και επισκόπηση των αρχείων καταγραφής.	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)	MEDIUM	ΜΕΤΑΦΟΡΑ	Εξ. Συνεργάτης	ΑΜΕΣΑ	LOW
Ubuntu 16.04/Windows Server 2012 R2	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration misuse)	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
		Έλλειψη αντιγράφων επαναφοράς του συστήματος	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ	LOW
MySQL/MariaDB	Επίθεση κλοπής/ αλλοίωσης δεδομένων	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	MEDIUM
		Μη χρήση μηχανισμών ελέγχου ακεραιότητας των ευαίσθητων δεδομένων	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	MEDIUM
MySQL/MariaDB	Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ. και στη βάση να περνούν μόνο έγκυρα πεδία….)	HIGH	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
		Έλλειψη ελέγχου ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	LOW
MySQL/MariaDB	Εσφαλμένη διαχείριση εφαρμογής	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)	MEDIUM	ΑΠΟΔΟΧΗ			MEDIUM
		Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΑΜΕΣΑ	LOW

Όνομα Αγαθού	Όνομα Απειλής	Όνομα Αδυναμίας	Επίπεδο Επικινδυνότητας	Στρατηγική	Υπεύθυνος Υλοποίησης	Χρόνος Υλοποίησης	Εναπομένων Κίνδυνος Residual Risk
		Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)	MEDIUM	ΜΕΤΡΙΑΣΜΟΣ	ADMIN 3	ΑΜΕΣΑ	LOW

Κεφάλαιο 5

Εκπόνηση Εκτίμησης Αντικτύπου σχετικά με προστασία δεδομένων

Στο προηγούμενο κεφάλαιο πραγματοποιήθηκε μία συνολική διαχείριση κινδύνων για τον οργανισμό. Όπως αναφέρθηκε, μία διαχείριση κινδύνων πραγματοποιείται εφαρμόζοντας μια γνωστή μεθοδολογία. Στο παρόν κεφάλαιο θα γίνει αξιοποίηση και ενσωμάτωση μιας ΕΑΠΔ ως προς το τμήμα των κινδύνων ασφάλειας. Στο παρόν κεφάλαιο θα διενεργηθεί η ΕΑΠΔ στον εν λόγω οργανισμό: για το σκοπό αυτό, θα αξιοποιηθεί ένα κατάλληλο λογισμικό ανοιχτού κώδικα για την διεξαγωγή αξιολόγησης προστασίας δεδομένων για τον ΓΚΠΔ. Το λογισμικό αυτό έχει τη δυνατότητα να αναλύει με σαφήνεια τη μεθοδολογία εκτίμησης αντικτύπου οπτικοποιώντας τα δεδομένα προσφέροντας έτσι τη γρήγορη κατανόηση των κινδύνων. Αυτό φυσικά δίνει τη δυνατότητα σε αυτόν που διενεργεί την ΕΑΠΔ να επιτύχει ένα σωστό αποτέλεσμα. Το λογισμικό αυτό είναι ελεύθερα διαθέσιμο από τη Γαλλική Αρχή Προστασίας Δεδομένων.

5.1 Εκτίμηση Αντικτύπου Privacy Impact Assessment (PIA)

Η μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Commission nationale de l'informatique et des libertés – CNIL [3]) είναι μια μεθοδολογία επαναληπτικής διαδικασίας που θα πρέπει να εγγυάται μια αιτιολογημένη και αξιόπιστη χρήση των προσωπικών δεδομένων κατά τη διάρκεια της επεξεργασίας. Εκτελούμενη κατ' αρχήν από υπεύθυνο επεξεργασίας δεδομένων, ο σκοπός μιας PIA είναι να δημιουργηθεί και να αποδειχθεί η εφαρμογή των αρχών για την προστασία της ιδιωτικότητας, ώστε τα υποκείμενα των δεδομένων

[3] Commission nationale de l'informatique et des libertés – CNIL https://www.cnil.fr/en/home

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

1. αρχές λήψης αποφάσεων οι οποίες αναθέτουν και επικυρώνουν τη δημιουργία νέων επεξεργασιών προσωπικών δεδομένων ή προϊόντων

2. ιδιοκτήτες έργων, οι οποίοι πρέπει να διενεργούν αξιολόγηση των κινδύνων για τα συστήματά τους και να ορίζουν τους στόχους ασφαλείας

3. κύριους εργολάβους, οι οποίοι πρέπει να προτείνουν λύσεις για την αντιμετώπιση των κινδύνων σύμφωνα με τους στόχους που προσδιορίζονται από τους ιδιοκτήτες έργων

4. υπεύθυνους προστασίας δεδομένων (ΥΠΔ), οι οποίοι πρέπει να υποστηρίζουν τους ιδιοκτήτες έργων και τις αρχές λήψης αποφάσεων στον τομέα της προστασίας των προσωπικών δεδομένων υπεύθυνους ασφάλειας κεντρικών συστημάτων πληροφορικής (ΥΑΚΠ – CISO), οι οποίοι πρέπει να υποστηρίξουν τους ιδιοκτήτες έργων στον τομέα της ασφάλειας των πληροφοριών (IS).

Η προσέγγιση συμμόρφωσης που εφαρμόζεται με τη διεξαγωγή μιας PIA βασίζεται σε δύο πυλώνες [8]:

1. τα θεμελιώδη δικαιώματα και αρχές, τα οποία είναι «μη διαπραγματεύσιμα», θεσπίζονται από τον νόμο και τα οποία πρέπει να τηρούνται, ανεξάρτητα από τη φύση, τη σοβαρότητα και την πιθανότητα κινδύνων

2. τη διαχείριση των κινδύνων ιδιωτικής ζωής των υποκειμένων των δεδομένων, η οποία καθορίζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων.

Εικόνα 2: Προσέγγιση συμμόρφωσης με τη χρήση PIA

Συνοψίζοντας, για να διενεργηθεί μια PIA είναι απαραίτητο να:

1. καθοριστεί και περιγραφεί τις περιστάσεις της επεξεργασίας των υπό εξέταση δεδομένων προσωπικού χαρακτήρα

2. αναλυθούν τα μέτρα που εγγυώνται τη συμμόρφωση με τις θεμελιώδεις αρχές: την αναλογικότητα και την αναγκαιότητα της επεξεργασίας και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων·

3. αξιολογηθούν οι κίνδυνοι για την προστασία της ιδιωτικότητας που συνδέονται με την ασφάλεια των δεδομένων και διασφαλιστεί ότι αντιμετωπίζονται κατάλληλα·

4. τεκμηριωθεί επισήμως η επικύρωση της PIA εν όψει των προηγούμενων διαθέσιμων στοιχείων ή αποφασιστεί η αναθεώρηση των προηγούμενων βημάτων.

Εικόνα 3: Γενική προσέγγιση για τη διενέργεια μιας PIA

Πρόκειται για μια διαδικασία συνεχούς βελτίωσης και αυτό σημαίνει ότι μερικές φορές απαιτούνται αρκετές επαναλήψεις για να επιτευχθεί ένα αποδεκτό σύστημα προστασίας της ιδιωτικότητας. Απαιτείται επίσης η παρακολούθηση των αλλαγών με την πάροδο του χρόνου (στις περιστάσεις, τα μέτρα, τους κινδύνους κ.λπ.), για παράδειγμα, κάθε έτος, και επικαιροποίηση κάθε φορά που συμβαίνει μια σημαντική αλλαγή. Η προσέγγιση πρέπει να υλοποιείται μόλις σχεδιαστεί μια νέα επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η εξαρχής υλοποίηση αυτής της προσέγγισης καθιστά δυνατό τον καθορισμό αναγκαίων και επαρκών μέτρων και, κατά συνέπεια, τη βελτιστοποίηση του κόστους. Αντίθετα, η υλοποίησή της μετά τη δημιουργία του συστήματος και την υλοποίηση των μέτρων μπορεί να θέσει υπό αμφισβήτηση τις επιλογές που έχουν γίνει.

5.2 Το λογισμικό Privacy Impact Assessment (PIA)

Το λογισμικό PIA στοχεύει στο να βοηθήσει τους υπευθύνους επεξεργασίαςνα οικοδομήσουν και να αποδείξουν τη συμμόρφωσή με το ΓΚΠΔ. Το εργαλείο του PIA παρέχεται με άδεια χρήσης ανοιχτού λογισμικού και είναι διαθέσιμο στα γαλλικά και στα αγγλικά, και διευκολύνει την εκπόνηση αξιολόγησης αντίκτυπου για την προστασία των δεδομένων, η οποία έχει καταστεί υποχρεωτική για συγκεκριμένες εργασίες επεξεργασίας δεδομένων από τις 25 Μαΐου 2018.

Το εργαλείο αυτό απευθύνεται σε υπεύθυνους επεξεργασίας δεδομένων προκειμένου να αξιοποιηθεί από τα κατάλληλα εξουσιοδοτημένα άτομα τα οποία είναι εξοικειωμένα με τη

διαδικασία αυτή. Μπορεί κάποιος να εγκαταστήσει το λογισμικό ως μεμονωμένη εφαρμογή στον υπολογιστή ή και να το ενσωματώσει ως εργαλείο στους διακομιστές ενός οργανισμού.

Το εργαλείο PIA έχει σχεδιαστεί γύρω από τρεις αρχές:

1. **Μια κοινόχρηστη διεπαφή για την εκτέλεση των PIA**: το εργαλείο βασίζεται σε φιλική προς το χρήστη διεπαφή για να επιτρέψει την απλή διαχείριση των PIA. Αναλύει με σαφήνεια τη μεθοδολογία αξιολόγησης του privacy impact assessment.

2. **Βάση νομικών και τεχνικών γνώσεων**: το εργαλείο περιλαμβάνει τα νομικά σημεία που εξασφαλίζουν τη νομιμότητα της επεξεργασίας και τα δικαιώματα των υποκειμένων των δεδομένων. Έχει επίσης μια contextual βάση γνώσεων , που είναι διαθέσιμη σε όλα τα βήματα της PIA, προσαρμόζοντας το περιεχόμενο που εμφανίζεται. Τα δεδομένα εξάγονται από τον ΓΚΠΔ, τους οδηγούς PIA και τον Οδηγό Ασφαλείας του CNIL.

3. **Ένα αρθρωτό εργαλείο**: Το PIA είναι σχεδιασμένο για να βοηθήσει τον χρήστη να οικοδομήσει τη συμμόρφωσή του, προσαρμόζοντας το εργαλείο στις συγκεκριμένες ανάγκες του καθενός. Επιπρόσθετα μιας και διανέμεται με ελεύθερη άδεια χρήσης, είναι δυνατή η τροποποίηση του πηγαίου κώδικα του εργαλείου, προκειμένου να προστεθούν λειτουργίες ή να ενσωματωθεί σε εργαλεία που χρησιμοποιούνται στον οργανισμό.

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

1. τα θεμελιώδη δικαιώματα και αρχές, τα οποία είναι «μη διαπραγματεύσιμα», θεσπίζονται από τον νόμο και τα οποία πρέπει να τηρούνται, ανεξάρτητα από τη φύση, τη σοβαρότητα και την πιθανότητα κινδύνων

2. τη διαχείριση των κινδύνων ιδιωτικής ζωής των υποκειμένων των δεδομένων, η οποία καθορίζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων.

Στα πλαίσια της παρούσας μεταπτυχιακής διατριβής παρουσιάζεται η καταγραφή των δεδομένων που συλλέγει, επεξεργάζεται και μεταδίδει η εν λόγω εταιρεία στα πλαίσια διαχείρισης ενός ευρωπαϊκού έργου.

Ακολουθώντας τα βήματα της μεθοδολογίας PIA και του διαθέσιμου εργαλείου παρακάτω παρουσιάζονται τα εξής βήματα:

5.2.1 Μελέτη των περιστάσεων (Context)

Αυτή η ενότητα παρέχει μια σαφή εικόνα της επεξεργασίας των εν λόγω προσωπικών δεδομένων.

