Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Εκτίμηση αντίκτυπου σχετικά με τα προσωπικά δεδομένα – Μελέτη περίπτωσης

Κωνσταντίνος Μαράντος

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Νοέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Εκτίμηση αντικτύπου σχετικά με τα προσωπικά δεδομένα – Μελέτη περίπτωσης

Κωνσταντίνος Μαράντος

Επιβλέπων Καθηγητής
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

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η διπλωματική διατριβή πραγματεύεται τη νέα διαδικασία της εκτίμησης αντικτύπου σχετικά με τα προσωπικά δεδομένα που συστήνει – και, σε ορισμένες περιπτώσεις, επιβάλλει - για πρώτη φορά ο Γενικός Κανονισμός Προσωπικών Δεδομένων (ΕΕ) 2016/679. Στόχος της διατριβής είναι η πλήρης υλοποίηση μίας εκτίμησης αντικτύπου σε μία περίπτωση επεξεργασίας αρχείων με προσωπικά δεδομένα μέσω υπολογιστικού νέφους, αξιοποιώντας παράλληλα και μία πρόσφατη μεθοδολογία διαχείρισης κινδύνων ασφαλείας, καταδεικνύοντας κατ αυτόν τον τρόπο τα οφέλη που μπορούν να ανακύψουν από έναν τέτοιο συνδυασμό ως προς την ορθή αποτίμηση κινδύνων.

Ειδικότερα, στην παρούσα διατριβή αρχικά αναλύονται βασικές έννοιες του ΓΚΠΔ που χρησιμοποιούνται στη συνέχεια για την εκτέλεση της εκτίμησης αντικτύπου. Ακολούθως, περιγράφονται τα βασικά χαρακτηριστικά του υπολογιστικού συστήματος που βασίζεται στη cloud πλατφόρμας της Office 365 μέσω της οποίας θα γίνει επεξεργασία προσωπικών δεδομένων, ως μελέτη περίπτωσης. Στο επόμενο βήμα θα παρουσιαστεί μία νέα μεθοδολογία που θα περιλαμβάνει τον συνδυασμό της εκτίμησης κινδύνου με εκτίμηση αντικτύπου. Η μέθοδος εκτίμησης κινδύνου που θα αξιοποιηθεί είναι μία πρόσφατη μεθοδολογία του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA), η οποία θα εφαρμοστεί πρώτα στις δεδομένες επεξεργασίες, ώστε να δημιουργηθεί μια βάση δεδομένων για την εκπόνηση της εκτίμησης επιπτώσεων με τη βοήθεια του λογισμικού αξιολόγησης επιπτώσεων ως προς τα προσωπικά δεδομένα. Στο τελικό στάδιο γίνεται αποτίμηση του βαθμού αντιμετώπισης όλων των κινδύνων προστασίας προσωπικών δεδομένων, με προτάσεις μέτρων βελτίωσης.

Summary

The thesis deals with the new process of personal data protection impact assessment (DPIA) introduced – in some cases, as a legal obligation - for the first time by the General Data of Protection Regulation (EU) 2016/679 (GDPR). The goal of the thesis is the development of a full DPIA for a specific personal data process that rests with cloud computing, via utilizing a known security risk assessment methodology. By these means, it becomes evident that incorporating such a methodology in a process of conducting a DPIA provides several benefits since it facilitates the assessment of the security risks.

More precisely, the basic concepts of the GDPR, which are subsequently used to perform the DPIA, are first described. Then the key features of the Office 365 cloud-based computing system that will process personal data, as a case-study, will be analysed. In the next step, a new methodology will be presented that includes the proper combination of a security risk assessment with a data protection impact assessment. The security risk assessment method that is being used is a recent methodology proposed by the European Union Agency for Cybersecurity (ENISA), which is first implemented in the given processes, to create a database for the execution of the impact assessment with the help of an appropriate PIA-impact assessment software. At the final stage, an overall evaluation of the remaining data protection risks is being conducted, whereas improvement measures are being proposed.

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω θερμά των καθηγητή κ. Κωνσταντίνο Λιμνιώτη για τον χρόνο που μου αφιέρωσε, για τις πολύτιμες συγγραφικές, νομικές και τεχνικές συμβουλές του.

Ευχαριστώ του γονείς μου, την αδερφή μου, τον Torsten Weißhaar και τον Marcus Bruns για την στήριξή τους κατά τη διάρκεια της συγγραφής της διπλωματικής αυτής διατριβής.

Περιεχόμενα

Κεφάλαιο 1ο
Εισαγωγή

1.1 Περιγραφή πεδίου και χώρου

Παρατηρώντας το παρελθόν καθίσταται αντιληπτή η έκταση της προόδου και η καθολική εφαρμογή της επιστήμης των πληροφοριών σε όλες τις εκφάνσεις του σύγχρονου τρόπου ζωής. Οι εφαρμογές της πληροφορικής έχουν πλέον επηρεάσει σε υψηλό βαθμό πολλές καθημερινές ανάγκες, όπως η αγορά υλικών αγαθών, η αγορά υπηρεσιών, η ψυχαγωγία, η ενημέρωση και η εκπαίδευση. Σε πολλούς από αυτούς τους τομείς η χρήση εφαρμογών αντικατέστησε τη φυσική παρουσία των ανθρώπων και αυτή η τάση είχε και έχει πολύπλευρα αποτελέσματα που δε γίνονται αισθητά αμέσως. Ο χρόνος και η απόσταση είναι δύο μεγέθη που έχουν επηρεαστεί θετικά από την ανάπτυξη της πληροφορικής. Χάρη στην πληροφορική ο άνθρωπος ξοδεύει λιγότερο χρόνο για τις καθημερινές ανάγκες με αποτέλεσμα να είναι σε θέση να αφιερώσει περισσότερο χρόνο εκεί που πραγματικά το επιθυμεί. Επίσης, η έννοια της απόστασης είναι πλέον σχετική από τη στιγμή που μέσω μιας εφαρμογής μπορεί πλέον κάποιος να αγοράσει ακόμη και ένα αγαθό ή μια υπηρεσία που παλιότερα προσφερόταν μόνο σε άλλη ήπειρο. Το γεγονός της εκμηδένισης της απόστασης θέτει σε νέο πλαίσιο τις έννοιες της αγοράς και της ζήτησης, δεδομένου ότι όλος ο πλανήτης έχει πρόσβαση σε μία παγκοσμιοποιημένη αγορά, όπου η ποικιλία της προσφοράς δεν έχει όρια. Σε αυτό το νέο πλαίσιο πραγματικότητας τα οικονομικά συστήματα - εμμέσως τα κράτη - είναι αναγκασμένα να προσαρμόζονται. Στο εγγύς μέλλον ωστόσο, θα πρέπει να βρουν μηχανισμούς για τη βάση λειτουργίας των εικονικών νομισμάτων. Είναι εύκολα κατανοητό στις παραπάνω περιπτώσεις ότι η πληροφορική ως επιστήμη δίνει λύσεις ή προσφέρει εναλλακτικές στο κοινωνικό σύνολο.

Η αντικατάσταση της φυσικής παρουσίας κρύβει μία αθέατη, τεχνική πλευρά της πληροφορικής, η οποία είναι αθέατη ακόμη στον καθημερινό χρήστη. Η πλευρά αυτή

φέρει το concept της αυθεντικοποίησης. Η αντικατάσταση της φυσικής παρουσίας από το ηλεκτρονικό αποτύπωμα ή την ηλεκτρονική ταυτότητα του χρήστη είναι μία διαδικασία που απαιτεί μία μορφή αυθεντικοποίησης. Συνήθως, όταν το ηλεκτρονικό περιεχόμενο διατίθεται δωρεάν και δεν υπάρχει κάποια μορφή χρηματικής συναλλαγής, τότε η αυθεντικοποίηση είναι απλή και απαιτεί μικρό αριθμό στοιχείων από το χρήστη που θέλει να έχει πρόσβαση. Αυτός ο μικρός αριθμό στοιχείων περιέχει σίγουρα προσωπικά στοιχεία, όπως είναι η ip διεύθυνση του υπολογιστή μας και το email του χρήστη. Εύκολα γίνεται δε η συνεπαγωγή ότι σε μία διαδικτυακή χρηματική συναλλαγή θα απαιτηθούν πολλά περισσότερα στοιχεία από το χρήστη που θα είναι κατά την πλειοψηφία τους προσωπικά. Μία απλή χρηματική συναλλαγή προϋποθέτει ότι ο χρήστης έχει οικειοθελώς κοινοποιήσει πλήθος προσωπικών του στοιχείων σε δύο οργανισμούς, στην τράπεζα και στο online-shop, ώστε να είναι δυνατή η αυθεντικοποίηση του χρήστη από την τράπεζα και από το online-shop. Το σύνολο των προσωπικών στοιχείων, το οποίο διακινείται στο Internet, αποτελεί ακόμα και σήμερα ένα χαοτικό πεδίο που δύσκολα μπορεί να τεθεί σε κανονικά πλαίσια, επειδή είναι δύσκολο να οριστεί ένα παγκόσμιο πλαίσιο στο οποίο θα συμφωνούν κράτη διαφορετικών πολιτισμών και οικονομιών με ετερόκλητες νομοθετικές λειτουργίες. Εκτός της ποσότητας και της ποιότητας των προσωπικών δεδομένων που κυκλοφορούν στο διαδίκτυο, σημαντικό ρόλο παρουσιάζει η ασφαλής αποθήκευση και η νόμιμη επεξεργασία τους.

Η επεξεργασία των προσωπικών δεδομένων αποτελεί ένα πολύ σημαντικό και μοντέρνο θέμα συζήτησης. Τα προσωπικά δεδομένα, ειδικότερα όταν ο όγκος τους είναι μεγάλος, μπορούν να επεξεργαστούν με αποτελέσματα που μπορούν να ερμηνευτούν και να χρησιμοποιηθούν με πολλούς και διάφορους τρόπους. Η στατιστική τους επεξεργασία μπορεί να δημιουργήσει αγοραστικά προφίλ, να αναδείξει συνήθειες και τάσεις, να υπολογίσει με τρομερή ακρίβεια συμπεριφορές και αντιδράσεις κοινωνικών ομάδων, ακόμα και να τις επηρεάσει στοχευμένα. Η δύναμη του φορέα που είναι σε θέση να επεξεργαστεί τον όγκο των προσωπικών δεδομένων, είναι πολύ μεγάλη και η χρήση της πληροφορίας που δημιουργείται από την επεξεργασία υπηρετεί το συμφέρον του. Είναι εύκολο να συμπεράνει κάποιος ότι αυτή η χρήση δεν ακολουθεί κατ' ανάγκη την ηθική ή την νομιμότητα.

Η ανάγκη για την ύπαρξη ενός μοντέρνου και εφαρμόσιμου νομικού πλαισίου που να μπορεί να θεσπίσει κανόνες, για τη χρήση και την επεξεργασία προσωπικών δεδομένων,

οδήγησε την Ευρωπαϊκή Ένωση στο να ψηφίσει τον Απρίλιο του 2016 το Γενικό Κανονισμό για την Προστασία των Δεδομένων 2016/679 [1]. Ο καινούριος αυτός κανονισμός προστατεύει τον χρήστη και θεσπίζει καινούρια δικαιώματα σε σχέση με το προηγούμενο συναφές θεσμικό πλαίσιο. Σε ένα περιβάλλον, στο οποίο οι συναλλαγές και οι υπηρεσίες είναι ηλεκτρονικές, είναι δύσκολο για έναν μεμονωμένο χρήστη που θα βρεθεί σε περίπτωση ανάγκης να αντιμετωπίσει το πρόβλημα. Οι χρήστες με τον καινούριο κανονισμό δεν έχουν μόνο καινούρια δικαιώματα αλλά και συγκεκριμένους τρόπους εξάσκησής τους, μία ευεργετική ρύθμιση υπέρ του χρήστη που εμμέσως ασκεί πίεση στους φορείς ως προς την εφαρμογή του νομικού πλαισίου.

Ο Γενικός Κανονισμός για την Προστασία των δεδομένων προβλέπει μέτρα που σταματούν – ή, τουλάχιστον αυτός είναι ο σκοπός του - την ανεξέλεγκτη επεξεργασία προσωπικών δεδομένων. Η συλλογή και η επεξεργασία των δεδομένων πρέπει πλέον να εκτελούνται βασιζόμενες σε διαδικασίες που προβλέπονται από τα άρθρα του κανονισμού. Κάθε φορέας που φέρει και συλλέγει προσωπικά δεδομένα πρέπει να ακολουθεί πολιτικές ελαχιστοποίησης των προσωπικών δεδομένων και να έχει έναν υπεύθυνο προστασίας προσωπικών δεδομένων. Προβλέπεται επίσης και η εκπόνηση της πολύ σημαντικής εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων. Κάθε φορά που συγκεκριμένες συνθήκες αλλάζουν, κάτω από οποίες εκτελείται επεξεργασία δεδομένων, τότε πρέπει να εκτελείται Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων, για να ελεγχθεί η επίδραση της αλλαγής στα προσωπικά δεδομένα και η επεξεργασία τους.