Θα πρέπει να εφαρμοστεί μια πολιτική που θα διαχειρίζεται και θα ελέγχει την προστασία δεδομένων

Επισκόπηση (Overview): Στην επισκόπηση οι ερωτήσεις που απαντώνται είναι οι εξής:

Ερώτηση	Βοήθημα εισαγωγής	Απάντηση
Ποια είναι η υπό εξέταση επεξεργασία;	Παρουσιάστε ένα σύντομο περίγραμμα της επεξεργασίας: το όνομά του, τους σκοπούς, τα διακυβεύματα, το πλαίσιο χρήσης, κ.λπ..	Στα πλαίσια και υπό το φάσμα της συνολικής υλοποίησης και διαχείρισης ενός ευρωπαϊκού προγράμματος γίνεται καταγραφή και επεξεργασία δεδομένων όπως αυτά αποτυπώνονται σε οικονομικά στοιχεία εταίρων που εμπλέκονται στο πρόγραμμα, αριθμοί λογαριασμού, διευθύνσεις, ηλεκτρονικά ταχυδρομεία, τα ονόματα των μελών της ομάδας του κάθε εταίρου που απασχολείται στο πρόγραμμα, το προφίλ της εταιρείας, η υφιστάμενη περιορισμένης πρόσβασης γνώση που παρέχεται και διαμοιράζεται στα πλαίσια της συνεργασίας (προϋπάρχον γνωσιακό υλικό που σχετίζεται με το πρόγραμμα), φωτογραφίες και ηχογραφημένο υλικό από συνέδρια που λαμβάνουν χώρα στα πλαίσια της συνεργασίας αλλά και ερωτηματολόγια που διαμοιράζονται σε εμπειρογνώμονες εκτός της κοινοπραξίας με σκοπό την αποτύπωση των γνώσεων τους για τις ανάγκες του ευρωπαϊκού προγράμματος). Ο σκοπός της επεξεργασίας των δεδομένων είναι καθαρά για λόγους σωστής διαχείρισης του έργου

		με όλους τους συμμετέχοντες να έχουν υποβάλει τα εν λόγω ανωτέρω στοιχεία. Υπεύθυνος επεξεργασίας είναι ο ίδιος ο οργανισμός, διά του διαχειριστή του ευρωπαϊκού προγράμματος.
Ποιες είναι οι ευθύνες που συνδέονται με την επεξεργασία;	Περιγράψτε τις ευθύνες των ενδιαφερομένων: του υπεύθυνου επεξεργασίας, ενδεχομένως των εκτελούντων την επεξεργασία και των από κοινού υπεύθυνων επεξεργασίας.	Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος βάσει του συμφώνου που υπογράφει να μην διαμοιράζει προσωπικά δεδομένα αλλά και δεδομένα που είναι για περιορισμένη πρόσβαση προς τρίτους εντός και εκτός του οργανισμού. Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα (όπως η ψευδωνυμοποίηση, η ελαχιστοποίηση των δεδομένων, διαφάνεια) προκειμένου να διασφαλίζει και να αποδεικνύει ότι οποιαδήποτε επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό. Συγκεκριμένα, σε περίπτωση υποβολής ερωτηματολογίων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλες πολιτικές προστασίας δεδομένων που σχετίζονται με τον τρόπο που καταγράφονται οι πληροφορίες (έντυπη ή ηλεκτρονική μορφή), με ποιο τρόπο διατηρούνται, επεξεργάζονται, διαχέονται και τέλος αποκαλύπτονται ως αποτελέσματα έρευνας μελέτης. Επίσης ο υπεύθυνος επεξεργασίας τηρεί ηλεκτρονικό αρχείο των δραστηριοτήτων αυτών της επεξεργασίας των δεδομένων. Ο εκτελών την επεξεργασία, στην περίπτωση διαχείρισης ευρωπαϊκού έργου είναι ο κάθε εταίρος, που δεσμεύεται σε σχέση με τον υπεύθυνο επεξεργασίας να καθορίζει κάθε φορά το αντικείμενο και τη διάρκεια επεξεργασίας, τη φύση και το σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες των υποκειμένων των δεδομένων, και

		τις υποχρεώσεις και τα δικαιώματα του υπεύθυνου επεξεργασίας. Ο εκτελών την επεξεργασία τηρεί εμπιστευτικότητα και διαγράφει ή επιστρέφει όλα τα δεδομένα μετά το πέρας της παροχής υπηρεσιών ή μπορεί και να διατηρεί αρχείο μέχρις ότου να ολοκληρωθεί το πρόγραμμα (συνήθως 3 χρόνια).
Υπάρχουν πρότυπα που ισχύουν για την επεξεργασία;	Αναφέρατε τα σχετικά πρότυπα που ισχύουν για την επεξεργασία, ειδικά εγκεκριμένους κώδικες δεοντολογίας και πιστοποιήσεις προστασίας δεδομένων.	Δεν υπάρχουν πιστοποιήσεις σχετικά με την προστασία δεδομένων και δεν χρησιμοποιούνται κώδικες δεοντολογίας.

Δεδομένα, διαδικασίες και υποστηρικτικά στοιχεία (Data, Processes and Supporting Assets): Στην υποενότητα αυτή επιτρέπεται να οριστεί και να περιγραφεί λεπτομερώς το αντικείμενο της επεξεργασίας. Οι ερωτήσεις που πρέπει να απαντώνται είναι οι εξής:

Ερώτηση	Βοήθημα εισαγωγής	Απάντηση
Ποιά προσωπικά δεδομένα υφίστανται επεξεργασία;	Καταγράψτε τα δεδομένα που συλλέγονται και τυγχάνουν επεξεργασίας. Καθορίστε για κάθε ένα τη	οικονομικά στοιχεία εταίρου (διατηρούνται για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου. πρόσβαση έχει ο υπεύθυνος έργου καθώς και ο οικονομικός σύμβουλος του οργανισμού) αριθμοί λογαριαμού εταίρου (διατηρούνται για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου.

	διάρκεια αποθήκευσης, τους αποδέκτες και τα άτομα που έχουν πρόσβαση σε αυτά.	πρόσβαση έχει ο υπεύθυνος έργου καθώς και ο οικονομικός σύμβουλος του οργανισμού) χρηματικό ποσό που λαμβάνει ο κάθε εταίρος (διατηρούνται για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου. πρόσβαση έχει ο υπεύθυνος έργου καθώς και ο οικονομικός σύμβουλος του οργανισμού) ταχυδρομικές διευθύνσεις (διατηρούνται για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου. σε περίπτωση αλλαγής διεύθυνσης στα χρόνια του προγράμματος διατίθεται η νέα. πρόσβαση έχει ο υπεύθυνος έργου και το άτομο που ορίζεται να επιβλέπει αν πληρούνται σωστά οι διαδικασίες) email (διατηρείται δια παντός καθώς βοηθάει στην επικοινωνία και περαιτέρω συνεργασία και σε άλλα προγράμματα. πρόσβαση έχει ο υπεύθυνος έργου και τα άτομα που ορίζονται για να επικοινωνούν με τον εταίρο) τηλέφωνο επικοινωνίας (διατηρείται τουλάχιστον για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου και σε περίπτωση περαιτέρω συνεργασίας διατηρείται επιπλέον. πρόσβαση έχει ο υπεύθυνος έργου καθώς και το άτομο που ορίζεται να επιβλέπει αν πληρούνται σωστά οι διαδικασίες) συμβάσεις εργασίας για τήρηση της συμφωνίας για παροχή εργασιών (διατηρείται αυστηρά για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου. πρόσβαση έχει ο υπεύθυνος έργου καθώς και το άτομο που ορίζεται να επιβλέπει αν πληρούνται σωστά οι διαδικασίες) ονόματα των μελών της ομάδας των εταίρων που απασχολούνται στο πρόγραμμα (διατηρείται τουλάχιστον για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου. πρόσβαση έχει ο υπεύθυνος

		έργου καθώς και τα άτομα που ορίζονται να επικοινωνούν μαζί τους στα πλαίσια συνεργασίας) το προφίλ της εταιρείας (διατηρείται μόνο για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου. πρόσβαση έχει ο υπεύθυνος έργου καθώς και τα άτομα που ορίζονται να βλέπουν το προφίλ στα πλαίσια συνεργασίας) το υφιστάμενο περιορισμένης πρόσβασης υλικό και λογισμικό αλλά και προγενέστερη γνώση για τα αντικείμενα μελέτης που παρέχεται και διαμοιράζεται στα πλαίσια της συνεργασίας (harware, software, access control systems, simulation platforms, κτλ.) (διατηρείται μόνο για 3 χρόνια μέχρις ότου τελειώσει η σύμβαση έργου. πρόσβαση έχουν μόνο εξουσιοδοτημένα άτομα που θα συμβάλουν στην περαιτέρω ανάπτυξη λογισμικού και θα λειτουργήσουν βοηθητικά στην ανάπτυξη εφαρμογών.) φωτογραφίες και ηχογραφημένο υλικό από συνέδρια που λαμβάνουν χώρα στα πλαίσια της συνεργασίας (διατηρείται τουλάχιστον για 3 χρόνια στα πλαίσια συνεργασίας με τον εταίρο αλλά σε περίπτωση που εκείνος δώσει την συγκατάθεσή του, μπορούν να διατηρηθούν για διάδοση των αποτελεσμάτων του προγράμματος) ερωτηματολόγια που διαμοιράζονται εκτός της κοινοπραξίας για σκοπούς λήψης πληροφοριών που θα φανούν χρήσιμες στα πλαίσια δημιουργίας λύσεων εντός του ευρωπαϊκού προγράμματος. (τα ερωτηματολόγια αυτά διατηρούνται για 3 χρόνια (όσο διαρκεί το ευρωπαϊκό πρόγραμμα και πρόσβαση σε αυτά έχει ο υπεύθυνος που τα δημιούργησε)

Πώς λειτουργεί ο κύκλος ζωής των δεδομένων και των διαδικασιών;	Παρουσιάστε και περιγράψτε τον κύκλο ζωής των δεδομένων (από τη συλλογή δεδομένων έως την καταστροφή δεδομένων, τα διάφορα στάδια επεξεργασίας, την αρχειοθέτηση, κ.λπ.), για παράδειγμα, χρησιμοποιώντας ένα διάγραμμα ροών δεδομένων (προσθέστε το ως συνημμένο) και μια λεπτομερή περιγραφή των διαδικασιών που διεξήχθη.	Τα δεδομένα συλλέγονται είτε με γραπτή επικοινωνία με ηλεκτρονικό ταχυδρομείο προς τον εταίρο, δια αλληλογραφίας ή τηλεφωνικώς. Κάθε πληροφορία που λαμβάνεται αρχειοθετείται για κάθε εταίρο σε ξεχωριστό ηλεκτρονικό και φυσικό φάκελο και τηρούνται τα αντίγραφα σε ερμάρια έχοντας πρόσβαση μόνο ο υπεύθυνος του προγράμματος. Ο υπεύθυνος του προγράμματος ανάλογα την περίπτωση των δεδομένων που ορίστηκε προηγουμένως ορίζει τον υπεύθυνο που θα έχει την επίβλεψη όλων των διαδικασιών και θα βοηθήσει στην τήρηση όλων των νόμινων διαδικασιών. Αναφορικά με τα ερωτηματολόγια, αυτά δημιουργούνται είτε με κάποιο κοινά αποδεκτό από την αρμόδια αρχή εργαλείο μέσω πλατφόρμας στο διαδίκτυο ή με εργαλείο επεξεργασίας εγγράφων. Σε κάθε περίπτωση, τα προσωπικά δεδομένα του εκάστοτε εμπειρογνώμονα δεν λαμβάνονται υπόψιν για την λήψη αποφάσεων. Τα ερωτηματολόγια αυτά συμπληρώνονται με δυο τρόπους: α) είτε από την αυτοματοποιημένη πλατφόρμα (όπου δεν χρειάζεται κανείς να αναφέρει τα προσωπικά του στοιχεία αλλά προσωρινά συλλέγονται διαδικτυακά ίχνη (IP διευθύνσεις)) ή β) κατόπιν συνεντεύξεων στους εν λόγω εμπειρογνώμονες. Και στις δυο περιπτώσεις τα δεδομένα συλλέγονται και δομούνται σε έγγραφο κειμένου. Όσον αφορά τα προσωπικά δεδομένα των εμπειρογνωμόνων, δεν διατηρούνται σε κανένα αρχείο. Ειδικά στην περίπτωση της συνέντευξης τα στοιχεία τους διατηρούνται για λίγες μέρες (3 μέρες) μέχρι να γίνει η ταυτοποίηση των όσων

		ανέφερε και κατόπιν διαγράφονται δια παντός. Και στις δυο περιπτώσεις, τα δεδομένα για έρευνα που συλλέγονται αποθηκεύονται σε αρχεία σε ηλεκτρονικούς υπολογιστές.
Ποια είναι τα μέσα που υποστηρίζουν τα δεδομένα;	Καταχωρίστε τα στοιχεία που υποστηρίζουν τα δεδομένα (λειτουργικά συστήματα, επιχειρηματικές εφαρμογές, συστήματα διαχείρισης βάσεων δεδομένων, σουίτες γραφείου, πρωτόκολλα, διαμορφώσεις, κ.λπ.)	Ubuntu 16.04, DELL PowerEdge T640, Apache / php 7, MySQL, Windows 10, OFFICE 365, FortiSwitch, FortiGate 200f, QNAP, Debian-based NAS

5.2.2 Μελέτη των θεμελιωδών αρχών (Fundamental principles)

Ο στόχος αυτού του σταδίου είναι η δημιουργία του συστήματος που εξασφαλίζει τη συμμόρφωση με τις αρχές προστασίας της ιδιωτικής ζωής. Αυτό το τμήμα επιτρέπει την απόδειξη ότι γίνεται εφαρμογή των απαραίτητων μέσων που θα επιτρέψουν στα ενδιαφερόμενα άτομα να ασκήσουν τα δικαιώματά τους.