Σημαντική οικονομική παράμετρος είναι και τα υψηλά πρόστιμα που προβλέπονται σε περίπτωση που οι ελεγχόμενοι φορείς δεν έχουν συμμορφωθεί με τον κανονισμό. Το γεγονός αυτό κινητοποίησε δημόσιο και ιδιωτικό τομέα ως προς την άμεση εφαρμογή του.

Σε γενικές γραμμές η Ευρωπαϊκή Ένωση με την ψήφιση του κανονισμού προσπαθεί να συγχρονιστεί με την ταχύτατη πρόοδο της πληροφορικής και κυρίως του τομέα Data Processing και να προστατέψει ταυτόχρονα του πολίτες της. Τα αποτελέσματα αυτής της προσπάθειας θα συζητηθούν τα επόμενα χρόνια, δεδομένου ότι η υλοποίηση των προβλεπόμενων διαδικασιών απαιτούν χρόνο.

1.2 Ερευνητικό πρόβλημα

Το κύριο χαρακτηριστικό του ερευνητικού προβλήματος είναι η εκτέλεση Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων, όταν η επεξεργασία γίνεται σε

περιβάλλον cloud μέσω της γνωστής εφαρμογής Microsoft Office 365. Η εν λόγω επεξεργασία αφενός γεννά ζητήματα που άπτονται της ιδιωτικότητας και εγκυμονεί κινδύνους ως προς την επεξεργασία προσωπικών δεδομένων, ενώ αφετέρου αποτελεί μία επεξεργασία η οποία συναντάται σε πλήθος οργανισμών, είτε μικρού είτε μεγάλου μεγέθους.

Το πρώτο σκέλος της εν λόγω έρευνας αποτελείται από την Εκτίμηση αντικτύπου, μία νέα και επίκαιρη έννοια που δημιούργησε ο Γενικός Κανονισμός για την Προστασία των Δεδομένων. Συγκεκριμένη και δοκιμασμένη μέθοδος για την εκτέλεσή της δεν υπάρχει ακόμα και η βάση της μεθόδου δίνεται από κρατικές και ευρωπαϊκές οδηγίες.

Το δεύτερο σκέλος αναφέρεται στον χώρο που θα εφαρμοστεί η Εκτίμηση Αντικτύπου, ο οποίος είναι το cloud περιβάλλον. Ο χώρος αυτός είναι πολύ διαφορετικός σε σχέση με ένα τοπικό δίκτυο. Πλέον η πρόσβαση, η επεξεργασία και η αποθήκευση δεν γίνονται τοπικά και παρουσιάζεται μία μεγάλη εξάρτηση του πελάτη προς το σύστημα που τον υπηρετεί.

Ο συνδυασμός της εκτίμησης αντικτύπου σε cloud περιβάλλον θα αναδείξει επίκαιρα θέματα ασφάλειας των δεδομένων, τα οποία θα πρέπει να αντιμετωπιστούν άμεσα, αφού η τάση για χρήση cloud προϊόντων είναι πραγματική.

Δεδομένου ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν έχει – κατά το χρονικό διάστημα εκπόνησης της παρούσας διατριβής - ούτε δύο χρόνια ζωής, ζητήματα όπως η συστηματική εκπόνηση εκτίμησης αντικτύπου για την προστασία προσωπικών δεδομένων σε συστήματα υπολογιστικού νέφους (cloud), αξιοποιώντας παράλληλα μία σύγχρονη μεθοδολογία διαχείρισης κινδύνων, δεν έχουν ακόμα πλήρως εξεταστεί και, ως εκ τούτου, καθίσταται αναγκαία η διερεύνησή τους.

1.2.1 Μεθοδολογία

Η μεθοδολογία που θα αναπτυχθεί στο κεφάλαιο 3ο είναι ανεξάρτητη των εργαλείων που θα χρησιμοποιηθούν στην συγκεκριμένη περίπτωση. Αρχικά θα εκτελεστεί μία αυτόνομη μεθοδολογία διαχείρισης κινδύνων ασφάλειας [2]. Ο σκοπός είναι να αναδειχθούν θέματα ασφάλειας και βελτιωτικά μέτρα, ώστε να υπάρχει μία πραγματική εικόνα του περιβάλλοντος στο οποίο θα εκτελεστεί η εκτίμηση αντικτύπου αλλά και για την προετοιμασία των δεδομένων που θα χρειαστούν. Στη συνέχεια θα ληφθεί απόφαση εκτέλεσης ή μη της ΕΑΠΔ με βάση τις σχετικές κατευθυντήριες γραμμές που απορρέουν από το Γενικό Κανονισμό Προστασίας Δεδομένων. Τα επόμενα βήματα θα εκτελεστούν

μέσω του open-source λογισμικού PIA-Εκτίμηση Αντικτύπου (Έκδοση v2.2.0) [3] που αναπτύχθηκε από το γαλλικό οργανισμό Commission nationale de l'informatique et des libertés (CNIL – Αρχή Προστασίας Δεδομένων της Γαλλίας) μέσω του οποίου θα πραγματοποιηθεί η Εκτίμηση Αντικτύπου. Κατά την διάρκεια αυτής της διαδικασίας θα αναλυθούν οι λόγοι της εκτέλεσης, τα μέτρα προστασίας των δεδομένων και τα θέματα ασφάλειας που βρέθηκαν στο πρώτο μέρος, θα εξεταστούν η απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, θα σχεδιαστούν και θα εφαρμοστούν μέτρα αντιμετώπισης κινδύνων και τέλος θα επαναξιολογηθεί το συνολικό σύστημα.

1.3 Δομή διατριβής

Το 2ο Κεφάλαιο αναφέρεται στο Γενικό Κανονισμό για την Προστασία των Δεδομένων 2016/679. Θα γίνει αρχικά μία ιστορική αναδρομή στην εξέλιξη της ασφάλειας και της ιδιωτικότητας στην επιστήμη της πληροφορικής. Στη συνέχεια θα αναφερθούν οι σημαντικότερες αλλαγές που φέρνει ο Γενικός Κανονισμός για την Προστασία των Δεδομένων 2016/679. Ειδικότερα θα αναλυθούν οι θετικές επιπτώσεις που επιφέρει το άρθρο 25 «Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού», το άρθρο 32 «Ασφάλεια επεξεργασίας» και το άρθρο 35 «Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων».

Στο πρώτο μέρος του 3ου κεφαλαίου γίνεται ανάλυση του πραγματικού project που λειτούργησε ως βάση της παρούσας διπλωματικής εργασίας. Θα αναλυθούν οι λόγοι που οδήγησαν στη λήψη της απόφασης της αλλαγής του υπολογιστικού περιβάλλοντος και τον αρχικό σχεδιασμό. Στη συνέχεια θα συγκριθούν τα τεχνικά χαρακτηριστικά των δομών των 2 περιβαλλόντων.
Στο δεύτερο μέρος θα γίνει ανάλυση των χαρακτηριστικών της Εκτίμησης Αντικτύπου και της μεθοδολογίας της: γιατί και πότε γίνεται, πώς γίνεται, ποια στοιχεία χρειάζονται, πώς χρησιμοποιούνται τα ευρήματα και πως εν τέλη προστατεύονται τα δεδομένα καλύτερα. Αυτά είναι κάποια από τα ερωτήματα που θα απαντηθούν.

Στο πρώτο μέρος του 4ου κεφαλαίου εκτελείται η διαχείριση κινδύνου, βάσει της μεθοδολογίας του ευρωπαϊκού οργανισμού κυβερνοασφάλειας Enisa. Αναλύεται το καινούριο περιβάλλον, εντοπίζονται προβλήματα ασφάλειας και προτείνονται μέτρα αντιμετώπισής τους.

Στο δεύτερο μέρος χρησιμοποιείται το ελεύθερα διαθέσιμο λογισμικό PIA-Εκτίμηση αντικτύπου. Μετά την πρώτη εκτίμηση λαμβάνονται μέτρα για την αντιμετώπιση των κινδύνων. Μετά την εφαρμογή αυτών των αλλαγών, η εκτίμηση αντικτύπου εκτελείται με νέα βελτιωμένα αποτελέσματα.

Στο τελευταίο 5ο κεφάλαιο, το οποίο αποτελεί τον επίλογο της διπλωματικής διατριβής, θα παρουσιαστούν τα συμπεράσματα σχετικά με την επιτυχία του συνδυασμού των δύο μεθόδων, της αξιολόγησης κινδύνου και της εκτίμησης αντικτύπου. Τέλος, θα προταθούν αλλαγές στη διεπαφή (interface) του λογισμικού ανοιχτού κώδικα PIA- Εκτίμηση αντικτύπου στα πλαίσια μελλοντικής έρευνας.

Κεφάλαιο 2ο
Γενικός Κανονισμός για την Προστασία Δεδομένων

2.1 Ιδιωτικότητα και προσωπικά δεδομένα

Σύμφωνα με το Γενικό Κανονισμό για την Προστασία Δεδομένων ορίζεται ένα πλαίσιο μέτρων για την προστασία της ιδιωτικότητας του ατόμου. Η ιδιωτικότητα είναι συνυφασμένη ως έννοια με το δικαίωμα ενός ατόμου ή μιας ομάδας στη μυστικότητα και στην απομόνωσης [4]. Το δικαίωμα της ιδιωτικότητας και η ανάγκη εξάσκησής του έγιναν ακόμα πιο καίρια με την εισχώρηση της τεχνολογίας στην καθημερινή ζωή. Πλέον ο Γενικός Κανονισμός για την Προστασία Δεδομένων όχι μόνο προστατεύει αλλά και δημιουργεί διαδικασίες άσκησης του δικαιώματος αυτού, ενισχύοντας προϋπάρχοντα δικαιώματα αλλά και εισάγοντας καινούρια. Στην επιστήμη της πληροφορικής η προστασία προσωπικών δεδομένων έχει συμβιωτική σχέση με την ιδιωτικότητα. Χωρίς ασφαλή προσωπικά δεδομένα δεν υπάρχει ιδιωτικότητα και το αντίστροφο.

Γενικότερα, προσωπικά δεδομένα ονομάζονται όλα τα δεδομένα που μπορεί να οδηγήσουν άμεσα ή έμμεσα στην ταυτοποίηση ενός ατόμου. Η έννοια των προσωπικών δεδομένων είναι εξαιρετικά ευρεία, ιδιαίτερα δε σε περιβάλλον Διαδικτύου: κάθε διαδικτυακό «ίχνος» ενός χρήστη, το οποίο δύναται, έστω και υπό προϋποθέσεις και με συνδυασμό άλλων πληροφοριών, να οδηγήσει σε αναγνώρισή του αποτελεί προσωπικό του δεδομένο. Με άλλα λόγια, εκτός των προσωπικών δεδομένων, τα οποία χρησιμοποιούνται για την ταυτοποίηση και αυθεντικοποίηση των χρηστών στο διαδίκτυο, υπάρχουν και τα προσωπικά δεδομένα που δημιουργούνται από τη διαδικτυακή δραστηριότητα των ατόμων. Για να γίνει κατανοητό το εύρος των προσωπικών δεδομένων και της δημιουργίας τους, θα γίνει αναφορά στην κατηγοριοποίηση αυτών με βάση τη δικτυακή τους χρήση στα κοινωνικά δίκτυα από τον Schneier [5] (αγγλική ορολογία):

- Service data: Δεδομένα που δίνουν οι χρήστες στο εκάστοτε δίκτυο, το οποίο μπορεί να τα χρησιμοποιήσει (όνομα, ηλικία, αριθμός τραπεζικού λογαριασμού)
- Disclosed data: Δεδομένα που γνωστοποιούνται από τους χρήστες μέσω των λογαριασμών τους.
- Entrusted data: Δεδομένα που γνωστοποιούνται από χρήστη σε τρίτους λογαριασμούς. Είναι παρόμοια δεδομένα με τα disclosed, με τη διαφορά ότι η κυριότητα των entrusted data κατέχεται από τον ιδιοκτήτη του λογαριασμού, στον οποίο δημοσιεύθηκαν και όχι από τον δημιουργό τους.
- Incidental data: Δεδομένα που αφορούν συγκεκριμένο χρήστη και η κυριότητα ανήκει σε τρίτους λογαριασμούς.
- Behavioral data: Δεδομένα που φέρουν πληροφορίες για τις συνήθειες των χρηστών και καταγράφονται από το δίκτυο.
- Derived data: Δεδομένα που αφορούν χρήστες και προέρχονται από επεξεργασία άλλων δεδομένων.

Πολλές από της προαναφερθέντες κατηγορίες περιλαμβάνουν προσωπικά δεδομένα, τα οποία είναι δύσκολο να εντοπιστούν, αφενός επειδή η διάδοσή τους είναι ραγδαία και αφετέρου διότι η κυριότητα των πληροφοριών είναι δυσδιάκριτη. Γίνεται εύκολα κατανοητό ότι η διαχείριση διαδικτυακών δεδομένων - δεδομένου ότι και ο όγκος είναι μεγάλος - παρουσιάζει τρομερές δυσκολίες στη διύλιση των δεδομένων και στην επιλογή νόμιμης επεξεργασίας τους.

Πρέπει επίσης να σημειωθεί ότι, ιδίως δε στην εποχή των μεγάλων δεδομένων (big data), από την ανάλυση προσωπικών δεδομένων μπορούν να εξαχθούν συμπεράσματα για ένα χρήστη (π.χ. προφίλ συμπεριφοράς). Κάθε τέτοια πληροφορία που εξάγεται κατόπιν ανάλυσης δεδομένων αποτελεί και η ίδια, με τη σειρά της, προσωπικό δεδομένο για το χρήστη.

Ο Γενικός Κανονισμός ορίζει τις κατηγορίες τόσο των προσωπικών δεδομένων όσο και των ευαίσθητων προσωπικών δεδομένων, με βάση την φύση τους, έτσι ώστε να γίνεται ευκολότερος ο εντοπισμός τους. Στα βασικά προσωπικά δεδομένα υπάγονται όλες οι πληροφορίες που αφορούν ένα πρόσωπο, όπως ενδεικτικά οι ακόλουθες:

- Προσωπικά Στοιχεία, όπως ονοματεπώνυμο, διεύθυνση κατοικίας, ηλεκτρονική διεύθυνση, τηλεφωνικός αριθμός, προσωπική φωτογραφία, επαγγελματική δραστηριότητα κ.α.
- Οικονομικά στοιχεία, όπως μισθός, τραπεζικές καταθέσεις, ακίνητη περιουσία, τραπεζικές οφειλές κ.α.
- Προσωπική δραστηριότητα, όπως προσωπικές απόψεις, ενδιαφέροντα και φυσικές δραστηριότητες κ.α.

Τα ευαίσθητα προσωπικά δεδομένα, τα οποία είναι και το βασικότερο χαρακτηριστικό της ιδιωτικότητας, σχετίζονται με του κάτωθι τομείς σύμφωνα με τα άρθρα 9 και 10 του ΓΚΠΔ:

- Δεδομένα υγείας
- Ποινικό μητρώο
- Δεδομένα ερωτικής ζωής ή γενετήσιου προσανατολισμού
- Εθνοτική και φυλετική καταγωγή
- Πολιτικές, φιλοσοφικές και θρησκευτικές πεποιθήσεις
- Συνδικαλιστική δραστηριότητα
- Γενετικά δεδομένα
- Βιομετρικά δεδομένα, εφόσον χρησιμοποιούνται με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου

2.2 Βασικοί ορισμοί

Ο ΓΚΠΔ χρησιμοποιεί συγκεκριμένους ορισμούς, οι οποίοι προσδιορίζουν συγκεκριμένες έννοιες και ρόλους σε μία επεξεργασία προσωπικών δεδομένων. Ακολούθως παραθέτουμε τους εν λόγω ορισμούς, δεδομένου ότι οι έννοιες αυτές χρησιμοποιούνται στη συνέχεια στην παρούσα διατριβή:

- «Επεξεργασία προσωπικών δεδομένων»: 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.

- «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.
- «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.
- «Υποκείμενο των δεδομένων»: το φυσικό πρόσωπο στο οποίο αναφέρονται τα προσωπικά δεδομένα.

2.3 Οι αλλαγές που φέρνει ο ΓΚΠΔ

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων έχει ως στόχο την ενίσχυση της προστασίας των προσωπικών δεδομένων των φυσικών προσώπων και της ιδιωτικότητάς τους απέναντι στην αθρόα επεξεργασία των δεδομένων τους και στη χρήση των αποτελεσμάτων της επεξεργασίας για ιδιωτικούς σκοπούς. Ο ΓΚΠΔ, σε σχέση με το προηγούμενο νομικό πλαίσιο (πυλώνας του οποίου ήταν η Οδηγία 95/46/ΕΚ), θεσπίζει καινούρια, αλλά και πιο ενισχυμένα, δικαιώματα των ατόμων, προβλέπει ειδική μέριμνα για τα δεδομένα ευαίσθητων ομάδων, δημιουργεί νέο πλαίσιο διαχείρισης και επεξεργασίας των προσωπικών δεδομένων με διαφανείς ρόλους και ευθύνες, περιορίζει την αυτοματοποιημένη επεξεργασία των δεδομένων, δημιουργώντας εργαλεία για την εκτίμηση αντικτύπου της. Οι βασικότερες αλλαγές που προβλέπει είναι οι ακόλουθες:

- Βασικές αρχές που διέπουν την επεξεργασία δεδομένων (Άρθρο 5 και 6). Οι θεμελιώδεις αυτές αρχές προϋπήρχαν και στο προηγούμενο νομικό πλαίσιο, ωστόσο εισάγεται με τον ΓΚΠΔ η αρχή της λογοδοσίας (άρ. 5, παρ. 2), σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις ανωτέρω αρχές.
- Θέσπιση νέων δικαιωμάτων της πρόσβασης, της διόρθωσης, της διαγραφής, του περιορισμού της επεξεργασίας, της εναντίωσης και της κατάρτισης προφίλ (Άρθρα 15 έως 22).

Ο ΓΚΠΔ παρέχει επίσης και άλλες σημαντικές έννοιες. Πολλές από αυτές αποτελούν «εργαλεία λογοδοσίας», υπό την έννοια ότι επιτρέπουν στον υπεύθυνο επεξεργασίας (ή και τον εκτελούντα την επεξεργασία, σε κάποιες περιπτώσεις) να κάνει απαραίτητες ενέργειες προκειμένου να μπορεί να αποδεικνύει τη συμμόρφωσή του με τις

προϋποθέσεις νομιμότητας. Τα πιο βασικά «εργαλεία λογοδοσίας» είναι τα εξής:

- Προστασία ιδιωτικότητας από το σχεδιασμό και εξ' ορισμού (Privacy by Default and by Design) (Άρθρο 25).
- Εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (Άρθρο 35).
- Οι ρόλοι του υπεύθυνου της προστασίας δεδομένων (Άρθρα 37 έως 39).

Τέλος ο ΓΚΠΔ δίνει έμφαση και στην ασφάλεια της επεξεργασίας, η οποία – πέραν του ότι αποτελεί θεμελιώδη προϋπόθεση νομιμότητας, όπως αναφέρεται στη συνέχεια – μνημονεύεται και σε διάφορα άλλα άρθρα (π.χ. άρ. 32-34).

2.3.1 Βασικές αρχές της νομιμότητα της επεξεργασίας

Οι βασικές αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων βάσει του Άρθρου 5 είναι οι ακόλουθες:

- Νομιμότητα, αντικειμενικότητα και διαφάνεια της επεξεργασίας.
- Ο περιορισμός του σκοπού της επεξεργασίας .
- Η ελαχιστοποίηση των δεδομένων κατά τη συλλογή τους.
- Η ακρίβεια των δεδομένων σε σχέση με την επεξεργασία για την οποία έχουν συλλεχθεί.
- Ο περιορισμός του χρόνου αποθήκευσης των δεδομένων και των αποτελεσμάτων της επεξεργασίας τους.
- Μέριμνα για τη διασφάλιση της ακεραιότητας και εμπιστευτικότητας των δεδομένων.
- Ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει την εφαρμογή των παραπάνω οδηγιών (λογοδοσία).

Στο Άρθρο 6 ορίζονται οι λεγόμενες νομικές βάσεις της επεξεργασίας των προσωπικών δεδομένων. Συγκεκριμένα, η επεξεργασία προσωπικών δεδομένων επιτρέπεται αν συντρέχει μία από τις ακόλουθες περιπτώσεις:
α) το υποκείμενο των δεδομένων έχει συναινέσει (παράσχει συγκατάθεση) 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

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.

2.3.2 Τα νέα δικαιώματα των υποκειμένων των δεδομένων

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων δεν θεσπίζει μόνο καινούρια δικαιώματα αλλά καθορίζει και τους τρόπους εξάσκησής τους. Ο υπεύθυνος προστασίας δεδομένων (ρόλος με συγκεκριμένα καθήκοντα, που ορίζεται στο άρ. 37) είναι πλέον ο συνδετικός κρίκος των υποκειμένων με τα δικαιώματά τους. Αρχικά τα υποκείμενα έχουν το δικαίωμα της πρόσβασης στα δεδομένα τους, καθώς και στις πληροφορίες σχετικά με το σκοπό της επεξεργασίας των δεδομένων τους, με τους αποδέκτες των αποτελεσμάτων της επεξεργασίας, με το χρόνο αποθήκευσης των δεδομένων, με τη δημιουργία προφίλ μέσω της επεξεργασίας κ.α.. Η διόρθωση των δεδομένων, η διαγραφή (δικαίωμα στη λήθη), ο περιορισμός και η εναντίωση της επεξεργασίας (η διαγραφή, ο περιορισμός και η εναντίωση εφαρμόζονται υπό όρους που πρέπει να εξεταστούν) συμπληρώνουν την ολοκλήρωση του πλαισίου δικαιωμάτων των υποκειμένων, προσδίδοντας διαφάνεια στην επεξεργασία.

2.3.3 Προστασία ιδιωτικότητας από το σχεδιασμό και εξ' ορισμού

Ο υπεύθυνος επεξεργασίας οφείλει όχι μόνο κατά τον σχεδιασμό της επεξεργασίας αλλά και κατά τη διάρκειά της να λαμβάνει τα κατάλληλα μέτρα προστασίας των προσωπικών δεδομένων, όπως η ελαχιστοποίηση των δεδομένων.

Επίσης πρέπει να διασφαλίζει την εξ' ορισμού νόμιμη επεξεργασία των δεδομένων. Μία τέτοια πρακτική συντελείται, όταν ο σκοπός της επεξεργασίας παραμένει αναλλοίωτος και γίνεται επεξεργασία μόνο των απαραίτητων δεδομένων που είναι απαραίτητα. Το

μέτρο αυτό έχει μεγάλο αντίκτυπο στην ανάπτυξη τόσο των λογισμικών όσο και hardware λύσεων, καθότι πλέον πρέπει να εφαρμόζονται μέτρα προστασίας των δεδομένων φιλικότερα στον χρήστη από τα αρχικά στάδια της υλοποίησης του συστήματος επεξεργασίας και όχι στο τελικό στάδιο ανάλυσης του αποτελέσματος.

2.3.4 Ψευδωνυμοποίηση των δεδομένων

Η ψευδωνυμοποίηση των δεδομένων εφαρμόζεται για να διασφαλίζεται η προστασία των προσωπικών δεδομένων κατά την επεξεργασία, ειδικότερα σε περιπτώσεις που ο σκοπός της επεξεργασίας αλλάζει και εξετάζεται η συμβατότητα της επεξεργασίας με τον αρχικό σκοπό. Επίσης η ψευδωνυμοποίηση χρησιμοποιείται συχνά για στατιστικούς και επιστημονικούς σκοπούς. Τεχνικές ψευδωνυμοποίησης εφαρμόζονται και στο σχεδιασμό λογισμικών, ώστε να επιτυγχάνεται η προστασία των δεδομένων εξ' ορισμού.