Αναλογικότητα και Αναγκαιότητα:

Ερώτηση	Βοήθημα εισαγωγής	Απάντηση

Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;	Εξηγήστε γιατί οι σκοποί της επεξεργασίας, είναι σαφείς, ρητοί και νόμιμοι.	Οι σκοποί της επεξεργασίας είναι σαφείς, ρητοί και νόμιμοι καθώς τηρούνται όλοι οι κανόνες και τα μέτρα προστασίας προσωπικών δεδομένων όπως αυτά ορίζονται από τον γενικό κανονισμό προστασίας δεδομένων.
Ποια είναι η νομική βάση που καθιστά την επεξεργασία νόμιμη;	Περιγράψτε ποια είναι η νομική βάση της επεξεργασίας σας (π.χ.: συγκατάθεση, εκτέλεση συμβολαίου, συμμόρφωση με νομική υποχρέωση, προστασία ζωτικών συμφερόντων, κ.λπ.)	Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος. Θεωρείται αναγκαίο να επεξεργάζονται τα δεδομένα στα πλαίσια σωστής διαχείρισης του ευρωπαϊκού έργου. Επιπλεόν, στα πλαίσια του ερωτηματολογίου απαιτείται συγκατάθεση για να γίνει η σωστή διαχείριση.
Τα προσωπικά δεδομένα που συλλέγονται είναι επαρκή, συναφή και περιορίζονται σε όσα είναι απαραίτητα σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία	Εξηγήστε γιατί κάθε ένα από τα δεδομένα που συλλέγονται είναι απαραίτητο για τους σκοπούς της επεξεργασίας σας.	Τα δεδομένα που συλλέγονται περιορίζονται σε όσα είναι απαραίτητα σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Συλλέγονται: Όνομα, Επίθετο, ηλεκτρονικό ταχυδρομείο, αριθμός τηλεφώνου, Αιτιολόγηση: Απαιτούνται λεπτομέρειες για τη δημιουργία ενός προφίλ επικοινωνίας. Δεν συλλέγονται δεδομένα που αφορούν την προσωπική ζωή (συνήθειες διαβίωσης, οικογενειακή κατάσταση) ή στοιχεία τα οποία δεν είναι αναγκαία για τη σύμβαση.

(«ελαχιστοποίηση των δεδομένων»);		Συλλέγονται επίσης: Επαγγελματική ζωή (βιογραφικό σημείωμα, εκπαίδευση και επαγγελματική κατάρτιση.) Αιτιολόγηση: Απαιτούνται λεπτομέρειες για τη δημιουργία μιας βάσης δεδομένων για οποιαδήποτε αναφορά στο επαγγελματικό προφίλ του εταίρου. Συλλέγονται: χρηματοοικονομικές πληροφορίες (αριθμός λογαριασμού με σύνδεση σε τράπεζα) Αιτιολόγηση: Απαιτούνται λεπτομέρειες για τη δημιουργία μιας βάσης δεδομένων για να γίνουν οι πληρωμές των εταίρων εφόσον παρέχουν υπηρεσίες στο πρόγραμμα σε διαστήματα που ορίζονται από την σύμβαση έργου. Συλλέγονται: Απαντήσεις από ερωτηματολόγια. Αιτιολόγηση: Σε περιπτώσεις συνεντεύξεων απαιτούνται για την λήψη δεδομένων για τη ταυτοποίηση του ατόμου που έδωσε το υλικό προς μελέτη και έρευνα με σκοπό την επιβεβαίωση των δεδομένων που έχει πει. Δεδομένα που θεωρούνται ευαίσθητα δεν συλλέγονται.
Τα δεδομένα είναι ακριβή και ενημερωμένα;	Περιγράψτε ποια είναι τα μέτρα που έχουν ληφθεί για τη διασφάλιση της ποιότητας των δεδομένων.	Τα δεδομένα προσωπικού χαρακτήρα είναι ακριβή και ενημερωμένα καθώς υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Επιπλέον συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Όταν είναι αναγκαίο επικαιροποιούνται και λαμβάνονται όλα τα εύλογα μέτρα (όταν ζητούνται) για την άμεση

		διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα. Όταν ζητάται από τον εταίρο να γίνει διαγραφή των δεδομένων του τότε ενημερώνεται ο αρμόδιος υπεύθυνος επεξεργασίας δεδομένων και διαγράφει από όλα τα αρχεία (ηλεκτρονικά και μη) τα δεδομένα αυτά. Υπογράφεται σύμβαση έργου αλλά και έγγραφο συγκατάθεσης για διατήρηση των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Αναφορικά με τα δεδομένα που παρουσιάζονται από τα ερωτηματολόγια, αυτά αφορούν αποκλειστικά το όνομα και το επίθετου του εμπειρογνώμονα και είναι πάντα ενημερωμένα.
Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;	Εξηγήστε γιατί οι διάρκειες αποθήκευσης δικαιολογούνται από τις νομικές απαιτήσεις ή / και τις ανάγκες της επεξεργασίας.	Τα δεδομένα για ερευνητικούς σκοπούς αλλά και αυτά των δεδομένων των εταίρων αποθηκεύονται για 3 τουλάχιστον χρόνια εκτός περιπτώσεων όπου ο χρόνος τήρησης καθορίζεται από νομική υποχρέωση.

Μέτρα για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων:

Ερώτηση	Βοήθημα εισαγωγής	Απάντηση
Πώς ενημερώνονται τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία;	Περιγράψτε ποιες είναι οι πληροφορίες που δίνονται στα	Τα υποκείμενα των δεδομένων υπογράφουν σύμβαση έργου για τα δεδομένα που διατηρούνται, για πόσα χρόνια και για ποιους λόγους γίνεται η επεξεργασία. Σχετικά με τα

	υποκείμενα των δεδομένων και ποια είναι τα μέσα για να γίνει αυτό.	ερωτηματολόγια και στην περίπτωση συνεντεύξεων, τα υποκείμενα των δεδομένων υπογράφουν φόρμα συναίνεσης αναφέροντας όλους τους λόγους για τους οποίους επεξεργάζονται τα δεδομένα.
Εάν ισχύει, πώς επιτυγχάνεται η συγκατάθεση των υποκειμένων των δεδομένων;	Περιγράψτε τα μέτρα που αποσκοπούν στη διασφάλιση της συγκατάθεσης των χρηστών.	Δεν υπάρχουν μέτρα που αποσκοπούν στη διασφάλιση της συγκατάθεσης των χρηστών.
Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους πρόσβασης και φορητότητας προσωπικών δεδομένων;	Περιγράψτε τα μέτρα που προορίζονται για να επιτρέψετε στα υποκείμενα δεδομένων να έχουν πρόσβαση, να λαμβάνουν και να διαβιβάζουν τα δεδομένα τους.	Το υποκείμενο των δεδομένων επικοινωνεί με τον υπεύθυνο επεξεργασίας και ρωτάει αν μπορεί να έχει πρόσβαση στα δεδομένα που απάντησε και πλέον υφίστανται της επεξεργασίας. Δεν έχει προβλεφθεί το να μπορούν να διαβιβάσουν τα δεδομένα τους παρά μόνο να τα λάβουν παρέχοντας τους αντίγραφο.
Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους διόρθωσης και διαγραφής;	Περιγράψτε τους ελέγχους που προορίζονται για να επιτρέψετε στα υποκείμενα δεδομένων να διορθώνουν και να διαγράφουν τα δεδομένα τους.	Το υποκείμενο των δεδομένων αιτείται με ηλεκτρονική ή έντυπη μορφή από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που τον αφορούν. Επιπλέον το υποκείμενο των δεδομένων αιτείται με τον ίδιο τρόπο τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης είτε σε γραπτή μορφή ή ζητώντας με ηλεκτρονικό ταχυδρομείο.
Πώς μπορούν τα υποκείμενα δεδομένων να	Περιγράψτε τα μέτρα που προορίζονται να	Το υποκείμενο δεδομένων στέλνει γραπτό αίτημα στον υπεύθυνο επεξεργασίας με σκοπό να του δοθεί το δικαίωμα περιορισμού και εναντίωση σε

ασκήσουν τα δικαιώματά τους περιορισμού και εναντίωσης;	επιτρέψουν στα υποκείμενα των δεδομένων να περιορίζουν και να αντιτίθενται στην επεξεργασία των δεδομένων τους.	όσα αναφέρονται στην έκθεση που αναφέρεται στην επεξεργασία των δεδομένων.
Οι υποχρεώσεις των εκτελούντων την επεξεργασία προσδιορίζονται σαφώς και διέπονται από σύμβαση;	Για κάθε εκτελούντα την επεξεργασία, περιγράψτε τις ευθύνες του (διάρκεια, πεδίο εφαρμογής, σκοπό, τεκμηριωμένες οδηγίες επεξεργασίας, προηγούμενη έγκριση) και προσκομίστε τις συμβάσεις, τους κώδικες δεοντολογία και τις πιστοποιήσεις που καθορίζουν τις αποστολές και τις υποχρεώσεις του.	Ο εκτελών την επεξεργασία είναι υπεύθυνος να επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας. Η διάρκεια ορίζεται από την σύμβαση που υπογράφεται με το υποκείμενο της επεξεργασίας.
Σε περίπτωση μεταφοράς δεδομένων εκτός της Ευρωπαϊκής	Για κάθε χώρα εκτός της Ευρωπαϊκής Ένωσης όπου	Δεν μεταφέρονται δεδομένα εκτός της Ευρωπαϊκής Ένωσης.

Ένωσης, τα προσωπικά δεδομένα προστατεύονται επαρκώς;	αποθηκεύονται ή υποβάλλονται σε επεξεργασία δεδομένα, ονομάστε την και δηλώστε εάν αναγνωρίζεται ότι προσφέρει επαρκές επίπεδο προστασίας δεδομένων ή περιγράψτε τις προβλέψεις που αφορούν στη μεταφορά.	

5.2.3 Κίνδυνοι

Αυτή η ενότητα επιτρέπει να γίνει αξιολόγηση των κινδύνων, λαμβάνοντας υπόψη υπάρχοντα ή προγραμματισμένα μέτρα για τα δεδομένα.

Προγραμματισμένα ή υπάρχοντα μέτρα:

Μέτρο	Βοήθημα εισαγωγής	Απάντηση
Ασφάλεια εγγράφων	Όταν κατά τη διάρκεια της επεξεργασίας χρησιμοποιούνται έγγραφα που περιέχουν προσωπικά δεδομένα, υποδείξτε εδώ τον τρόπο με τον	Όταν χρησιμοποιούνται έγγραφα που περιέχουν προσωπικά δεδομένα αυτά εκτυπώντονται σε έναν συγκεκριμένο εκτυπωτή που είναι διαθέσιμος μόνο στο δίκτυο του οργανισμού, αποθηκεύονται σε ερμάριο που έχει πρόσβαση μόνο ο υπεύθυνος επεξεργασίας. Σε περίπτωση που επέλθει το χρονικό περιθώριο των 3 χρόνων τότε αυτά καταστρέφονται με τον καταστροφέα

	οποίο εκτυπώνονται, αποθηκεύονται, καταστρέφονται και ανταλλάσσονται.	εγγράφων με σκοπό την ελαχιστοποίηση του κινδύνου κλοπής.
Έλεγχος φυσικής πρόσβασης	Αναφέρετε πως διεξάγεται ο έλεγχος στη φυσική πρόσβαση σχετικά με τους χώρους όπου στεγάζεται η επεξεργασία.	Στους χώρους όπου στεγάζονται τα δεδομένα υπάρχει πρόσβαση από το προσωπικό του οργανισμού αλλά δεν γνωρίζουν τα σημεία όπου φυλάσσονται τα έγγραφα αυτά.
Παρακολούθηση των μέτρων προστασίας δεδομένων	Αναφέρετε αν ελέγχεται η αποτελεσματικότητα και η επάρκεια των μέτρων προστασίας των δεδομένων.	Δεν ελέγχεται η επάρκεια των μέτρων προστασίας δεδομένων.
Διαχείριση σταθμών εργασίας	Περιγράψτε τα μέτρα που εφαρμόζονται σε σταθμούς εργασίας.	Οι σταθμοί εργασίας εντός του οργανισμού που κάνει τη διαχείριση δεδομένων, κλειδώνουν αυτόματα και είναι σε ασφαλείς φυσικούς χώρους.
Αντίγραφα ασφαλείας	Υποδείξτε τον τρόπο διαχείρισης των αντιγράφων ασφαλείας. Διασαφηνίστε αν αποθηκεύονται σε ασφαλές μέρος.	Τα αντίγραφα ασφαλείας αποθηκεύονται σε ασφαλή υπολογιστή εκτός δικτύου και υπάρχει περιορισμένη πρόσβαση από τα εξουσιοδοτημένα άτομα.
Ανωνυμοποίηση	Αναφέρετε τους μηχανισμούς ανωνυμοποίησης που εφαρμόζονται.	Κατά τη συμπλήρωση ερωτηματολογίων των εμπειρογνωμόνων στο εργαλείο μέσω διαδικτύου δεν είναι υποχρεωτικά προς συμπλήρωση τα στοιχεία που αφορούν τα προσωπικά τους δεδομένα.

Παρακάτω αναλύονται τα αίτια και οι συνέπειες της αθέμιτης πρόσβασης στα προσωπικά δεδομένα και εκτίμηση της σοβαρότητας και της πιθανότητάς της αναφορικά με την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Για το λόγο αυτό χρησιμοποιούνται οι επιπτώσεις, οι απειλές και οι πηγές κινδύνου όπως αυτές έχουν διαμορφωθεί στο Κεφάλαιο 4 κατά τη διαχείριση κινδύνων στον οργανισμό που μελετάται.

Αθέμιτη πρόσβαση στα δεδομένα:

Αθέμιτη πρόσβαση στα δεδομένα	Απάντηση
Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα δεδομένων αν επέρχονταν ο κίνδυνος;	• Ζημιές σε συνεργάτες του Οργανισμού • Επιπτώσεις στις Διεθνείς σχέσεις • Επιπτώσεις στη φήμη / εικόνα του Οργανισμού • Διαταραχή ελέγχου διαχείρισης • Υποβάθμιση υπηρεσιών • Απρόβλεπτες ή πρόσθετες δαπάνες • Απώλεια αγαθών • Υπέρβαση προϋπολογισμού • Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού • Κατάχρηση προσωπικών δεδομένων • Παρεμπόδιση εφαρμογής νόμου ή κανονισμών • Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements) • Νομική ευθύνη και κυρώσεις
Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;	• Απώλεια δεδομένων

Ποιές είναι οι πηγές κινδύνου;	• Μη διαθεσιμότητα αντιγράφων ασφαλείας • Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας • Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα • Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας
Ποιά από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;	• Ασφάλεια εγγράφων • Παρακολούθηση των μέτρων ασφαλείας δεδομένων • Έλεγχος φυσικής πρόσβασης • Διαχείριση σταθμών εργασίας • Αντίγραφα ασφαλείας • Ανωνυμοποίηση
Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;	**Περιορισμένο**: Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές δυσκολίες που πρόκειται όμως να αντιμετωπίσουν. Για παράδειγμα: δυσφήμιση της εταιρείας, απρόβλεπτες πληρωμές κτλ.
Πώς υπολογίζετε την πιθανότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;	**Περιορισμένο:** Φαίνεται δύσκολο για τις επιλεγμένες πηγές κινδύνου να υλοποιήσουν την απειλή (π.χ.: κλοπή έντυπων εγγράφων αποθηκευμένων σε δωμάτιο που προστατεύεται από βιομετρική συσκευή).

Ανεπιθύμητη τροποποίηση των δεδομένων:

Αθέμιτη πρόσβαση στα δεδομένα	Απάντηση
Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα δεδομένων σε περίπτωση επέλευσης του κινδύνου;	• Ζημιές σε συνεργάτες του Οργανισμού • Επιπτώσεις στις Διεθνείς σχέσεις • Επιπτώσεις στη φήμη / εικόνα του Οργανισμού • Διαταραχή ελέγχου διαχείρισης • Υποβάθμιση υπηρεσιών • Απρόβλεπτες ή πρόσθετες δαπάνες • Απώλεια αγαθών • Υπέρβαση προϋπολογισμού • Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού • Κατάχρηση προσωπικών δεδομένων • Παρεμπόδιση εφαρμογής νόμου ή κανονισμών • Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements) • Νομική ευθύνη και κυρώσεις
Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;	• Απώλεια δεδομένων
Ποιές είναι οι πηγές κινδύνου;	• Μη διαθεσιμότητα αντιγράφων ασφαλείας • Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας • Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα • Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας
Ποιά από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;	• Ασφάλεια εγγράφων • Παρακολούθηση των μέτρων ασφαλείας δεδομένων • Έλεγχος φυσικής πρόσβασης • Διαχείριση σταθμών εργασίας • Αντίγραφα ασφαλείας

	• Ανωνυμοποίηση
Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;	• **Περιορισμένο**: Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές δυσκολίες που πρόκειται όμως να αντιμετωπίσουν. Για παράδειγμα: δυσφήμιση της εταιρείας, απρόβλεπτες πληρωμές κτλ.
Πώς υπολογίζετε την πιθανότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;	• **Περιορισμένο:** Φαίνεται δύσκολο για τις επιλεγμένες πηγές κινδύνου να υλοποιήσουν την απειλή (π.χ.: κλοπή έντυπων εγγράφων αποθηκευμένων σε δωμάτιο που προστατεύεται από βιομετρική συσκευή).

Εξαφάνιση δεδομένων:

Αθέμιτη πρόσβαση στα δεδομένα	Απάντηση
Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα δεδομένων σε περίπτωση επέλευσης του κινδύνου;	• Ζημιές σε συνεργάτες του Οργανισμού • Επιπτώσεις στις Διεθνείς σχέσεις • Επιπτώσεις στη φήμη / εικόνα του Οργανισμού • Διαταραχή ελέγχου διαχείρισης • Υποβάθμιση υπηρεσιών • Απρόβλεπτες ή πρόσθετες δαπάνες • Απώλεια αγαθών • Υπέρβαση προϋπολογισμού

	• Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού • Κατάχρηση προσωπικών δεδομένων • Παρεμπόδιση εφαρμογής νόμου ή κανονισμών • Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements) • Νομική ευθύνη και κυρώσεις
Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;	• Απώλεια δεδομένων
Ποιές είναι οι πηγές κινδύνου;	• Μη διαθεσιμότητα αντιγράφων ασφαλείας • Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας • Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα • Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας
Ποιά από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;	• Ασφάλεια εγγράφων • Παρακολούθηση των μέτρων ασφαλείας δεδομένων • Έλεγχος φυσικής πρόσβασης • Διαχείριση σταθμών εργασίας • Αντίγραφα ασφαλείας • Ανωνυμοποίηση
Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;	• **Περιορισμένο**: Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές δυσκολίες που πρόκειται όμως να αντιμετωπίσουν. Για παράδειγμα: δυσφήμιση της εταιρείας, απρόβλεπτες πληρωμές κτλ.
Πώς υπολογίζετε την πιθανότητα	• **Περιορισμένο:** Φαίνεται δύσκολο για τις επιλεγμένες πηγές κινδύνου να υλοποιήσουν την απειλή (π.χ.: κλοπή έντυπων

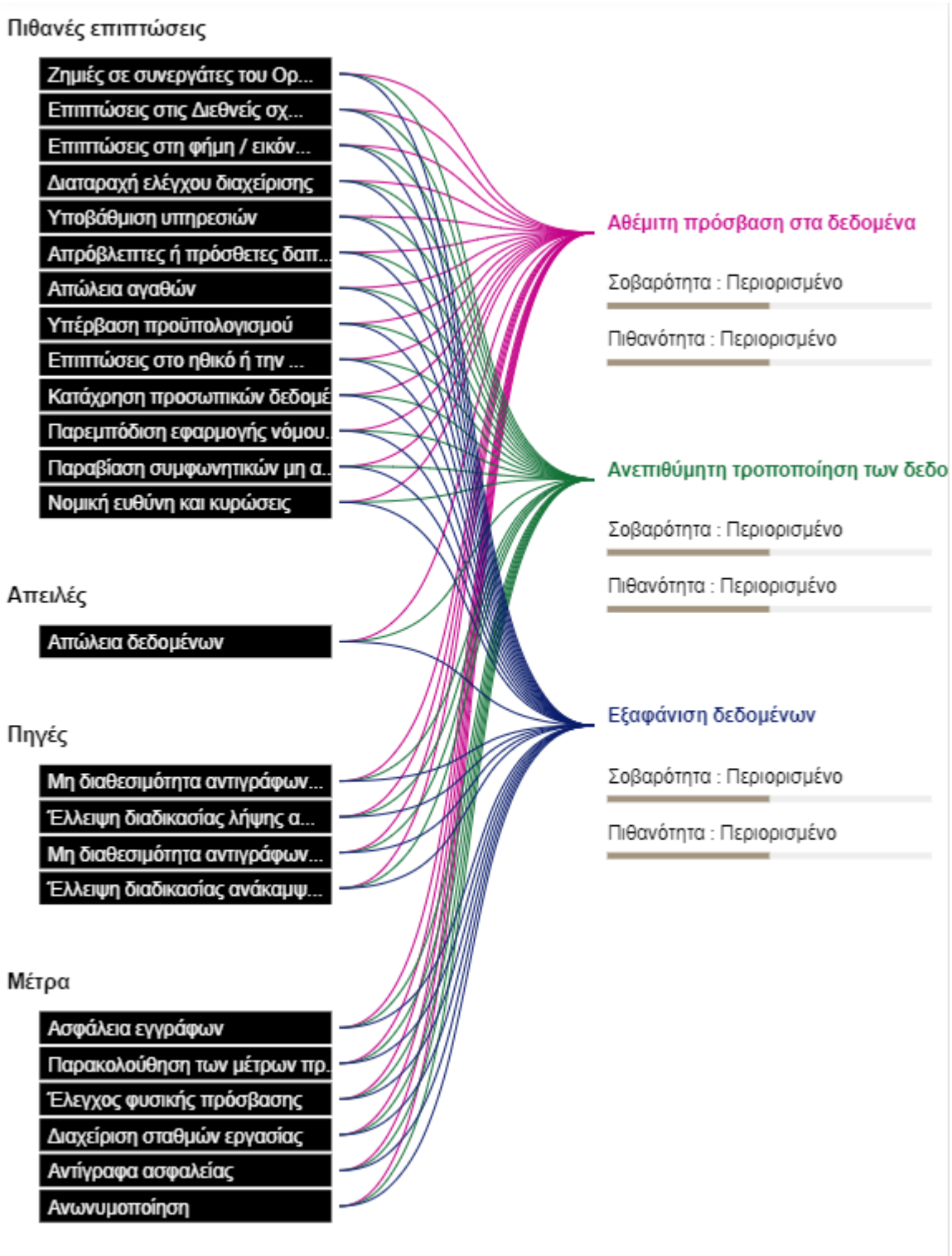
του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;	εγγράφων αποθηκευμένων σε δωμάτιο που προστατεύεται από βιομετρική συσκευή).