2.3.5 Εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων

Η εκτίμηση αντικτύπου (ΕΑΠΔ) είναι μία διαδικασία που αναλύει τους κινδύνους της επεξεργασίας προσωπικών δεδομένων. Μια ΕΑΠΔ δεν εκτελείται με σκοπό εκμηδένισης του ρίσκου αλλά για να αναδείξει παθογένειες και θέματα ασφάλειας του συστήματος επεξεργασίας. Επιπλέον προλαμβάνει προβλήματα που εντοπίζονται σε αρχικά στάδια σχεδιασμού της επεξεργασίας και συμμορφώνει τον οργανισμό ως προς τις οδηγίες του ΓΚΠΔ. Η εκτέλεση μιας ΕΑΠΔ βελτιώνει το σύστημα επεξεργασίας και την ασφάλεια του γενικότερου υπολογιστικού δικτύου, τις πολιτικές διαχείρισης και αποθήκευσης των δεδομένων, καθώς και συμμορφώνει την εταιρία με τις διατάξεις του ΓΚΠΔ.

Σύμφωνα με το άρθρο 35 παρ.3 του ΓΚΠΔ, η εκτέλεση μια εκτίμησης αντικτύπου απαιτείται, όταν η επεξεργασία ανήκει σε κάποιο από τα τρία ακόλουθα πλαίσια:

- Συστηματική, εκτεταμένη και αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, η οποία δημιουργεί προφίλ χρηστών, πάνω στην οποία βασίζονται έννομες αποφάσεις που επηρεάζουν άμεσα ή έμμεσα τα υποκείμενα.
- Επεξεργασία μεγάλης κλίμακας ευαίσθητων δεδομένων
- Συστηματική επεξεργασία μεγάλης κλίμακας δημοσίων χώρων

Υπάρχουν επίσης σκοποί και τρόποι επεξεργασίας με υψηλή πιθανότητα παρουσίασης κινδύνων για τους οποίους ενδείκνυται η εκτέλεση αντικτύπου σχετικά με την επεξεργασία των δεδομένων και είναι οι εξής [6]:

- Επεξεργασία ευαίσθητων προσωπικών δεδομένων με σκοπό την αξιολόγηση και την δημιουργία προφίλ που θα οδηγήσει σε πρόβλεψη συμπεριφοράς των υποκειμένων.
- Επεξεργασία προσωπικών δεδομένων με σκοπό τη λήψη αποφάσεων που επηρεάζουν έμμεσα ή άμεσα τα υποκείμενα.
- Επεξεργασία δεδομένων που προκύπτουν από συστηματική παρακολούθηση και των υποκειμένων που συχνά γίνεται και χωρίς συγκατάθεση.
- Επεξεργασία εξαιρετικά ευαίσθητων προσωπικών δεδομένων.
- Επεξεργασία προσωπικών δεδομένων σε μεγάλη κλίμακα.
- Επεξεργασία προσωπικών δεδομένων που προέχονται από ταυτοποίηση και ένωση διαφορετικών βάσεων δεδομένων, οι οποίες έχουν συλλεχθεί και επεξεργαστεί για διαφορετικούς σκοπούς.
- Επεξεργασία προσωπικών δεδομένων που ανήκουν σε ευαίσθητες κοινωνικές ομάδες.
- Επεξεργασία προσωπικών δεδομένων μέσω καινούριων τεχνολογιών που επηρεάζουν την συλλογή, την επεξεργασία και την αποθήκευση των δεδομένων.
- Επεξεργασία προσωπικών δεδομένων που δεν προσφέρουν στα υποκείμενα τρόπους άσκησης των δικαιωμάτων τους.

Η ομάδα εκπόνησης και η ακριβής διαδικασία της ΕΑΠΔ δεν ορίζονται αυστηρά από τον ΓΚΠΔ, γεγονός που αφήνει περιθώρια στη σύνθεση της ομάδας αλλά στο σχεδιασμό της διαδικασίας. Η ομάδα που θα εκτελέσει την ΕΑΠΔ θα πρέπει να αποτελείται από μέλη με διαφορετικό γνωσιακό υπόβαθρο, επειδή θα απαιτηθεί συνδυασμός νομικών, πληροφοριακών και οργανωτικών ικανοτήτων. Ο υπεύθυνος προστασίας δεδομένων, ένα τουλάχιστον στέλεχος του τμήματος πληροφορικής, ένα τουλάχιστον στέλεχος της ομάδας που εκτελεί την επεξεργασία δεδομένων και τέλος οι νομικοί εκπρόσωποι της εταιρίας και των υποκειμένων της επεξεργασίας απαρτίζουν μία προτεινόμενη δομή της ομάδας. Η συγκεκριμένη σύσταση συνδυάζει τα γνωσιακά αντικείμενα που αναφέρθηκαν. Η διαδικασία εκπόνησης της ΕΑΠΔ θα αναλυθεί στο επόμενο κεφάλαιο.

2.3.6 Υπεύθυνος προστασίας δεδομένων

Ο υπεύθυνος προστασίας δεδομένων είναι μία οργανική θέση που κατέχει την εποπτεία όλων των διαδικασιών που αφορούν τα προσωπικά δεδομένα. Διαδικασίες, όπως συλλογή, επεξεργασία και αποθήκευση δεδομένων οφείλουν πλέον να ακολουθούν

εγκεκριμένα κανονιστικά πλαίσια. Ειδικότερα ο υπεύθυνος προστασίας δεδομένων έχει τις ακόλουθες αρμοδιότητες [7]:

- Εποπτεύει τη διαδικασία της επεξεργασίας δεδομένων
- Ελέγχει τη συμμόρφωση της επεξεργασίας δεδομένων με τον ΓΚΠΔ
- Ενημερώνει και συμβουλεύει τους εκτελούντες την της επεξεργασίας και τους υπευθύνους της επεξεργασίας για τις υποχρεώσεις που απορρέουν από τη νομοθεσία.
- Συμμετέχει σε όλα τα στάδια της εκτίμησης αντικτύπου και αποφασίζει για την αναγκαιότητα και την μεθοδολογία και ελέγχει το αποτέλεσμά της.
- Είναι ο συνδετικός κρίκος της εταιρίας με την Αρχή Προστασίας Δεδομένων και διαχειρίζεται τα ζητήματα που προκύπτουν μεταξύ τους.
- Τα υποκείμενα των δεδομένων πρέπει να είναι σε θέση μέσω του υπεύθυνου προστασίας δεδομένων να ασκούν τα δικαιώματά τους.
- Πρέπει να συμβουλεύει τη διοίκηση για μέτρα που αφορούν στη συμμόρφωση της εταιρίας στο Γενικό Κανονισμό.
- Έχει συμβουλευτικό ρόλο στη δημιουργία ρεαλιστικού πλάνου διαχείρισης ρίσκου και στο σχεδιασμό αρχείου των διαδικασιών και επεξεργασιών που εμπεριέχουν προσωπικά δεδομένα.

Κεφάλαιο 3ο
Προσωπικά δεδομένα: Εκτίμηση αντικτύπου

3.1 Ανάλυση της επεξεργασίας

Η επεξεργασία προσωπικών δεδομένων η οποία αποτέλεσε αντικείμενο της παρούσας έρευνας είναι πραγματική. Για λόγους εμπιστευτικότητας δεν θα ονομαστούν ούτε οι χώρες ούτε και τα είδη των βιομηχανιών. Συγκεκριμένα, το συνολικό έργο (project) είναι πραγματικό και εκτελέστηκε σε εταιρικό περιβάλλον πάνω σε ένα υπολογιστικό δίκτυο τριών (3) εργοστασίων, δύο (2) εκ των οποίων βρίσκονται στη Χώρα Α και το τρίτο στη Χώρα Β, οι οποίες ανήκουν στην ευρωπαϊκή ένωση. Η επιπλέον ανάλυση των τεχνικών χαρακτηριστικών θα βοηθήσουν στο σχεδιασμό μέτρων σε περίπτωση κινδύνου και στην εκτίμηση κινδύνου ENISA και στη ΕΑΠΔ.

3.2 Αιτίες και αφορμή

Τα τελευταία 2 χρόνια άρχισαν να εμφανίζονται αιτήματα (Tickets) στο Helpdesk σύστημα της εταιρίας (SysAid) από πολλούς χρήστες, τα οποία είχαν ως κοινό χαρακτηριστικό τη λανθασμένη δομή του file Server. Τα αιτήματα σχετίζονταν με την ύπαρξη πολλών φακέλων που είχαν δημιουργηθεί σε λάθος μέρη και με λανθασμένη εξουσιοδότηση. Το γεγονός αυτό ανέδειξε δύο προβλήματα: Το πρώτο έγκειται στη μεγάλη κατανάλωση εργασιακού χρόνου για την αναζήτηση εγγράφων, μειώνοντας έτσι την αποδοτικότητα των υπαλλήλων, και το δεύτερο στη λανθασμένη εξουσιοδότηση πρόσβασης χρηστών σε φακέλους, εγείροντας αυτομάτως ζητήματα ασφάλειας και εμπιστευτικότητας δεδομένων.

Στο file Server υπάρχουν κυρίως 2 ειδών φάκελοι:

- Προσωπικοί φάκελοι. Σε κάθε χρήστη αντιστοιχεί ένας προσωπικός φάκελος. Πρόσβαση σε κάθε προσωπικό φάκελο έχει ο αντίστοιχος χρήστης και ο διαχειριστής του δικτύου.
- Φάκελοι τμημάτων, φάκελοι Project και γενικότερα κοινοί φάκελοι, στους οποίους έχουν εξουσιοδότηση ομάδες χρηστών.

Ως απόρροια των ανωτέρω, η εταιρεία ξεκίνησε project με σκοπό την εύρεση μιας εναλλακτικής μορφής διαχείρισης αρχείων για τη μελλοντική αντικατάσταση του υπάρχοντος file Server. Οι εναλλακτικές αρχιτεκτονικές ήταν η εγκατάσταση ενός καινούριου file Server με νέα δομή φακέλων και η αυστηρότερη διαχείριση πρόσβασης καθώς και η εγκατάσταση καινούριου λογισμικού διαχείρισης αρχείων σε περιβάλλον cloud. Η αφορμή δόθηκε, όταν η Microsoft ανακοίνωσε ότι η υποστήριξη της Microsoft Office 2010 σταματάει στις 13 Οκτωβρίου 2020 [8]. Αυτό σημαίνει ότι το λογισμικό θα σταματήσει να λαμβάνει ενημερώσεις ασφάλειας (security updates), γεγονός που θέτει σε κίνδυνο το εταιρικό δίκτυο. Το γεγονός αυτό οδήγησε στην απόφαση της εγκατάστασης του λογισμικού Microsoft Office 365, το οποίο εκτός του ότι αντικαθιστούσε το πακέτο εφαρμογών της Office 2010, παρείχε επιπλέον και εφαρμογές διαχείρισης και αποθήκευσης αρχείων που θα οδηγούσαν στην κατάργηση του υπάρχοντος file Server. Οι εφαρμογές αυτές ήταν οι Microsoft Teams και OneDrive.

Η εφαρμογή OneDrive προσφέρει σε κάθε χρήστη ξεχωριστά αποθηκευτικό χώρο στο cloud της Microsoft και κάποιες επιπλέον υπηρεσίες, όπως η αυτόματη αποθήκευση, η δημιουργία εκδόσεων κάθε εγγράφου, η δυνατότητα επαναφοράς σβησμένων εγγράφων, η δυνατότητα μοιράσματος αρχείων και η γραμμή εύρεσης, η οποία ψάχνει και το περιεχόμενο των αρχείων. Στόχος ήταν η αντικατάσταση των προσωπικών φακέλων από τη συγκεκριμένη εφαρμογή.

Η εφαρμογή Microsoft Teams είναι μια πλατφόρμα, πάνω στην οποία οι χρήστες μπορούν να εργάζονται ομαδικά. Τα κυριότερα χαρακτηριστικά είναι τα ζωντανά κανάλια συνομιλιών - ακόμη και με χρήστες εκτός της domain - ο χώρος επεξεργασίας αρχείων, ο οποίος επιτρέπει στα μέλη της ομάδας να επεξεργάζονται ταυτόχρονα τα αρχεία τους και η διαχείριση των καθηκόντων των μελών κάθε ομάδας. Επιπλέον η εφαρμογή αυτή λειτουργεί και ως πλατφόρμα που υποστηρίζει διαφορετικά λογισμικά της Microsoft καθώς και τρίτων κατασκευαστών.

3.2.1 Τεχνικά χαρακτηριστικά της Microsoft Office 2010

Κατά τη διάρκεια της εγκατάστασης του υπολογιστικού συστήματος, το οποίο απαιτούνταν από την καινούρια εφαρμογή, παρατηρήθηκε ότι η πολυπλοκότητα στο τοπικό δίκτυο ήταν αρκετά υψηλότερη σε σχέση με την προηγούμενη εφαρμογή. Η καινούρια κατάσταση ανέδειξε καινούρια θέματα ασφάλειας και πρόσβασης. Η δομή της Microsoft Office 2010 αποτελούταν από δύο (2) Microsoft Exchange Servers 2010, ένα για κάθε χώρα. Η δομή ήταν αρκετά απλή. Οι Servers ήταν έτσι συνδεδεμένοι μεταξύ τους, ώστε οι λίστες των διευθύνσεων των χρηστών και των δύο πλευρών να είναι ανανεωμένες καθημερινά.