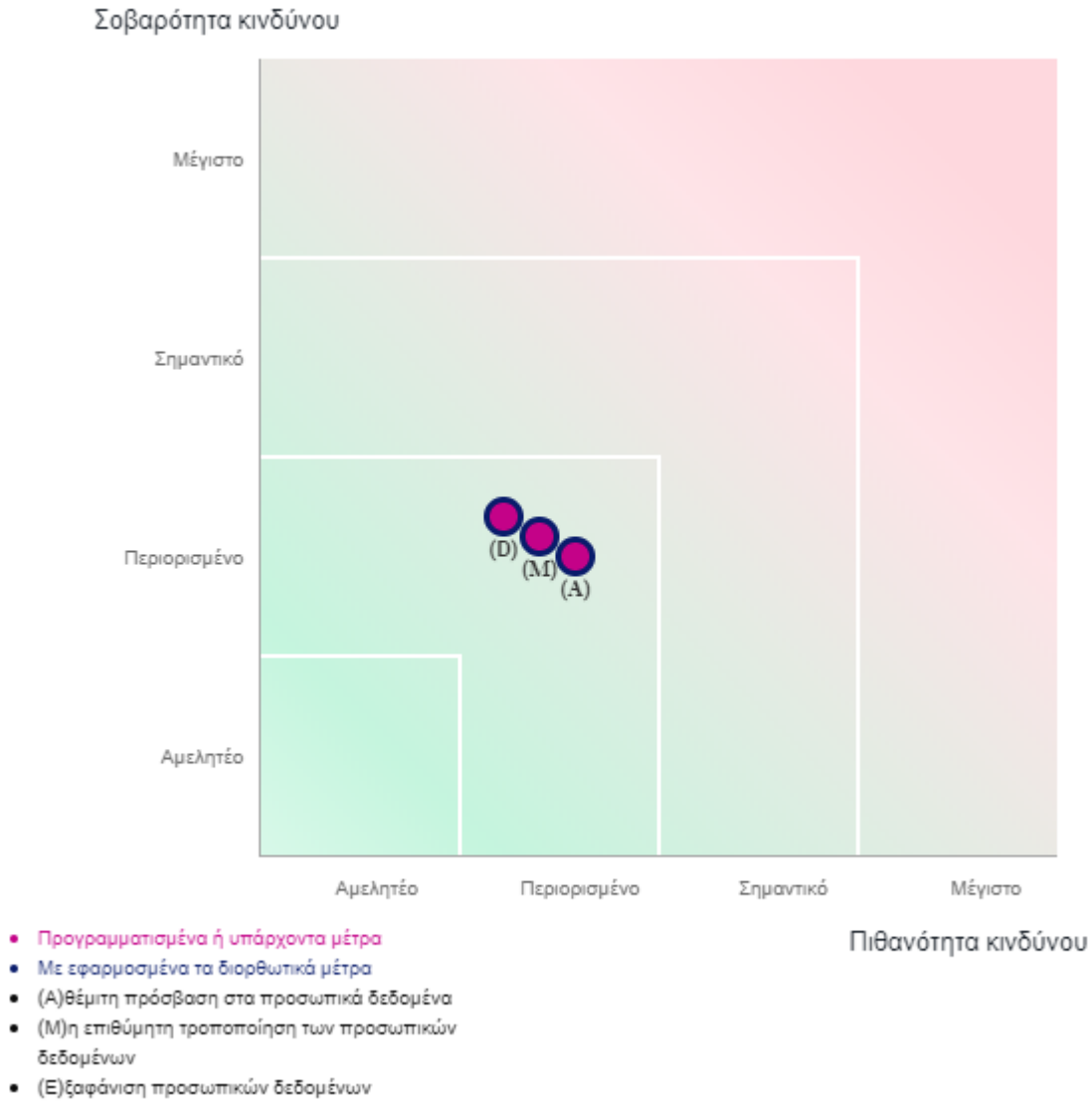
Αυτή η απεικόνιση παρέχει μια σφαιρική και συνθετική άποψη των επιπτώσεων των μέτρων στους κινδύνους που προέρχονται από την επεξεργασία.

5.2.4 Επικύρωση

Αυτή η ενότητα επιτρέπει την προετοιμασία και να επισημοποίηση της επικύρωσης της εκτίμησης αντικτύπου.

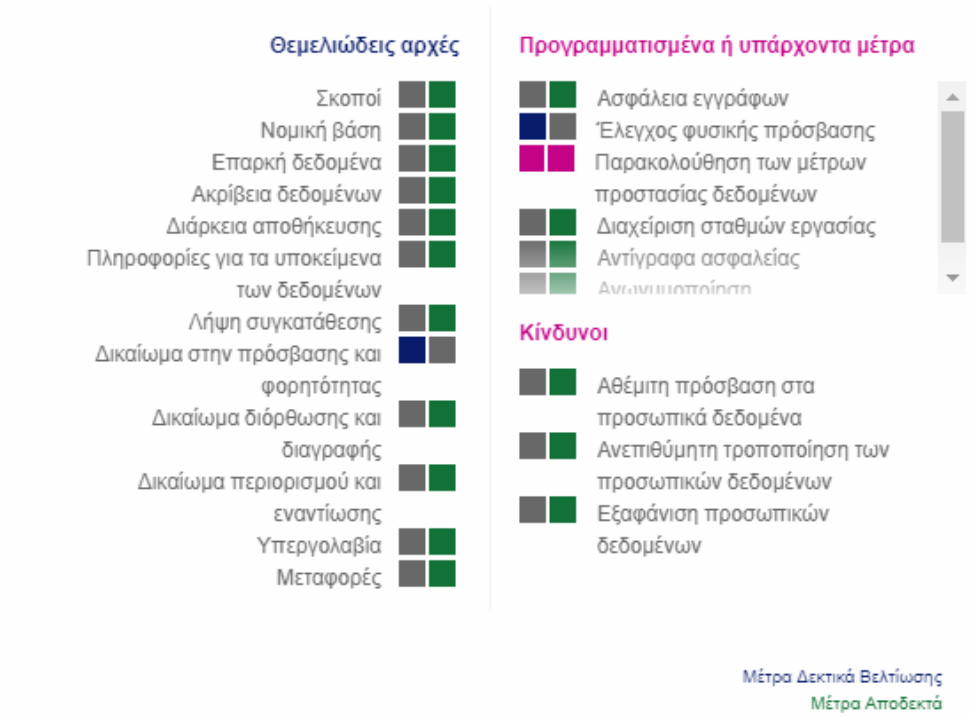
Χαρτογράφηση κινδύνων: Αυτή η απεικόνιση επιτρέπει την συνολική και συνθετική άποψη των κινδύνων, πριν και μετά την εφαρμογή των συμπληρωματικών μέτρων.

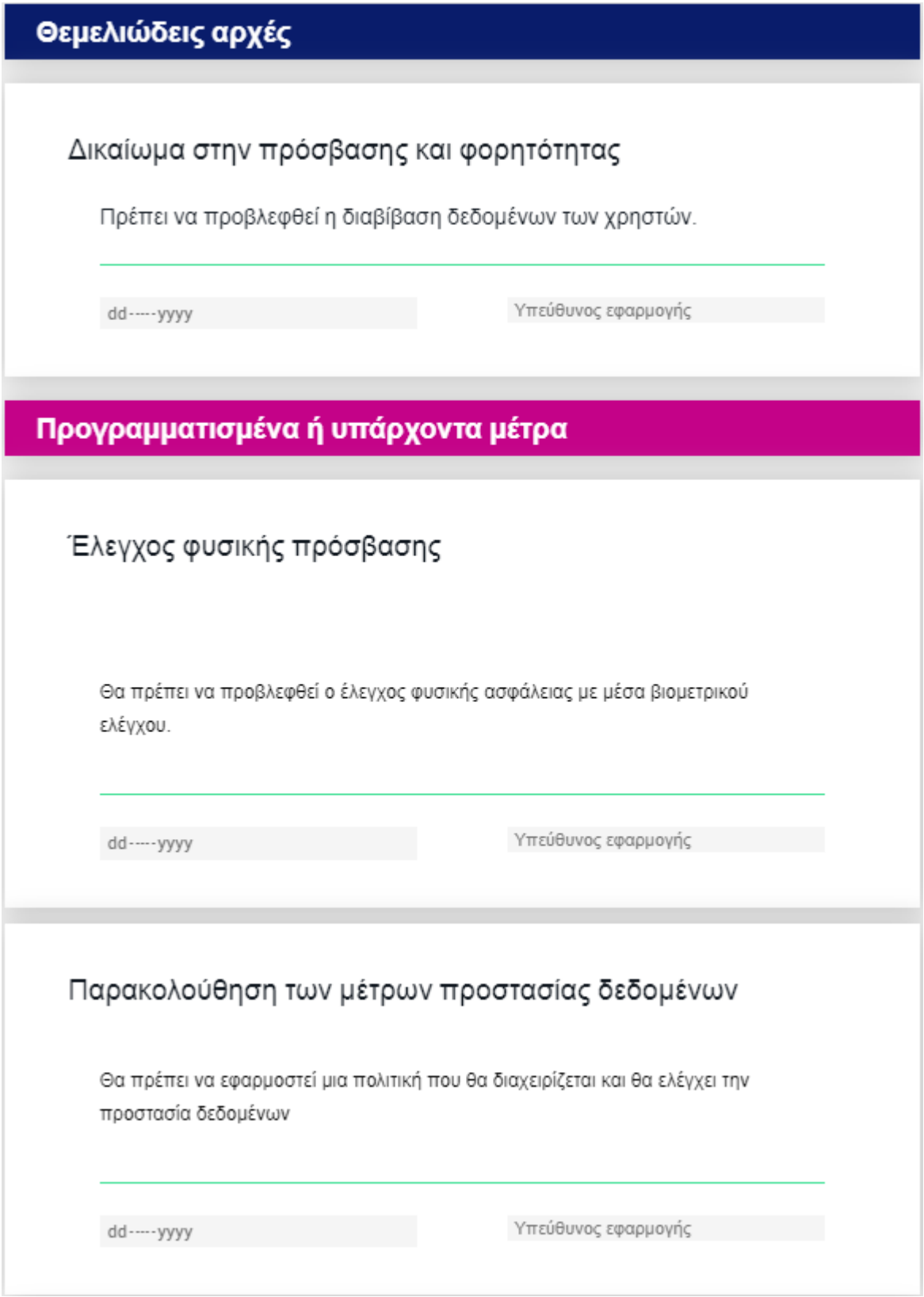

Πιθανές επιπτώσεις
Ζημιές σε συνεργάτες του Op...
Επιπτώσεις στις Διεθνείς σχ...
Επιπτώσεις στη φήμη / εικόν...
Διαταραχή ελέγχου διαχείρισης
Υποβάθμιση υπηρεσιών
Απρόβλεπτες ή πρόσθετες δαπ...
Απώλεια αγαθών
Υπέρβαση προϋπολογισμού
Επιπτώσεις στο ηθικό ή την ...
Κατάχρηση προσωπικών δεδομέ
Παρεμπόδιση εφαρμογής νόμου...
Παραβίαση συμφωνητικών μη α...
Νομική ευθύνη και κυρώσεις
Απειλές
Απώλεια δεδομένων
Πηγές
Μη διαθεσιμότητα αντιγράφων...
Έλλειψη διαδικασίας λήψης α...
Μη διαθεσιμότητα αντιγράφων...
Έλλειψη διαδικασίας ανάκαμψ...
Μέτρα
Ασφάλεια εγγράφων
Παρακολούθηση των μέτρων πρ...
Έλεγχος φυσικής πρόσβασης
Διαχείριση σταθμών εργασίας
Αντίγραφα ασφαλείας
Ανωνυμοποίηση
Αθέμιτη πρόσβαση στα δεδομένα
Σοβαρότητα : Περιορισμένο
Πιθανότητα : Περιορισμένο
Ανεπιθύμητη τροποποίηση των δεδο
Σοβαρότητα : Περιορισμένο
Πιθανότητα : Περιορισμένο
Εξαφάνιση δεδομένων
Σοβαρότητα : Περιορισμένο
Πιθανότητα : Περιορισμένο



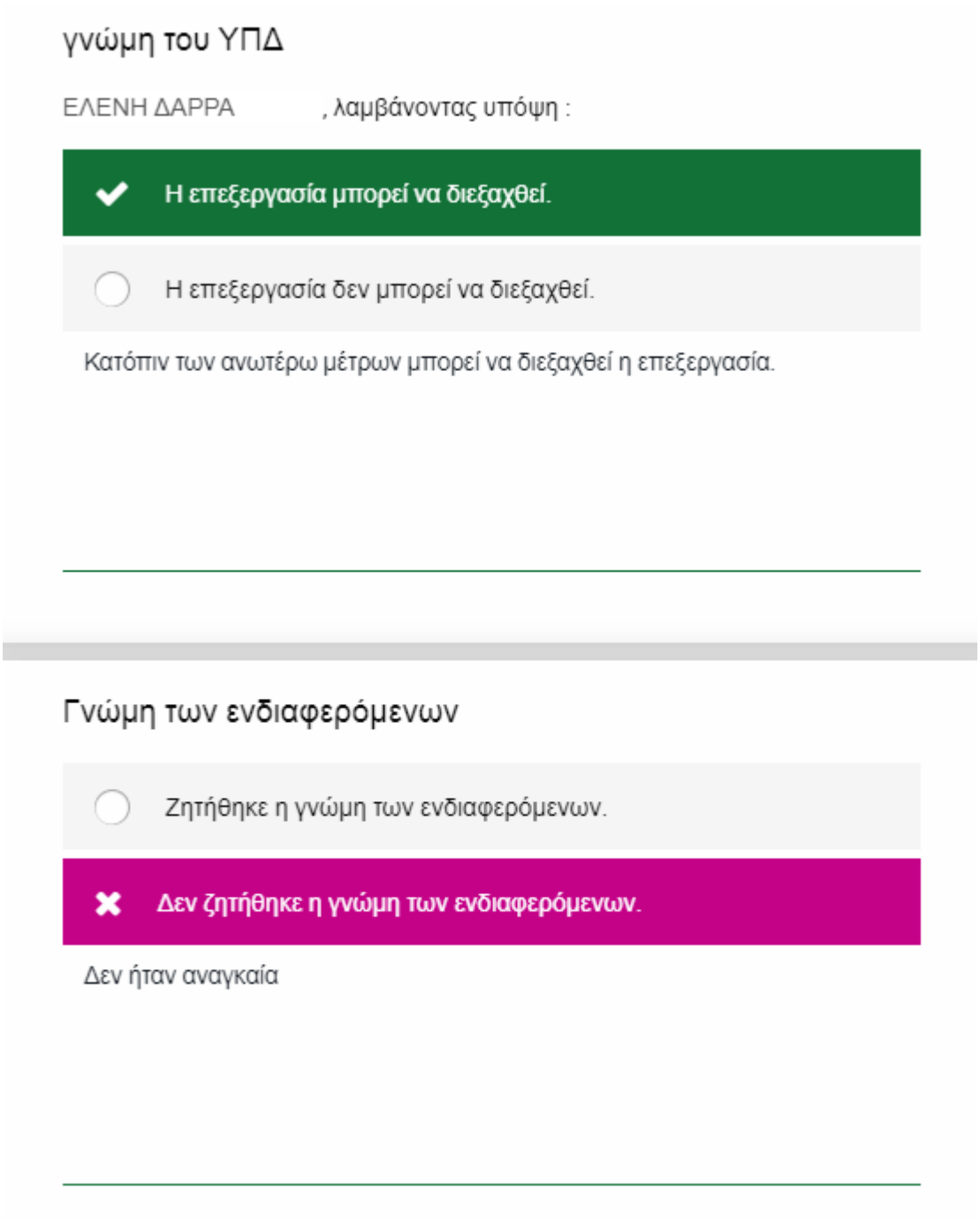
Σχέδιο δράσης: Σχεδιάζεται λεπτομερώς η εφαρμογή των πρόσθετων μέτρων που εντοπίστηκαν κατά τη διάρκεια της εκτίμησης αντικτύπου. Το σχέδιο δράσης ενημερώνεται αυτόματα κατά την αξιολόγηση των διαφόρων στοιχείων που περιλαμβάνονται στην εκτίμηση αντικτύπου.

Επισκόπηση


Θεμελιώδεις αρχές
Σκοποί
Νομική βάση
Επαρκή δεδομένα
Ακρίβεια δεδομένων
Διάρκεια αποθήκευσης
Πληροφορίες για τα υποκείμενα των δεδομένων
Λήψη συγκατάθεσης
Δικαίωμα στην πρόσβασης και φορητότητας
Δικαίωμα διόρθωσης και διαγραφής
Δικαίωμα περιορισμού και εναντίωσης
Υπεργολαβία
Μεταφορές
Προγραμματισμένα ή υπάρχοντα μέτρα
Ασφάλεια εγγράφων
Έλεγχος φυσικής πρόσβασης
Παρακολούθηση των μέτρων προστασίας δεδομένων
Διαχείριση σταθμών εργασίας
Αντίγραφα ασφαλείας
Κίνδυνοι
Αθέμιτη πρόσβαση στα προσωπικά δεδομένα
Ανεπιθύμητη τροποποίηση των προσωπικών δεδομένων
Εξαφάνιση προσωπικών δεδομένων
Μέτρα Δεκτικά Βελτίωσης
Μέτρα Αποδεκτά



Γνώμες ΥΠΔ και ενδιαφερόμενων προσώπων: Παρουσιάζονται οι συμβουλές του υπεύθυνου προστασίας δεδομένων και προστασίας της ιδιωτικής ζωής (εκπρόσωπος προστασίας δεδομένων εάν υπάρχει). Παρουσιάζονται οι απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους.



Σαν τελικό στάδιο είναι η επικύρωση της εκτίμησης αντικτύπου λαμβάνοντας υπόψιν τα παρακάτω:

Άτομο υπεύθυνο για την επικύρωση της ΕΑ: .

Μετά την ανάγνωση της πλήρους ΕΑ που σχετίζεται με την επεξεργασία δεδομένων που συνδέεται με **DPIA**

- ✔ Βεβαιώνω ότι το πλαίσιο της επεξεργασίας προσωπικών δεδομένων που περιγράφεται στην ΕΑ είναι συνεπές με την πραγματικότητα.
- ✔ Βεβαιώνω ότι γνωρίζω τους κινδύνους ανάλογα με τα υπάρχοντα ή τα προγραμματισμένα μέτρα.
- ✔ Επικυρώνω τα διορθωτικά μέτρα που αναφέρονται στο σχέδιο δράσης.
- ✔ Δεσμεύομαι να υλοποιήσω το συντομότερο δυνατόν τις υποδεδειγμένες διορθωτικές ενέργειες.

Απόρριψη ΕΑ | Έγκριση ΕΑ (άμεση) | Έγκριση ΕΑ (υπογεγραμμένη)

Όλα τα κουτιά πρέπει να συμπληρωθούν

Κεφάλαιο 6

Συμπεράσματα

Λαμβάνοντας λοιπόν υπόψιν όλα τα ανωτέρω, θα πρέπει να αναφερθεί ότι πλέον είναι επιτακτική ανάγκη η εκπόνηση Εκτίμησης Αντικτύπου ως προς την προστασία Προσωπικών Δεδομένων (ΕΑΠΔ). Ένας οργανισμός μπορεί να βοηθηθεί από την υλοποίηση της αξιοποιώντας τη διαχείριση κινδύνων που συνήθως πραγματοποιείται στα πλαίσια βελτίωσης του οργανισμού. Η ΕΑΠΔ αποτελεί μία διαδικασία, που εξετάζει θέματα ασφάλειας προσωπικών δεδομένων θέματα που άπτονται, του πώς ικανοποιούνται τα δικαιώματα των προσώπων των οποίων τα δεδομένα υφίστανται επεξεργασία ή του αν συλλέγονται υπέρμετρα προσωπικά δεδομένα σε σχέση με τους επιδιωκόμενους σκοπούς.

Πιο συγκεκριμένα, παρατηρήθηκε ότι η ΕΑΠΔ υποχρεώνει τους υπεύθυνους επεξεργασίας να συμμορφώνονται με τις προδιαγραφές του ΓΚΠΔ, αλλά και να αποδεικνύουν ότι έχουν λάβει τα απαραίτητα μέτρα για τη διασφάλιση της συμμόρφωσης με τον Κανονισμό. Τέλος, η μη συμμόρφωση με τις απαιτήσεις ΕΑΠΔ μπορεί να οδηγήσει στην επιβολή κυρώσεων από την εκάστοτε αρμόδια εποπτική αρχή. Επίσης, αξίζει να αναφερθεί ότι η ΕΑΠΔ ,μιας και είναι στα πρώιμα στάδια εφαρμογής της, υπάρχει αρκετό ερευνητικό ενδιαφέρον που μπορεί να βελτιώσει στη λειτουργία των οργανισμών.

Βιβλιογραφία

[1] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46". Official Journal of the European Union (OJ), 59, σσ. 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, wp248rev.01, 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[3] Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2018 (https://www.dpa.gr/portal/page?_pageid=33,223264&_dad=portal&_schema=PORTAL)

[4] Article "Η υποχρέωση διενέργειας εκτίμησης αντικτύπου (Data protection impact assessment - DPIA) στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)" - Δημήτρης Γ. Ζωγραφόπουλος - Περιοδικό Συνήγορος

[5] Κωνσταντίνος Σιασιάκος, Σοφία Αναστασίου, Κανέλλος Τούντας, "Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης", May 2017

[6] Σιασιάκος, Αναστασίου, & Τούντας (2016). Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης. Εκπαίδευση, Δια Βίου Μάθηση, Έρευνα και Τεχνολογική Ανάπτυξη, Καινοτομία και Οικονομία, 1, 542-555. Available from: https://www.researchgate.net/publication/317109414_Ektimese_ton_Epiptoseon_schetika_me_ten_Prostasia_Dedomenon_se_erga_Elektronikes_Diakyberneses [accessed Nov 27 2019].