3.2.2 Τεχνικά χαρακτηριστικά της Microsoft Office 365

Η έκδοση της Office 365 λειτουργεί πάνω σε μία δομή από Servers On-Premise σε συνδυασμό με Online Servers. Οι διαχειριστές μέσω της πλατφόρμας στο cloud έχουν πρόσβαση στα λεγόμενα admin portals των ακολούθων εφαρμογών:

- Security and compliance
- Azure Active directory online (free edition)
- Exchange online
- SharePoint Online
- Teams
- OneDrive

Η εφαρμογή για να λειτουργήσει σωστά χρειαζόταν την υποστήριξη των ακολούθων τοπικών Servers:

- Δύο (2) Exchange Servers: Για την εγκατάσταση της Microsoft Office 365 είναι αρχικά αναγκαίοι δύο (2) Microsoft Exchange Servers 2016, οι οποίοι θα εκτελέσουν το mail migration, διότι οι Microsoft Exchange Servers 2010 δεν ήταν συμβατοί. Μετά το τέλος του migration θα απεγκαταστηθούν οι παλιοί Exchange Servers 2010. Οι 2 καινούριοι Microsoft Exchange Servers 2016 θα παραμείνουν συνδεμένοι με τον Exchange Online. Ο λόγος είναι το anonymous relay των τοπικών exchange Servers που δίνει τη δυνατότητα σε λογισμικά και δικτυακές συσκευές να παράγουν και να στέλνουν μη κρυπτογραφημένα emails εντός της domain, σε αντίθεση με τον Exchange Online που δημιουργεί και διαχειρίζεται μόνο κρυπτογραφημένα emails.
- 2 Azure Servers: Οι Microsoft Azure Servers συγχρονίζουν τα Active Directories των τοπικών domain controllers με τον Azure Active Directory Online κάθε 30

λεπτά, έτσι ώστε οι ταυτότητες των χρηστών και τα security/distribution groups να είναι πάντα ανανεωμένα.

- Τρεις (3) ADFS Servers: Για την αυθεντικοποίηση επιλέχθηκε η εγκατάσταση 3 Active Directory Federation Services Servers, δύο (2) στη Χώρα Α της ευρωπαϊκής ένωσης και ένας (1) στη Χώρα Β της ευρωπαϊκής ένωσης . Όταν ο χρήστης εκτελεί μια εφαρμογή της Office 365 και βρίσκεται εντός του τοπικού δικτύου, τότε χρησιμοποιείται η τεχνολογία Single Sign On και ο χρήστης έχει πρόσβαση στην εφαρμογή με αυτόματη αυθεντικοποίηση από τους ADFS Servers. Όταν ο χρήστης βρίσκεται εκτός δικτύου, τότε το αίτημα αυθεντικοποίησης που δέχεται ο Azure Active Directory Online το ανακατευθύνει στη σελίδα αυθεντικοποίησης του WAP Server, ο οποίος στέλνει με την σειρά του το αίτημα στους ADFS Servers.
- 1 WAP Server: Ο WAP Server είναι ο μοναδικός τοπικός Server, ο οποίος είναι προσβάσιμος μέσω διαδικτύου και λειτουργεί ως host της σελίδας αυθεντικοποίησης για τους εξωτερικούς χρήστες.

3.2.3 Ανάλυση της επεξεργασίας προσωπικών δεδομένων

Στην εξεταζόμενη περίπτωση η επεξεργασία προσωπικών δεδομένων πραγματοποιείται από το τμήμα προσωπικού για την εκτέλεση της μισθοδοσίας και από το οικονομικό τμήμα για την κατάρτιση στατιστικών αναλύσεων επί των προσωπικών. Το λογισμικό που δημιουργεί τις λίστες μισθοδοσίας δέχεται αρχεία excel με τα απαιτούμενα προσωπικά δεδομένα των υπαλλήλων ως δεδομένα. Η δημιουργία, η επεξεργασία και η αποθήκευση των δεδομένων αυτών θα γίνεται στο cloud. Το ίδιο ισχύει και για τις στατιστικές αναλύσεις του οικονομικού τμήματος.

3.3 Microsoft Office 365 Vs ΕΑΠΔ

Κατά την διάρκεια την σύνταξης της παρούσας μεταπτυχιακής διατριβής υπάρχουν στην Γερμανία ανοιχτά θέματα που αφορούν την επεξεργασία προσωπικών δεδομένων στην Office 365. Οι πρώτες αμφιβολίες όσον αφορά τη διαφάνεια της επεξεργασία προσωπικών δεδομένων στο Microsoft cloud είχαν εκφραστεί από την Αρχή προστασίας δεδομένων του γερμανικού κρατιδίου της Έσσης [9]. Σύμφωνα με την συγκεκριμένη αρχή, η Microsoft δεν έχει δώσει συγκεκριμένες απαντήσεις σε ερωτήματα που αφορούν τις διαδικασίες της εξουσιοδότησής και διαχείρισης ρόλων που διέπουν το cloud

περιβάλλον της. Συνεχίζοντας η Αρχή έθεσε ερωτήσεις για την πολιτική πρόσβασης σε ευαίσθητα προσωπικά δεδομένα μαθητών που αποθηκεύονται στο cloud και για το αν οι αμερικάνικες αρχές έχουν το δικαίωμα να αποκτήσουν πρόσβαση σε τέτοιας φύσεως δεδομένα και υπό ποιες συνθήκες. Ένα ακόμα θέμα μη διαφανούς επεξεργασίας δεδομένων ανέδειξε η Αρχή προστασίας δεδομένων της Βαυαρίας. Η εφαρμογή MyAnalytics που ενεργοποιείται πολλές φορές αυτόματα με την ενεργοποίηση άδειας της Office 365 έχει τη δυνατότητα δημιουργία και αποστολή δεδομένων τηλεμετρίας. Η Microsoft δεν έχει ακόμα απαντήσει σε ερωτήσεις πάνω στο είδος των δεδομένων που συλλέγονται και στέλνονται και το είδος της επεξεργασίας στην οποία υπόκεινται.

Στην περίπτωση της διπλωματικής διατριβής η συγκεκριμένη εφαρμογή είναι απενεργοποιημένη και ο έλεγχος της επεξεργασίας των προσωπικών δεδομένων θα επικεντρωθεί στο υπολογιστικό εταιρικό σύστημα και όχι γενικά στο cloud περιβάλλον.

3.4 Ανάλυση διαδικασίας της ΕΑΠΔ

Η μεθοδολογία που θα εφαρμοστεί στη συγκεκριμένη περίπτωση βασίζεται στην εκτίμηση ρίσκου με την μεθοδολογία του Enisa, η οποία αρχικά θα παράγει ένα σύνολο πληροφοριών πάνω στο οποίο θα βασίσουμε την ΕΑΠΔ. Με τη χρήση του λογισμικού ανοικτού κώδικα PIA-Εκτίμηση αντικτύπου (v2.2.0), η οποία έχει αναπτυχθεί από γαλλική Αρχή Προστασίας Δεδομένων, θα γίνει εμβάθυνση στα δεδομένα, στους κινδύνους και στα μέτρα που αφορούν άμεσα την επεξεργασία προσωπικών δεδομένων. Η διαδικασία ακολουθεί τις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για την προστασία δεδομένων. Η συγκεκριμένη ομάδα είχε συσταθεί με το άρθρο 29 της οδηγίας 95/46/ΕΚ, αποτελούνταν από εκπροσώπους των αρχών προστασίας δεδομένων όλων των Κρατών-Μελών και εξέδιδε, μεταξύ άλλων, γνώμες για ειδικά θέματα εφαρμογής της νομοθεσίας περί προσωπικών δεδομένων (πλέον έχει αντικατασταθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, το οποίο θεσπίζεται στο ΓΚΠΔ).

Τα ακόλουθα βήματα αποτελούν μία διαδικασία, η οποία είναι ανεξάρτητη των μεθοδολογιών που εφαρμόστηκαν. Ακολουθώντας τα παρακάτω βήματα, μπορεί ο εκτελών την ΕΑΠΔ να μην αποφασίσει τη χρήση του λογισμικού PIA και την εκτίμηση κινδύνου ENISA αλλά να διαλέξει τις δικές του μεθοδολογίες. Τέλος θα πρέπει να σημειωθεί ότι θα αναλυθούν ταυτόχρονα δύο επεξεργασίες με δύο διαφορετικούς

σκοπούς. Επειδή οι επεξεργασίες αυτές γίνονται πάνω στο ίδιο υπολογιστικό σύστημα και θα ακολουθήσουν τα ίδια διαδικαστικά βήματα, θα ελεγχθούν παράλληλα αλλά θα υπάρξουν στο τέλος και στοχευμένα μέτρα για κάθε περίπτωση αν κρίνεται αναγκαίο.

3.4.1 1ο Βήμα: Αξιολόγηση κινδύνου (Μεθοδολογία ENISA)

Αρχικά εκτελέστηκε η αξιολόγηση κινδύνου και τα μέτρα ασφάλειας για τα προσωπικά δεδομένα. Σκοπός είναι η δημιουργία μιας βάσης πληροφοριών που θα μας διευκολύνει στην ομαδοποίηση των δεδομένων, των μέτρων και των κινδύνων. Η μεθοδολογία του ENISA μας επιτρέπει να συλλέξουμε τις βασικές πληροφορίες για να σχεδιάσουμε μία πρώτη επισκόπηση της επεξεργασίας των προσωπικών δεδομένων. Ακολούθως γίνεται μία πρώτη αξιολόγηση των επιπτώσεων σε περίπτωση απώλειας της εμπιστευτικότητας, ακεραιότητας και αξιοπιστίας των δεδομένων. Τελευταίο πολύ σημαντικό συμπέρασμα της αξιολόγησης κινδύνου είναι οι κίνδυνοι που ανιχνευθήκαν καθώς και τα προτεινόμενα μέτρα ασφάλειας.

3.4.2 2ο Βήμα: Απόφαση για την εκτέλεση της ΕΑΠΔ

Από τη συλλογή των πληροφοριών της επεξεργασίας των προσωπικών δεδομένων σε συνδυασμό με την ανίχνευση κινδύνων μέσω του πρώτου βήματος, η ομάδα που είναι υπεύθυνη για την εκτέλεση της ΕΑΠΔ μπορεί να διακρίνει, αν η επεξεργασία εμπίπτει σε μία από τις περιπτώσεις που περιέγραψε η ομάδα εργασίας του άρθρου 29 στις σχετικές κατευθυντήριες γραμμές της. Στη συγκεκριμένη περίπτωση η επεξεργασία ανήκει στην κατηγορία «Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων». Η επεξεργασία αλλάζει χώρο και μέσο διεξαγωγής. Το περιβάλλον cloud αποτελεί μία νέα τεχνολογική πλατφόρμα εφαρμογών, στην οποία η πρόσβαση των χρηστών και η αποθήκευση των δεδομένων γίνονται με διαφορετικό τρόπο.

3.4.3 3ο Βήμα: Κύρια ανάλυση της επεξεργασίας των προσωπικών δεδομένων

Σε αυτό το βήμα ουσιαστικά ξεκινάει η εκτέλεση της ΕΑΠΔ με την ανάλυσης της επεξεργασίας δεδομένων. Ο Γενικός Κανονισμός εισάγει 4 βασικές πτυχές της επεξεργασίας δεδομένων, τη φύση, την έκταση, το πλαίσιο και το σκοπό της

επεξεργασίας των δεδομένων. Τα βασικά χαρακτηριστικά της κάθε πτυχής είναι συγκεντρωμένα στην κάτωθι λίστα.