[7] Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων https://www.prolegisproject.eu/index.php/bg/about-the-project/public-deliverables/category/7-el?download=72:modules-el

[8] "PRIVACY IMPACT ASSESSMENT (PIA) Methodology (how to carry out a PIA)" – CNIL, June 2015 Edition https://www.cnil.fr/en/privacy-impact-assessment-pia

Παράρτημα Α

Πίνακες – Αποτίμηση Αγαθών Δεδομένων

Στο παράρτημα αυτό περιλαμβάνεται η αποτίμηση των αγαθών δεδομένων ως προς την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα. Παρακάτω υπάρχουν ενδεικτικοί πίνακες:

#	2	ΑΓΑΘΟ	Δεδομένα για έρευνα & ανάλυση	
ΑΠΩΛΕΙΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ				
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** **0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ** **Σενάρια Απώλειας Εμπιστευτικότητας**			**Σχόλια**
	Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Εξωτερικό περιβάλλον				
Επιπτώσεις στις πολιτικές σχέσεις				
Διαταραχή πολιτικής απόφασης				
Ζημιές σε συνεργάτες του Οργανισμού	1	2	3	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	3			
Επιπτώσεις στις Διεθνείς σχέσεις		3	4	
Ειπτώσεις στη δημόσια τάξη	1			
Διαδικασίες και Συστήματα				
Διαταραχή ελέγχου διαχείρισης				
Υποβάθμιση υπηρεσιών				
Απρόβλεπτες ή πρόσθετες δαπάνες		3		
Απώλεια αγαθών	2			

Υπέρβαση προϋπολογισμού				
Επιπτώσεις σε πελάτες / υπαλλήλους				
Υγεία και ασφάλεια				
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	2			
Κατάχρηση προσωπικών δεδομένων		3		
Νομικές και κανονιστικές επιπτώσεις				
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών			1	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)			3	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων			4	
Νομική ευθύνη και κυρώσεις		1	2	
Summary of ratings	**Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας**	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	3	3	4	
Τελικός Βαθμός Αποτίμησης Αγαθού	**4**			Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΠΟΛΎ ΥΨΗΛΟ**			

Πίνακας 12: Αγαθό 2 - Απώλεια Εμπιστευτικότητας

#	**2**	**ΑΓΑΘΟ**	**Δεδομένα για έρευνα & ανάλυση**		
ΑΠΩΛΕΙΑ ΑΚΕΡΑΙΟΤΗΤΑΣ					
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**				**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ				
	Σενάρια Απώλειας Ακεραιότητας				
	Μερική Καταστροφή των δεδομένων	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	

Εξωτερικό περιβάλλον					
Επιπτώσεις στις πολιτικές σχέσεις		2			
Διαταραχή πολιτικής απόφασης			2		
Ζημιές σε συνεργάτες του Οργανισμού			3	2	
Επιπτώσεις στις Διεθνείς σχέσεις	2	4			
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού			2	1	
Ειπτώσεις στη δημόσια τάξη					
Διαδικασίες και Συστήματα					
Διαταραχή ελέγχου διαχείρισης					
Υποβάθμιση υπηρεσιών					
Απρόβλεπτες ή πρόσθετες δαπάνες		2			
Απώλεια αγαθών					
Υπέρβαση προϋπολογισμού		1			
Επιπτώσεις σε πελάτες / υπαλλήλους					
Υγεία και ασφάλεια					
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	1	2	1		
Κατάχρηση προσωπικών δεδομένων					
Νομικές και κανονιστικές επιπτώσεις					
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών					
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)			2		
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων			2	2	
Νομική ευθύνη και κυρώσεις		1			
Συνολικοί βαθμοί	**Μερική Καταστροφή των δεδομένων**	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**2**	**4**	**3**	**2**	

Τελικός Βαθμός Αποτίμησης Αγαθού	4	Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΠΟΛΎ ΥΨΗΛΟ**	

Πίνακας 13: Αγαθό 2 - Απώλεια Ακεραιότητας

#	2	ΑΓΑΘΟ	Δεδομένα για έρευνα & ανάλυση					
ΑΠΩΛΕΙΑ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ								
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** 0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ **Διάρκεια Διακοπής**							**Σχόλια**
	15 Λεπτα	**1 ώρα**	**3 ώρες**	**12 ώρε**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Εξωτερικό περιβάλλον								
Επιπτώσεις στις πολιτικές σχέσεις				0	1	2	2	
Διαταραχή πολιτικής απόφασης								
Ζημιές σε συνεργάτες του Οργανισμού					2	2	3	
Επιπτώσεις στις Διεθνείς σχέσεις							2	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού				0	1	1	2	
Ειπτώσεις στη δημόσια τάξη								
Διαδικασίες και Συστήματα								
Διαταραχή ελέγχου διαχείρισης								
Υποβάθμιση υπηρεσιών				1	1	1	2	
Απρόβλεπτες ή πρόσθετες δαπάνες								
Απώλεια αγαθών							1	
Υπέρβαση προϋπολογισμού								
Επιπτώσεις σε πελάτες / υπαλλήλους								
Υγεία και ασφάλεια								
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού			1	1	2	2	3	
Κατάχρηση προσωπικών δεδομένων								

Νομικές και κανονιστικές επιπτώσεις								
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών								
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)					1	1	2	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων					3	3	3	
Νομική ευθύνη και κυρώσεις								
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ	**15 Λεπτα**	**1 ώρα**	**3 ώρες**	**12 ώρε**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**0**	**1**	**1**	**3**	**3**	**3**	
Τελικός Βαθμός Αποτίμησης Αγαθού	**3**							Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	ΥΨΗΛΟ							

Πίνακας 14: Αγαθό 2 - Απώλεια Διαθεσιμότητας

#	**3**	**ΑΓΑΘΟ**	**Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)**	
ΑΠΩΛΕΙΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ				
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**			**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ			
	Σενάρια Απώλειας Εμπιστευτικότητας			
	Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	

Εξωτερικό περιβάλλον				
Επιπτώσεις στις πολιτικές σχέσεις				
Διαταραχή πολιτικής απόφασης				
Ζημιές σε συνεργάτες του Οργανισμού	1	2		
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	2			
Επιπτώσεις στις Διεθνείς σχέσεις				
Ειπτώσεις στη δημόσια τάξη				
Διαδικασίες και Συστήματα				
Διαταραχή ελέγχου διαχείρισης	1	2		
Υποβάθμιση υπηρεσιών	1	1		
Απρόβλεπτες ή πρόσθετες δαπάνες				
Απώλεια αγαθών				
Υπέρβαση προϋπολογισμού				
Επιπτώσεις σε πελάτες / υπαλλήλους				
Υγεία και ασφάλεια				
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	2	1		
Κατάχρηση προσωπικών δεδομένων				
Νομικές και κανονιστικές επιπτώσεις				
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών				
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)				
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων			0	
Νομική ευθύνη και κυρώσεις				
Summary of ratings	**Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας**	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	2	2	0	
Τελικός Βαθμός Αποτίμησης Αγαθού	**2**			Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΜΕΤΡΙΟ**			

Πίνακας 15: Αγαθό 3 - Απώλεια Εμπιστευτικότητας

#	3	ΑΓΑΘΟ	Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)		
ΑΠΩΛΕΙΑ ΑΚΕΡΑΙΟΤΗΤΑΣ					
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**				**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ				
	Σενάρια Απώλειας Ακεραιότητας				
	Μερική Καταστροφή των δεδομένων	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Εξωτερικό περιβάλλον					
Επιπτώσεις στις πολιτικές σχέσεις					
Διαταραχή πολιτικής απόφασης					
Ζημιές σε συνεργάτες του Οργανισμού	2	3	3	1	
Επιπτώσεις στις Διεθνείς σχέσεις					
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού		1			
Ειπτώσεις στη δημόσια τάξη					
Διαδικασίες και Συστήματα					
Διαταραχή ελέγχου διαχείρισης					
Υποβάθμιση υπηρεσιών					
Απρόβλεπτες ή πρόσθετες δαπάνες					
Απώλεια αγαθών	1	2			
Υπέρβαση προϋπολογισμού	0	1			
Επιπτώσεις σε πελάτες / υπαλλήλους					
Υγεία και ασφάλεια					
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού			1		
Κατάχρηση προσωπικών δεδομένων					
Νομικές και κανονιστικές επιπτώσεις					

Παρεμπόδιση εφαρμογής νόμου ή κανονισμών					
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)					
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων					
Νομική ευθύνη και κυρώσεις					
Συνολικοί βαθμοί	**Μερική Καταστροφή των δεδομένων**	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**2**	**3**	**3**	**1**	
Τελικός Βαθμός Αποτίμησης Αγαθού	3				Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΥΨΗΛΟ**				

Πίνακας 16: Αγαθό 3 - Απώλεια Ακεραιότητας

#	**3**	**ΑΓΑΘΟ**	**Κοινόχρηστα αρχεία κοινού ενδιαφέροντος (word, excel κλπ.)**					
ΑΠΩΛΕΙΑ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ								
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**							**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ							
	Διάρκεια Διακοπής							
	15 Λεπτα	**1 ώρα**	**3 ώρες**	**12 ώρε**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Εξωτερικό περιβάλλον								
Επιπτώσεις στις πολιτικές σχέσεις								
Διαταραχή πολιτικής απόφασης								

Ζημιές σε συνεργάτες του Οργανισμού	0	0	1	2	3	3	3	
Επιπτώσεις στις Διεθνείς σχέσεις				1	1	2	2	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού								
Επιπτώσεις στη δημόσια τάξη								
Διαδικασίες και Συστήματα								
Διαταραχή ελέγχου διαχείρισης						3		
Υποβάθμιση υπηρεσιών				1	1	1	2	
Απρόβλεπτες ή πρόσθετες δαπάνες								
Απώλεια αγαθών					1	1	2	
Υπέρβαση προϋπολογισμού								
Επιπτώσεις σε πελάτες / υπαλλήλους								
Υγεία και ασφάλεια								
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού			0	1	1	1	2	
Κατάχρηση προσωπικών δεδομένων								
Νομικές και κανονιστικές επιπτώσεις								
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών								
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)								
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων								
Νομική ευθύνη και κυρώσεις								
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ	**15 Λεπτα**	**1 ώρα**	**3 ώρες**	**12 ώρε**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**0**	**1**	**2**	**3**	**3**	**3**	
Τελικός Βαθμός Αποτίμησης Αγαθού	**3**							Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	ΥΨΗΛΟ							

Πίνακας 17: Αγαθό 3 - Απώλεια Διαθεσιμότητας

#	4	ΑΓΑΘΟ	Δεδομένα back-up συστήματος	
ΑΠΩΛΕΙΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ				
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** **0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ** **Σενάρια Απώλειας Εμπιστευτικότητας**			**Σχόλια**
	Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Εξωτερικό περιβάλλον				
Επιπτώσεις στις πολιτικές σχέσεις		0		
Διαταραχή πολιτικής απόφασης	0			
Ζημιές σε συνεργάτες του Οργανισμού				
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού				
Επιπτώσεις στις Διεθνείς σχέσεις				
Ειπτώσεις στη δημόσια τάξη				
Διαδικασίες και Συστήματα				
Διαταραχή ελέγχου διαχείρισης	1			
Υποβάθμιση υπηρεσιών		2	1	
Απρόβλεπτες ή πρόσθετες δαπάνες				
Απώλεια αγαθών				
Υπέρβαση προϋπολογισμού				
Επιπτώσεις σε πελάτες / υπαλλήλους				
Υγεία και ασφάλεια				
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	1			
Κατάχρηση προσωπικών δεδομένων				
Νομικές και κανονιστικές επιπτώσεις				
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών				
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)				

Αποκάλυψη ευαίσθητων προσωπικών δεδομένων				
Νομική ευθύνη και κυρώσεις				
Summary of ratings	**Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας**	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	1	2	1	
Τελικός Βαθμός Αποτίμησης Αγαθού	**2**			Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΜΕΤΡΙΟ**			

Πίνακας 18: Αγαθό 4 - Απώλεια Εμπιστευτικότητας

#	**4**	**ΑΓΑΘΟ**	**Δεδομένα back-up συστήματος**		
ΑΠΩΛΕΙΑ ΑΚΕΡΑΙΟΤΗΤΑΣ					
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**				**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ				
	Σενάρια Απώλειας Ακεραιότητας				
	Μερική Καταστροφή των δεδομένων	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Εξωτερικό περιβάλλον					
Επιπτώσεις στις πολιτικές σχέσεις					
Διαταραχή πολιτικής απόφασης					
Ζημιές σε συνεργάτες του Οργανισμού			1		
Επιπτώσεις στις Διεθνείς σχέσεις					
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	0	1	1	0	

Ειπτώσεις στη δημόσια τάξη					
Διαδικασίες και Συστήματα					
Διαταραχή ελέγχου διαχείρισης	1	2			
Υποβάθμιση υπηρεσιών					
Απρόβλεπτες ή πρόσθετες δαπάνες		1			
Απώλεια αγαθών					
Υπέρβαση προϋπολογισμού					
Επιπτώσεις σε πελάτες / υπαλλήλους					
Υγεία και ασφάλεια					
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού					
Κατάχρηση προσωπικών δεδομένων					
Νομικές και κανονιστικές επιπτώσεις					
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών					
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)					
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων					
Νομική ευθύνη και κυρώσεις					
Συνολικοί βαθμοί	**Μερική Καταστροφή των δεδομένων**	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**2**	**1**	**0**	
Τελικός Βαθμός Αποτίμησης Αγαθού	2				Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΜΕΤΡΙΟ**				

Πίνακας 19: Αγαθό 4 - Απώλεια Ακεραιότητας

#	4	ΑΓΑΘΟ	Δεδομένα back-up συστήματος

ΑΠΩΛΕΙΑ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ

Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** 0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ **Διάρκεια Διακοπής**							**Σχόλια**
	15 Λεπτα	**1 ώρα**	**3 ώρες**	**12 ώρε**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Εξωτερικό περιβάλλον								
Επιπτώσεις στις πολιτικές σχέσεις								
Διαταραχή πολιτικής απόφασης								
Ζημιές σε συνεργάτες του Οργανισμού								
Επιπτώσεις στις Διεθνείς σχέσεις								
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού							0	
Επιπτώσεις στη δημόσια τάξη								
Διαδικασίες και Συστήματα								
Διαταραχή ελέγχου διαχείρισης			0	0	1	1	1	
Υποβάθμιση υπηρεσιών								
Απρόβλεπτες ή πρόσθετες δαπάνες					0	0	1	
Απώλεια αγαθών								
Υπέρβαση προϋπολογισμού								
Επιπτώσεις σε πελάτες / υπαλλήλους								
Υγεία και ασφάλεια								
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού								
Κατάχρηση προσωπικών δεδομένων								
Νομικές και κανονιστικές επιπτώσεις								
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών								
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)								
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων								
Νομική ευθύνη και κυρώσεις								
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ	**15 Λεπτά**	**1 ώρα**	**3 ώρες**	**12 ώρες**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	

Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**0**	**0**	**0**	**1**	**1**	**1**	
Τελικός Βαθμός Αποτίμησης Αγαθού	**1**							Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	ΧΑΜΗΛΟ							

Πίνακας 20: Αγαθό 4 - Απώλεια Διαθεσιμότητας

#	**5**	**ΑΓΑΘΟ**	**Δεδομένα παραμετροποίησης ιστοσελίδας**	
ΑΠΩΛΕΙΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ				
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** **0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ** **Σενάρια Απώλειας Εμπιστευτικότητας**			**Σχόλια**
	Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Εξωτερικό περιβάλλον				
Επιπτώσεις στις πολιτικές σχέσεις				
Διαταραχή πολιτικής απόφασης				
Ζημιές σε συνεργάτες του Οργανισμού				
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	3			
Επιπτώσεις στις Διεθνείς σχέσεις		3		
Ειπτώσεις στη δημόσια τάξη				
Διαδικασίες και Συστήματα				

Διαταραχή ελέγχου διαχείρισης				
Υποβάθμιση υπηρεσιών				
Απρόβλεπτες ή πρόσθετες δαπάνες		3		
Απώλεια αγαθών				
Υπέρβαση προϋπολογισμού				
Επιπτώσεις σε πελάτες / υπαλλήλους				
Υγεία και ασφάλεια				
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	1			
Κατάχρηση προσωπικών δεδομένων		3		
Νομικές και κανονιστικές επιπτώσεις				
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών			1	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)				
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων				
Νομική ευθύνη και κυρώσεις				
Summary of ratings	**Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας**	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	3	3	1	
Τελικός Βαθμός Αποτίμησης Αγαθού	**3**			Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΥΨΗΛΟ**			

Πίνακας 21: Αγαθό 5 - Απώλεια Εμπιστευτικότητας

#	5	ΑΓΑΘΟ	Δεδομένα παραμετροποίησης ιστοσελίδας
ΑΠΩΛΕΙΑ ΑΚΕΡΑΙΟΤΗΤΑΣ			
	Επίπεδο Επίπτωσης (ISO 27005)		**Σχόλια**

Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ				
	Σενάρια Απώλειας Ακεραιότητας				
	Μερική Καταστροφή των δεδομένων	Ολική καταστροφή δεδομένων (και των backup)	Σκόπιμη αλλοίωση δεδομένων	Ακούσια Αλλοίωση δεδομένων	
Εξωτερικό περιβάλλον					
Επιπτώσεις στις πολιτικές σχέσεις		2			
Διαταραχή πολιτικής απόφασης			2		
Ζημιές σε συνεργάτες του Οργανισμού			1		
Επιπτώσεις στις Διεθνείς σχέσεις	1	2			
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού					
Ειπτώσεις στη δημόσια τάξη					
Διαδικασίες και Συστήματα					
Διαταραχή ελέγχου διαχείρισης					
Υποβάθμιση υπηρεσιών					
Απρόβλεπτες ή πρόσθετες δαπάνες		2			
Απώλεια αγαθών					
Υπέρβαση προϋπολογισμού		1			
Επιπτώσεις σε πελάτες / υπαλλήλους					
Υγεία και ασφάλεια					
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού			1		
Κατάχρηση προσωπικών δεδομένων					
Νομικές και κανονιστικές επιπτώσεις					
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών					
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)					
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων					
Νομική ευθύνη και κυρώσεις					

Συνολικοί βαθμοί	Μερική Καταστροφή των δεδομένων	Ολική καταστροφή δεδομένων (και των backup)	Σκόπιμη αλλοίωση δεδομένων	Ακούσια Αλλοίωση δεδομένων	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**1**	**2**	**2**	**0**	
Τελικός Βαθμός Αποτίμησης Αγαθού	2				Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΜΕΤΡΙΟ**				

Πίνακας 22: Αγαθό 5 - Απώλεια Ακεραιότητας

#	5	ΑΓΑΘΟ	Δεδομένα παραμετροποίησης ιστοσελίδας					
ΑΠΩΛΕΙΑ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ								
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** 0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ **Διάρκεια Διακοπής**							**Σχόλια**
	15 Λεπτά	**1 ώρα**	**3 ώρες**	**12 ώρες**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Εξωτερικό περιβάλλον								
Επιπτώσεις στις πολιτικές σχέσεις	0	0						
Διαταραχή πολιτικής απόφασης								
Ζημιές σε συνεργάτες του Οργανισμού								
Επιπτώσεις στις Διεθνείς σχέσεις								
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού								
Ειπτώσεις στη δημόσια τάξη								
Διαδικασίες και Συστήματα								
Διαταραχή ελέγχου διαχείρισης								
Υποβάθμιση υπηρεσιών				1	1	1	2	
Απρόβλεπτες ή πρόσθετες δαπάνες								
Απώλεια αγαθών							1	

Υπέρβαση προϋπολογισμού								
Επιπτώσεις σε πελάτες / υπαλλήλους								
Υγεία και ασφάλεια								
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού			1					
Κατάχρηση προσωπικών δεδομένων								
Νομικές και κανονιστικές επιπτώσεις								
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών								
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)								
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων								
Νομική ευθύνη και κυρώσεις								
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ	**15 Λεπτά**	**1 ώρα**	**3 ώρες**	**12 ώρες**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**0**	**1**	**1**	**1**	**1**	**2**	
Τελικός Βαθμός Αποτίμησης Αγαθού	**2**							Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	ΜΕΤΡΙΟ							

Πίνακας 23: Αγαθό 5 - Απώλεια Διαθεσιμότητας

#	6	ΑΓΑΘΟ	Δεδομένα Αυθεντικοποίησης
ΑΠΩΛΕΙΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ			
	Επίπεδο Επίπτωσης (ISO 27005)		**Σχόλια**

Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ** **Σενάρια Απώλειας Εμπιστευτικότητας**			
	Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Εξωτερικό περιβάλλον				
Επιπτώσεις στις πολιτικές σχέσεις				
Διαταραχή πολιτικής απόφασης				
Ζημιές σε συνεργάτες του Οργανισμού				
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	2	3	4	
Επιπτώσεις στις Διεθνείς σχέσεις				
Ειπτώσεις στη δημόσια τάξη				
Διαδικασίες και Συστήματα				
Διαταραχή ελέγχου διαχείρισης	1			
Υποβάθμιση υπηρεσιών				
Απρόβλεπτες ή πρόσθετες δαπάνες		3		
Απώλεια αγαθών				
Υπέρβαση προϋπολογισμού				
Επιπτώσεις σε πελάτες / υπαλλήλους				
Υγεία και ασφάλεια				
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού		1	2	
Κατάχρηση προσωπικών δεδομένων	1	3	3	
Νομικές και κανονιστικές επιπτώσεις				
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών				
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)		3	3	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων				
Νομική ευθύνη και κυρώσεις				
Summary of ratings	**Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας**	**Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας**	**Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	2	3	4	

Τελικός Βαθμός Αποτίμησης Αγαθού	**4**	Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΠΟΛΥ ΥΨΗΛΟ**	

Πίνακας 24: Αγαθό 6 - Απώλεια Εμπιστευτικότητας

#	6	ΑΓΑΘΟ	Δεδομένα Αυθεντικοποίησης		
ΑΠΩΛΕΙΑ ΑΚΕΡΑΙΟΤΗΤΑΣ					
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**				**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ				
	Σενάρια Απώλειας Ακεραιότητας				
	Μερική Καταστροφή των δεδομένων	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Εξωτερικό περιβάλλον					
Επιπτώσεις στις πολιτικές σχέσεις		2			
Διαταραχή πολιτικής απόφασης			2		
Ζημιές σε συνεργάτες του Οργανισμού			1		
Επιπτώσεις στις Διεθνείς σχέσεις					
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού					
Ειπτώσεις στη δημόσια τάξη					
Διαδικασίες και Συστήματα					
Διαταραχή ελέγχου διαχείρισης					
Υποβάθμιση υπηρεσιών					
Απρόβλεπτες ή πρόσθετες δαπάνες		2			
Απώλεια αγαθών					
Υπέρβαση προϋπολογισμού		1			
Επιπτώσεις σε πελάτες / υπαλλήλους					
Υγεία και ασφάλεια					
Επιπτώσεις στο ηθικό ή την			1		

παραγωγικότητα του προσωπικού					
Κατάχρηση προσωπικών δεδομένων					
Νομικές και κανονιστικές επιπτώσεις					
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών					
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)					
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων					
Νομική ευθύνη και κυρώσεις					
Συνολικοί βαθμοί	**Μερική Καταστροφή των δεδομένων**	**Ολική καταστροφή δεδομένων (και των backup)**	**Σκόπιμη αλλοίωση δεδομένων**	**Ακούσια Αλλοίωση δεδομένων**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**2**	**2**	**0**	
Τελικός Βαθμός Αποτίμησης Αγαθού	2				Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	**ΜΕΤΡΙΟ**				

Πίνακας 25: Αγαθό 6 - Απώλεια Ακεραιότητας

#	**6**	**ΑΓΑΘΟ**	**Δεδομένα Αυθεντικοποίησης**				
ΑΠΩΛΕΙΑ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ							
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**						**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ						
	Διάρκεια Διακοπής						
	15 Λεπτά	**1 ώρα**	**3 ώρες**	**12 ώρες**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**

Εξωτερικό περιβάλλον								
Επιπτώσεις στις πολιτικές σχέσεις								
Διαταραχή πολιτικής απόφασης								
Ζημιές σε συνεργάτες του Οργανισμού								
Επιπτώσεις στις Διεθνείς σχέσεις		0	0	1	1	2	3	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού			0	1	1	1	2	
Επιπτώσεις στη δημόσια τάξη								
Διαδικασίες και Συστήματα								
Διαταραχή ελέγχου διαχείρισης				1	2	2	3	
Υποβάθμιση υπηρεσιών				1	1	1	1	
Απρόβλεπτες ή πρόσθετες δαπάνες	0	0	0	0	1	1	2	
Απώλεια αγαθών								
Υπέρβαση προϋπολογισμού								
Επιπτώσεις σε πελάτες / υπαλλήλους								
Υγεία και ασφάλεια								
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού		0	1	1	2	2	3	
Κατάχρηση προσωπικών δεδομένων								
Νομικές και κανονιστικές επιπτώσεις								
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών								
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)	0	0			1	1	1	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων								
Νομική ευθύνη και κυρώσεις								
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ	**15 Λεπτά**	**1 ώρα**	**3 ώρες**	**12 ώρες**	**1 ημέρα**	**2 ημέρες**	**1 εβδομάδα**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**0**	**1**	**1**	**2**	**2**	**3**	
	3							

Τελικός Βαθμός Αποτίμησης Αγαθού		Μέγιστος βαθμός αποτίμησης όλων των σεναρίων
Επίπεδο Επίπτωσης	ΥΨΗΛΟ	

Πίνακας 26: Αγαθό 6 - Απώλεια Διαθεσιμότητας