- Φύση της επεξεργασίας
    - Ο τρόπος συλλογής και επεξεργασίας δεδομένων.
    - Ο χώρος αποθήκευσης των δεδομένων.
    - Το πλαίσιο λειτουργίας της ομάδας που έχει πρόσβαση στα στοιχεία και εκτελεί την επεξεργασία.
    - Τα λογισμικά με τα οποία εκτελείται η επεξεργασία.
- Έκταση της επεξεργασίας
    - Το είδος και το μέγεθος των προσωπικών δεδομένων.
    - Το μέγεθος του συνόλου των υποκειμένων της επεξεργασίας.
    - Η συχνότητα και η διάρκεια της επεξεργασίας.
- Πλαίσιο της επεξεργασίας
    - Η σχέση ανάμεσα στον υπεύθυνο και στα υποκείμενα της επεξεργασίας.
    - Η δυνατότητα των υποκειμένων να ελέγξουν τα δεδομένα τους.
    - Εφαρμογή συγκεκριμένων προτύπων επεξεργασίας.
    - Διαφάνεια των ρόλων του εκτελούντος την επεξεργασία, του υπευθύνου της επεξεργασίας και του υπεύθυνου της προστασίας των προσωπικών δεδομένων.
- Σκοπός της επεξεργασίας
    - Ο λόγος για τον οποίο η εταιρία ή ο οργανισμός επεξεργάζεται προσωπικά δεδομένα.
    - Ύπαρξη νομικών δεσμεύσεων που επιβάλλουν την επεξεργασία.
    - Έλεγχος των επιπτώσεων της επεξεργασίας στα υποκείμενα και στον υπεύθυνο της επεξεργασίας.

3.4.4 4ο Βήμα: Ανάγκη και αναλογικότητα της επεξεργασίας

Στο βήμα αυτό ελέγχεται βαθύτερα η φύση της επεξεργασίας, ως προς την συλλογή δεδομένων και το πλαίσιο της επεξεργασίας, καθώς και ως προς τους υπάρχοντες μηχανισμούς που έχουν τα υποκείμενα για την άσκηση των δικαιωμάτων τους. Ειδικότερα πρέπει να αναλυθούν οι διαδικασίες που εξυπηρετούν την ελαχιστοποίηση των δεδομένων, το οποίο σημαίνει ότι πρέπει συλλέγονται τα ελάχιστα, αναγκαία και έγκυρα δεδομένα που απαιτούνται από την επεξεργασία. Επίσης πρέπει να προβλέπονται

μηχανισμοί που διευκολύνουν την άσκηση των δικαιωμάτων της διαγραφής, της πρόσβασης, της διόρθωσης, της εναντίωσης, του περιορισμού, της ενημέρωσης και της συγκατάθεσης.

3.4.5 5ο Βήμα: Εφαρμοζόμενα Μέτρα προστασίας

Σε αυτό το στάδιο θα συγκεντρωθούν όλα τα μέτρα προστασίας του συστήματος που υποστηρίζει την επεξεργασία των δεδομένων. Οι κυριότερες πολιτικές ασφάλειας είναι οι ακόλουθες:

- Πολιτική ασφάλειας κωδικών
- Πολιτική προστασίας και ενημέρωσης των υπολογιστών και υπολογιστικών κέντρων (Hardware - Software)
- Πολιτική πρόσβασης και αυθεντικοποίησης στο δίκτυο
- Σχέδιο προστασίας από κυβερνοεπιθέσεις και κακόβουλα λογισμικά
- Ανάλυση διαδικασίας εξουσιοδότησης των χρηστών
- Έλεγχος φυσικής πρόσβασης
- Πρόγραμμα ενημέρωσής και εκπαίδευσης χρηστών
- Ανάλυσης διαδικασίας των αντιγράφων ασφαλείας
- Κρυπτογράφηση εμπιστευτικών αρχείων
- Διαχείριση φυσικών καταστροφών

Επίσης θα πρέπει να αναφερθούν μέτρα που δεν εφαρμόζονται αλλά θα μπορούσαν να είχαν θετικό αντίκτυπο στο σύστημα της επεξεργασίας.

3.4.6 6ο Βήμα: Εντοπισμός Κινδύνων

Η προγενέστερη εικόνα των κινδύνων και της πιθανότητάς τους μέσω της εκτίμησης κινδύνου του ENISA διευκολύνει τη σύνθεση των δεδομένων του τρίτου, του τέταρτου και του πέμπτου βήματος. Η ομάδα που εκτελεί τη ΕΑΠΔ εκτιμά την καταλληλόλητα και την πληρότητα των μέτρων του πέμπτου βήματος στην προστασία των δεδομένων και των μηχανισμών του τρίτου και τέταρτου βήματος. Η κριτική αυτή διαδικασία αναδεικνύει και καταγράφει τους κινδύνους και τις περιοχές, στις οποίες εμφανίζονται.

3.4.7 7ο Βήμα: Ανάλυση Κινδύνων

Αρχικά αναλύεται η επίπτωση, η σοβαρότητα και η πιθανότητα εμφάνισης κάθε κινδύνου ξεχωριστά. Στη συνέχεια, ομαδοποιούνται οι κίνδυνοι ως προς το είδος των επιπτώσεών τους, δηλαδή ως προς το είδος απώλειας που μπορεί να προξενήσουν. Δημιουργείται δηλαδή ένα πλαίσιο αξιολόγησης της σοβαρότητας και της πιθανότητας των απωλειών της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Σε τελικό στάδιο αποφασίζονται οι περιοχές ρίσκου που είναι βιώσιμες και ελεγχόμενες, όπως και οι περιοχές στις οποίες πρέπει να σχεδιαστούν καινούρια μέτρα ή να βελτιωθούν τα υπάρχοντα.

3.4.8 8ο Βήμα: Νέα μέτρα περιορισμού κινδύνου και συμμόρφωσης

Εκπόνηση και εφαρμογή νέων μέτρων και πολιτικών ασφάλειας για την αντιμετώπιση των ανοιχτών θεμάτων ασφαλείας του συστήματος επεξεργασίας.

3.4.9 9ο Βήμα: Επαλήθευση των αποτελεσμάτων των μέτρων και επικύρωση

Επαλήθευση των βελτιώσεων της επεξεργασίας δεδομένων και της συμμόρφωσης του συστήματος επεξεργασίας με τον ΓΚΠΔ. Επικύρωση της ΕΑΠΔ από τις συμμετέχουσες ομάδες ή αρχές.

Κεφάλαιο 4ο
Εκτίμηση αντικτύπου και αξιολόγηση κινδύνων

Στο παρόν κεφάλαιο θα πραγματοποιήσουμε, για την περίπτωσή μας, μία ανάλυση κινδύνων ασφαλείας, ακολουθώντας τη σχετική μεθοδολογία του οργανισμού Enisa [2]. Η μεθοδολογία αυτή απευθύνεται ιδίως σε μικρομεσαίες επιχειρήσεις (Small and Medium-sized Enterprises – SMEs) και παρέχει μία συστηματική διαδικασία για μία ορθή διαδικασία διαχείρισης κινδύνων ασφαλείας, όταν το αγαθό το οποίο θέλουμε να προστατεύσουμε είναι προσωπικά δεδομένα. Συνεπώς, η μεθοδολογία αυτή μπορεί από μόνη της να αποτελέσει μία βασική διαδικασία για υπευθύνους επεξεργασίας προκειμένου να λάβουν κατάλληλες αποφάσεις ως προς την ορθή αντιμετώπιση κινδύνων ασφάλειας για τα προσωπικά δεδομένα που επεξεργάζονται.

Για την παρούσα διατριβή, η παρούσα προσέγγιση, όπως ήδη αναφέρθηκε νωρίτερα, θα αξιοποιηθεί στη συνέχεια στο πλαίσιο εκπόνησης μίας συνολικής εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων, έχοντας ήδη - μέσω αυτής – αποτιμήσει κατάλληλα ζητήματα ασφάλεια προσωπικών δεδομένων: το γεγονός ότι η μεθοδολογία του Enisa εστιάζει ακριβώς σε προσωπικά δεδομένα και δεν είναι γενική μέθοδος διαχείρισης οποιωνδήποτε κινδύνων ασφάλειας, την καθιστά μία σωστή επιλογή στο πλαίσιο αυτό.

Στο υπόλοιπο τμήμα του παρόντος κεφαλαίου ακολουθούνται συστηματικά τα βήματα της εν λόγω μεθοδολογίας.

4.1 Εκτίμηση κινδύνου με τη μεθοδολογίας του ENISA.

4.1.1 1ο Βήμα: Ορισμός της επεξεργασίας και του πλαισίου της

Στο πρώτο στάδιο θα ορίσουμε τα βασικά χαρακτηριστικά των προσωπικών δεδομένων και της επεξεργασίας τους, απαντώντας στις ακόλουθες ερωτήσεις:

4.1.1.1 Ποια είναι η λειτουργία επεξεργασίας δεδομένων προσωπικού χαρακτήρα;

Τα δεδομένα που επεξεργάζονται είναι οι χρόνοι εργασίας και τα προσωπικά δεδομένα που περιέχουν τα συμβόλαια των υπαλλήλων, ώστε να παραχθούν η καρτέλα μισθοδοσίας για το τμήμα προσωπικού και οι στατιστικοί υπολογισμοί παραγωγικότητας.

4.1.1.2 Ποιοι τύποι προσωπικών δεδομένων επεξεργάζονται;

Τα προσωπικά δεδομένα που προκύπτουν από το σύστημα ελέγχου πρόσβασης και καταγραφής εργασιακού χρόνου είναι οι ημέρες άδειας, οι ημέρες ασθένειας και οι ώρες εργασίας. Από τα συμβόλαια των εργαζομένων προκύπτουν προσωπικά δεδομένα και ευαίσθητα δεδομένα. Τα προσωπικά δεδομένα είναι τα ακόλουθα: Ονοματεπώνυμο, διεύθυνση κατοικίας, ηλεκτρονική διεύθυνση, αριθμός κινητού τηλεφώνου, ημερομηνία γέννησης, φωτογραφία, αριθμός τραπεζικού λογαριασμού, αριθμός ασφαλιστικού μητρώου, αριθμός φορολογικού μητρώου, φορολογική κλίμακα, λίστα προηγούμενων εργοδοτών και εκπαιδευτικό ιστορικό. Τα ευαίσθητα δεδομένα που περιλαμβάνονται στα ηλεκτρονικά συμβόλαια είναι τα εξής: εθνικότητα, τόπος γέννησης, θρησκεία και αναπηρική ταυτότητα.

4.1.1.3 Ποιος είναι ο σκοπός της επεξεργασίας;

Η επεξεργασία γίνεται με σκοπό την εκτέλεση πληρωμών του προσωπικού και την ανάλυση και αξιολόγηση των επιδόσεων του προσωπικού αλλά και της εταιρίας γενικότερα.

4.1.1.4 Ποια είναι τα μέσα που χρησιμοποιούνται για την επεξεργασία των προσωπικών δεδομένων;

Οι εφαρμογές, μέσω των οποίων θα επεξεργάζονται τα προσωπικά δεδομένα, είναι οι εφαρμογές Microsoft Teams και Excel online. Ουσιαστικά η Excel online λειτουργεί πάνω στην εφαρμογή Teams και επεξεργάζεται τα αρχεία που βρίσκονται αποθηκευμένα πάνω σε αυτή.

4.1.1.5 Πού λαμβάνει χώρα η επεξεργασία δεδομένων προσωπικού χαρακτήρα;

Η επεξεργασία και η αποθήκευση των αρχείων που γίνεται μέσω της Εφαρμογής Microsoft Teams λαμβάνει μέρος πάνω στη διαδικτυακή πλατφόρμα στο cloud της Microsoft. Η επεξεργασία των αρχείων μισθοδοσίας θα γίνεται στον τοπικό Server που υποστηρίζει το λογισμικό μισθοδοσίας.

4.1.1.6 Ποιες είναι οι κατηγορίες των υποκειμένων των δεδομένων;

Υποκείμενα των δεδομένων (Data Subjects) είναι όσοι υπάλληλοι έχουν συμβόλαιο με την εταιρεία.

4.1.1.7 Ποιοι είναι οι παραλήπτες των δεδομένων;

Οι αποδέκτες των επεξεργασμένων δεδομένων είναι το τμήμα προσωπικού, το τμήμα ελέγχου/οικονομικών και εξωτερικά στέλνονται οι καταστάσεις μισθοδοσίας σε εταιρία εκτύπωσης μισθοδοσίας. Ουσιαστικά, δεν υπάρχουν εξωτερικοί αποδέκτες – όλες οι ανωτέρω οντότητες υπάγονται στον υπεύθυνο επεξεργασίας.

4.1.2 2ο Βήμα: Κατανόηση και αξιολόγηση των επιπτώσεων

Αρχικά θα πρέπει να τεθούν σε σωστή και λογική βάση οι επιπτώσεις στις ζωές εργαζομένων μίας πιθανής απώλειας ασφάλειας των προσωπικών δεδομένων τους. Στη συγκεκριμένη περίπτωση το αποδεκτό επίπεδο επίπτωσης αποτιμάται σε υψηλό (High) όπως φαίνεται και στον πίνακα 1 με έντονα γράμματα. Η διαρροή προσωπικών δεδομένων, όπως εργασιακό συμβόλαιο που περιέχει συμφωνημένη αμοιβή, τραπεζικός λογαριασμός, οικογενειακή κατάσταση, θρήσκευμα, αξιολόγηση υπαλλήλου, μέρες ασθένειας κ.α. ενδέχεται να προξενήσει σημαντικές δυσκολίες σε υπαλλήλους της εταιρίας.

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	**Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).**
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Πίνακας 1. Περιγραφή επιπέδων των επιπτώσεων. Με έντονα γράμματα δηλώνεται το επίπεδο που επιλέχθηκε.

4.1.2.1 Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα

Σε αυτό το στάδιο θα εκτιμηθούν οι επιπτώσεις σε απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.

- **Εμπιστευτικότητα** : Σε περίπτωση απώλειας της εμπιστευτικότητας των προσωπικών δεδομένων οι επιπτώσεις θα είναι μέτριας κλίμακας (Medium) (πίνακας 2), δεδομένου του όγκου των δεδομένων και της περιοχής στην οποία δραστηριοποιείται η εταιρία.
- **Ακεραιότητα** : Πιθανή αλλοίωση των δεδομένων μπορεί να επηρεάσει αρνητικά των υπολογισμό των μισθών. Οι επιπτώσεις θα είναι υψηλής κλίμακας (High) (πίνακας 2), ιδίως σε χαμηλόμισθες ομάδες.
- **Διαθεσιμότητα** : Αν και είναι σημαντικό να διασφαλίζεται η διαθεσιμότητα, η φύση των πληροφοριών είναι τέτοια ώστε σε περίπτωση απώλειας της διαθεσιμότητας δεν θα υπάρξουν σημαντικές επιπτώσεις γιατί η επανασυλλογή τους είναι σχετικά ευχερής αλλά χρονοβόρα. Η επίπτωση αξιολογείται ως μέτρια. (Medium) (πίνακας 2).

NO	QUESTION	EVALUATION
I.1.	Please reflect on the impact that an unauthorized disclosure (loss of confidentiality) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐Low ☒**Medium** ☐High ☐Very high
I.2.	Please reflect on the impact that an unauthorized alteration (loss of integrity) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐Low ☐Medium ☒**High** ☐Very high
I.3.	Please reflect on the impact that an unauthorized destruction or loss (loss of availability) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐Low ☒**Medium** ☐High ☐Very high

Πίνακας 2. Ερωτήσεις για την αξιολόγηση των επιπτώσεων σε περίπτωση απώλειας της εμπιστευτικότητας, της ακεραιότητας και της προσβασιμότητας. Με έντονο χρώμα οι επιλογές της αξιολόγησης.

4.1.3 3ο Βήμα: Ορισμός πιθανών απειλών και αξιολόγηση της πιθανότητάς τους

A. NETWORK AND TECHNICAL RESOURCES

1. Εκτελείται κάποιο μέρος της επεξεργασίας προσωπικών δεδομένων μέσω του διαδικτύου;

Οι εφαρμογές, μέσω των οποίων θα επεξεργάζονται τα προσωπικά δεδομένα, είναι οι εφαρμογές Microsoft Teams και Excel online. Η εφαρμογή Microsoft Teams λειτουργεί μόνο μέσω διαδικτυακής σύνδεσης στο cloud της Microsoft.

2. Είναι δυνατή η πρόσβαση σε ένα εσωτερικό σύστημα επεξεργασίας προσωπικών δεδομένων μέσω του διαδικτύου (π.χ. για ορισμένους χρήστες ή ομάδες χρηστών);

Οι εφαρμογές που διαχειρίζονται τα αρχεία προσωπικών δεδομένων είναι διαδικτυακού τύπου, όπως αναφέρθηκε και στο πρώτο ερώτημα. Συνεπώς οι χρήστες έχουν πρόσβαση σε αυτά μόνο μέσω Internet. Ο Server, στον οποίο είναι εγκατεστημένο το λογισμικό μισθοδοσίας, είναι προσβάσιμος μόνο τοπικά.

3. Είναι το σύστημα επεξεργασίας προσωπικών δεδομένων διασυνδεδεμένο με άλλο εξωτερικό ή εσωτερικό (στο οργανισμό σας) σύστημα ή υπηρεσία πληροφορικής;

Οι εφαρμογές MS Teams, OneDrive ανήκουν στην ευρύτερη διαδικτυακή πλατφόρμα της εταιρίας, η οποία είναι εγκατεστημένη στο cloud της Microsoft. Η πλατφόρμα αυτή είναι συνδεδεμένη με τα τοπικά υπολογιστικά δίκτυα των διαφορετικών εταιριών του ομίλου. Μέσω αυτού του δικτύου μπορούν οι υπάλληλοι των εταιριών να έχουν πρόσβαση στη διαδικτυακή πλατφόρμα.

4. Μπορούν τα μη εξουσιοδοτημένα άτομα να έχουν εύκολη πρόσβαση στο περιβάλλον επεξεργασίας δεδομένων;

Μέχρι τώρα δεν έχει παρατηρηθεί κάποια παραβίαση πρόσβασης της πλατφόρμας. Αρχικά εφαρμόζεται μία αυστηρή κοινή πολιτική κωδικών πρόσβασης στα τοπικά δίκτυα των εταιριών. Συμπληρωματικά έχει ενεργοποιηθεί και αυθεντικοποίηση δύο παραγόντων (2 factor authentication) που προσφέρεται από την Microsoft όπου αποστέλλεται δεύτερος κωδικός σε εφαρμογή κινητού που πιστοποιεί την ταυτότητα του χρήστη.

5. Το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα σχεδιάζεται, υλοποιείται ή συντηρείται χωρίς να ακολουθούνται οι σχετικές βέλτιστες πρακτικές;

Η κατασκευή αυτού του δικτύου ακολουθεί τις καλύτερες και τις πιο ασφαλείς πρακτικές της Microsoft. Όπως αναφέρθηκε στο 4ο ερώτημα, ακολουθείται μια αρκετά ισχυρή πολιτική κωδικών πρόσβασης με βάση τις καλύτερες πρακτικές της Microsoft. Επιπλέον εφαρμόζεται εσωτερικός κανονισμός για τη μυστικότητα των κωδικών που ισχύει για όλους τους εργαζομένους. Τέλος εφαρμόζεται ένα αυστηρό σύστημα εξουσιοδότησης και στους τοπικούς file Servers και στη διαδικτυακή πλατφόρμα.

B. PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA

1. Είναι οι ρόλοι και οι ευθύνες όσον αφορά την επεξεργασία των προσωπικών δεδομένων ασαφείς ή δεν ορίζονται σαφώς;

Η εξουσιοδότηση και οι ρόλοι των χρηστών που διαχειρίζονται αρχεία προσωπικών δεδομένων είναι καθορισμένη από εγκεκριμένες διαδικασίες επιχειρησιακών λειτουργιών της διοίκησης του ομίλου. Η διαχείριση και λειτουργία των εφαρμογών που επεξεργάζονται προσωπικά δεδομένα είναι συμβατή με τον νέο Γενικό Κανονισμό Προστασίας Δεδομένων.

2. Είναι η αποδεκτή χρήση του δικτύου, του συστήματος και των φυσικών πόρων εντός του οργανισμού διφορούμενη ή όχι σαφώς καθορισμένη;

Υπάρχει εσωτερικός κανονισμός χρήσεως των δικτυακών μηχανημάτων (ηλεκτρονικοί υπολογιστές, δικτυακοί εκτυπωτές κ.α.). Οι υπάλληλοι μετά την πρόσληψή τους και εντός της πρώτης εβδομάδος υποχρεούνται να διαβάσουν και να υπογράψουν την κατανόηση των κανόνων. Σε περίπτωση ερωτήσεων απευθύνονται στο Helpdesk. Οι κανόνες για τη χρήση που πρέπει να ακολουθεί ένας τελικός χρήστης είναι ενημερωμένοι και σύμφωνοι με τις καλύτερες πρακτικές ασφάλειας.

3. Είναι οι υπάλληλοι που επιτρέπεται να φέρουν και να χρησιμοποιούν τις δικές τους συσκευές για να συνδεθούν με το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα;

Στα τοπικά δίκτυα συνδέονται μόνο υπολογιστές που αποκτούνται, εγκαθίστανται και ελέγχονται από τα τμήματα πληροφορικής της κάθε εταιρίας. Κανένας υπάλληλος δεν μπορεί να συνδέσει δική του συσκευή στο τοπικό δίκτυο. Ωστόσο η διαδικτυακή πλατφόρμα της Microsoft (με την τρέχουσα ρύθμιση) δίνει τη δυνατότητα στους εγγεγραμμένους χρήστες της να έχουν πρόσβαση μέσω συσκευών που δεν είναι ενσωματωμένες στον τοπικό domain controller. Αυτό συνεπάγεται, ότι οι χρήστες που έχουν πρόσβαση στις εφαρμογές που επεξεργάζονται προσωπικά δεδομένα, θα μπορούν να έχουν πρόσβαση από οποιαδήποτε συσκευή θέλουν.

4. Επιτρέπεται στους υπαλλήλους να μεταφέρουν, να αποθηκεύουν ή να επεξεργάζονται με άλλο τρόπο προσωπικά δεδομένα εκτός των εγκαταστάσεων του οργανισμού;

Στα εταιρικά συμβόλαια των υπαλλήλων υπάρχει παράγραφος, η οποία ορίζει την απαγόρευση της εξαγωγής αρχείων από την εταιρία. Υπάρχει επίσης και εσωτερικός κανονισμός από τα τμήματα πληροφορικής, ο οποίος επεξηγεί, ότι απαγορεύεται κάθε μορφή μεταφοράς εταιρικών δεδομένων που δεν προβλέπεται από εταιρικές διαδικασίες. Από τεχνικής άποψης υπάρχει πολιτική ασφάλειας που απενεργοποιεί τις usb-συνδέσεις και εφαρμόζεται μόνο σε κάποιους από τους υπολογιστές που βρίσκονται στην παραγωγή. Στην πραγματικότητα όμως ένας υπάλληλος, ο οποίος έχει πρόσβαση σε αρχεία προσωπικών δεδομένων, μπορεί να συνδέσει μία συσκευή αποθήκευσης χωρίς πρόβλημα και να μεταφέρει τα αρχεία εκτός εταιρικού περιβάλλοντος.

5. Μπορούν να διεξαχθούν δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα χωρίς να δημιουργηθούν αρχεία καταγραφής;

Η διαχειριστική πύλη της εταιρικής πλατφόρμας στο cloud της Microsoft καταγράφει σε log files όλες τις ενέργειες των χρηστών που επεξεργάζονται αρχεία εταιρικών και προσωπικών δεδομένων.

C. PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA

1. Εκτελείται η επεξεργασία προσωπικών δεδομένων από μη καθορισμένο αριθμό εργαζομένων;

Οι ρόλοι, το επίπεδο πρόσβασης και τα μέλη της ομάδας που διαχειρίζονται τις εφαρμογές που φέρουν προσωπικά δεδομένα είναι λεπτομερώς καθορισμένα από τη διοίκηση και το τμήμα πληροφορικής και ελέγχονται συνεχώς.

2. Συμπεριλαμβάνεται οποιοδήποτε μέρος της διαδικασίας επεξεργασίας δεδομένων από έναν ανάδοχο / τρίτο (επεξεργαστή δεδομένων)

Τα προσωπικά δεδομένα επεξεργάζονται μόνο εσωτερικά και βέβαια τηρούνται στο cloud της Microsoft όπως έχει προαναφερθεί. Καμία τρίτη εταιρία δεν έχει πρόσβαση ούτε σε προσωπικά δεδομένα, ούτε στα αποτελέσματα της επεξεργασίας τους.

3. Είναι οι υποχρεώσεις των ομάδων / ατόμων που εμπλέκονται στην επεξεργασία προσωπικών δεδομένων διφορούμενες ή δεν αναφέρονται σαφώς;

Οι ρόλοι, η εξουσιοδότηση και η ευθύνη της ομάδας που έχει πρόσβαση στην επεξεργασία προσωπικών δεδομένων έχει αναλυθεί στα μέλη της λεπτομερώς. Τα μέλη της, μετά από σειρά εκπαίδευσης και σεμιναρίων, έχουν υπογράψει σχετικό έγγραφο ότι κατανοούν τη μεθοδολογία της επεξεργασίας των προσωπικών δεδομένων και τα θέματα ασφάλειας που προκύπτουν από λανθασμένους χειρισμούς.

4. Συμμετέχει προσωπικό στην επεξεργασία προσωπικών δεδομένων που δεν είναι εξοικειωμένο με θέματα ασφάλειας των πληροφοριών;

Τα μέλη της ομάδας που επεξεργάζονται αρχεία προσωπικών δεδομένων λαμβάνουν μέρος τέσσερις (4) φορές το χρόνο σε εκπαιδευτικά σεμινάρια του τμήματος πληροφορικής πάνω σε θέματα ασφάλειας και σε θέματα χειρισμού των νέων λειτουργιών των εφαρμογών που χρησιμοποιούν.

5. Έχει παρατηρηθεί ποτέ παράληψη ασφαλούς αποθήκευσης ή / και διαγραφή προσωπικών δεδομένων από τις ομάδες / άτομα που εμπλέκονται στην διαδικασία επεξεργασίας προσωπικών δεδομένων;

Έχουν παρατηρηθεί δύο (2) φαινόμενα λανθασμένων χειρισμών πάνω σε αρχεία προσωπικών δεδομένων. Το πρώτο ήταν ένα email με προσωπικά δεδομένα υπαλλήλων που στάλθηκε σε λάθος παραλήπτες. Το δεύτερο ήταν σβήσιμο αρχείων με προσωπικά δεδομένα, το οποίο ωστόσο αποκαταστάθηκε με τη βοήθεια του backup συστήματος του file Server.

D. BUSINESS SECTOR AND SCALE OF PROCESSING

1. Θεωρείτε ότι ο επιχειρησιακός τομέας της εταιρίας είναι επιρρεπής σε κυβερνοεπιθέσεις;

Το διοικητικό συμβούλιο σε συνεργασία με τα τμήματα πληροφορικής δεν θεωρεί τον όμιλο εταιριών ως πιθανό στόχο κάποιας κυβερνοεπίθεσης. Ο ευρύτερος κλάδος των μικρομεσαίων βιομηχανιών δεν αποτελεί συνήθη στόχο.

2. Έχει υποστεί ο οργανισμός σας οποιαδήποτε κυβερνοεπίθεση ή άλλου είδους παραβίαση ασφαλείας τα τελευταία δύο χρόνια;

Στην πραγματικότητα δεν παρουσιάζονται προηγμένες κυβερνοεπιθέσεις. Η συχνότερη είναι τα συστηματικά fishing emails και CEO-email frauds. Η συγκεκριμένη επίθεση αποτρέπεται από το εγκατεστημένο σύστημα email security που ελέγχει τα εισερχόμενα και εξερχόμενα emails. Σπανιότερα παρατηρούνται port-scanning τα οποία αντιμετωπίζονται από τα firewalls με domain blocking αλλά και email flooding που αντιμετωπίζονται από το σωστά ρυθμισμένο exchange online Server.

3. Έχετε λάβει ειδοποιήσεις ή / και καταγγελίες σχετικά με την ασφάλεια του συστήματος πληροφορικής (που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων) κατά το τελευταίο έτος;

Μέχρι τώρα δεν έχει παρουσιαστεί κάποιο θέμα ασφάλειας πάνω στη διαδικτυακή πλατφόρμα. Συχνά όμως παρατηρείται από εργαζομένους που έχουν πρόσβαση στα αρχεία προσωπικών δεδομένων να σημειώνουν τον κωδικό σε χαρτί και να το τοποθετούν σε εμφανές μέρος πάνω στο γραφείο τους, το οποίο απαγορεύεται από τον εσωτερικό κανονισμό ασφάλειας που ισχύει για όλους.

4. Αφορά η διαδικασία επεξεργασίας μεγάλο αριθμό ατόμων ή / και προσωπικών δεδομένων;

Τα αρχεία φέρουν προσωπικά δεδομένα 1000 περίπου εργαζομένων από 3 διαφορετικές εταιρίες και το μέγεθός τους είναι περίπου 100 GB.

5. Υπάρχουν τυχόν βέλτιστες πρακτικές ασφαλείας του επιχειρησιακού τομέα που δεν έχουν εφαρμοστεί επαρκώς;

Τα τμήματα πληροφορικής εφαρμόζουν κοινές πολιτικές ασφάλειας, ώστε σε περίπτωση κινδύνου να πρέπει να εξεταστεί μόνο ένα ενιαίο πλαίσιο ασφάλειας και όχι 3 διαφορετικά. Εντούτοις τα τοπικά δίκτυα παρουσιάζουν διαφορές. Σε 2 από τα 3 τοπικά δίκτυα υπάρχουν ακόμα Servers που λειτουργούν σε Windows 2008 R2, οι οποίοι ολοκληρώνουν τον κύκλο ζωής τους στις 14/1/2020. Οι Servers αυτοί έπρεπε να είχαν ήδη αναβαθμιστεί. Το συγκεκριμένο πρόβλημα δεν επηρεάζει καθόλου τη λειτουργία της διαδικτυακής πλατφόρμας της Microsoft που εξετάζεται.

Αξιολόγηση τομέων

Το επόμενο στάδιο είναι η οριοθέτηση της πιθανότητας εμφάνισης κινδύνου στους τέσσερις (4) αντίστοιχους τομείς αξιολόγησης.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	☐Low	1
	☐Medium	2
	☒High	**3**
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	☐Low	1
	☐Medium	2
	☒High	**3**
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	☐Low	1
	☒Medium	**2**
	☐High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	**☒Low**	**1**
	☐Medium	2
	☐High	3

Πίνακας 3. Αξιολόγηση κινδύνου ανά περιοχή ελέγχου. Με έντονα γράμματα οι επιλογές της αξιολόγησης.

A. Network and Technical Resources

Η πιθανότητα εμφάνισης κινδύνου είναι υψηλή (High) (πίνακας 3), επειδή η επεξεργασία των προσωπικών δεδομένων θα γίνεται εξ' ολοκλήρου μέσω του διαδικτύου, στη διαδικτυακή πλατφόρμα στο cloud της Microsoft. Αυτό συνεπάγεται ότι η πιθανότητα μιας online επίθεσης είναι πολύ μεγαλύτερη σε σύγκριση με την προηγούμενη τεχνολογία. Δεδομένου ότι η πρόσβαση σε αυτήν την πλατφόρμα εξαρτάται μόνο από την ύπαρξη διαδικτυακής σύνδεσης, το σύστημα είναι εξαρτημένο από το διαδικτυακό πάροχο και η πιθανότητα της απώλειας της διαθεσιμότητας είναι υψηλή.

B. Processes/Procedures Related to the Processing of Personal Data

Η πιθανότητα εμφάνισης κινδύνου είναι και σε αυτόν τον τομέα υψηλή (High) (πίνακας 3). Ο κύριος λόγος είναι η δυνατότητα πρόσβασης στην πλατφόρμα μέσω συσκευών, οι οποίες δεν ανήκουν στον domain controller του τοπικού δικτύου. Οι χρηστές δηλαδή μπορούν να έχουν πρόσβαση από υπολογιστές που δεν ακολουθούν τις πολιτικές ασφάλειας του τοπικού δικτύου. Το γεγονός αυτό θέτει σε κίνδυνο τους κωδικούς των χρηστών που συνδέονται μέσω αυτών. Η πιθανότητα μη εξουσιοδοτημένης πρόσβασης είναι υψηλή.

C. Parties/People involved in the Processing of Personal Data

Στο συγκεκριμένο τομέα αξιολόγησης, οι ρόλοι και η εξουσιοδότηση των υπαλλήλων που θα επεξεργάζονται προσωπικά δεδομένα είναι σωστά προκαθορισμένοι. Η ύπαρξη περιπτώσεων της παραβίασης του εσωτερικού κανονισμού της προστασίας των κωδικών από υπάλληλο με υψηλή εξουσιοδότηση ορίζει την πιθανότητα κινδύνου ως μέση (Medium) (πίνακας 3).

D. Business Sector and Scale of Processing

Δεδομένου του χαμηλού εταιρικού ιστορικού κυβερνοεπιθέσεων αλλά και γενικότερα του επιχειρηματικού τομέα στον οποίο ανήκει, σε συνδυασμό με την μέτρια - ως προς το μέγεθος - επεξεργασία δεδομένων, η πιθανότητα κινδύνου είναι χαμηλή (Low) (πίνακας 3).

4.1.4 4ο Βήμα: Αξιολόγηση του κινδύνου

Η συνολική βαθμολογία από τον πίνακα 3 είναι 9 και χαρακτηρίζεται από τον πίνακα 4 ως υψηλή (High).

OVERALL SUM OF THREAT OCCURRENCE PROBABILITY	THREAT OCCURRENCE PROBABILITY LEVEL
4 - 5	Low
6 - 8	Medium
9 -12	**High**

Πίνακας 4. Επίπεδα εμφάνισης απειλής. Με έντονα γράμματα το επίπεδο της εμφάνισης στη συγκεκριμένη περίπτωση.

Η πιθανότητα εμφάνισης κινδύνου (9-High) σε συνδυασμό με το υψηλό επίπεδο επιπτώσεων (High) από τον πίνακα 1, αποδεικνύουν ότι η συγκεκριμένη επεξεργασία προσωπικών δεδομένων πάνω στο παρόν πλαίσιο που εκτελείται έχει κενά ασφάλειας που μπορεί να θέσουν τα δεδομένα σε κίνδυνο και ανήκει στην κόκκινη περιοχή του πίνακα 5.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low			
	Medium			
	High			**X**

Πίνακας 5. Τελική αξιολόγηση του κινδύνου. Με έντονο **X** η επίπτωση σε συνάρτηση με την πιθανότητα εμφάνισης του κινδύνου.

4.1.5 5ο Βήμα: Μέτρα ασφάλειας

Τα κυριότερα μέτρα ασφάλειας που προτείνονται αφορούν τις 2 περιοχές με την υψηλότερη επικινδυνότητα, Network and Technical Resources και Processes/Procedures Related to the Processing of Personal Data.

Για τον τομέα αξιολόγησης Network and Technical Resources και Processes προτείνονται τα ακόλουθα μέτρα:

- Η εταιρία θα πρέπει να διαθέτει τουλάχιστον 2 συνδέσεις Internet από διαφορετικούς παρόχους. Λόγω του ότι η επεξεργασία και η αποθήκευση θα γίνεται αποκλειστικά online - και για να ελαχιστοποιηθεί η πιθανότητα απώλειας της διαθεσιμότητάς - προτείνονται 3 συνδέσεις.
- Κρυπτογραφημένες συνδέσεις για τους χρήστες που ανήκουν στην ομάδα επεξεργασίας των προσωπικών δεδομένων.

Για τον τομέα αξιολόγησης Processes/Procedures Related to the Processing of Personal Data προτείνονται τα ακόλουθα μέτρα:

- Θα πρέπει να εφαρμοστεί μία πολιτική ασφάλειας, η οποία να εμποδίζει την πρόσβαση στις εφαρμογές, όταν η σύνδεση του χρήστη γίνεται από συσκευή που δεν είναι ενσωματωμένη στην local domain.

4.2 Εκτίμηση αντικτύπου

4.2.1 Γενικό Πλαίσιο

Στην παρούσα ενότητα θα πραγματοποιηθούν τα βήματα μίας εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων: ουσιαστικά, τα ζητήματα ασφάλειας έχουν ήδη αντιμετωπιστεί παραπάνω με τη μέθοδο διαχείρισης κινδύνων που εκπονήσαμε. Παραμένουν όμως ουσιαστικά ερωτήματα που πρέπει να διερευνηθούν, τα οποία άπτονται ιδίως της ιδιωτικότητας. Για παράδειγμα πρέπει να διερευνηθεί η νομική βάση της επεξεργασίας, εάν ικανοποιούνται τα δικαιώματα των υποκειμένων των δεδομένων, αν τυχόν συλλέγονται περισσότερα δεδομένα από ό,τι χρειάζεται εν όψει των σκοπών επεξεργασίας κ.ο.κ.

Τα βήματα που ακολουθούν είναι στο πλαίσιο της εκτίμησης αντικτύπου, αξιοποιώντας τη σχετική υλοποίηση σε ελεύθερα διαθέσιμο εργαλείο λογισμικού της γαλλικής Αρχής Προστασίας Δεδομένων CNIL, όπως αναφέρθηκε και νωρίτερα. Για κάθε στάδιο του ελέγχου υπάρχει και το αντίστοιχο στιγμιότυπο στο παράρτημα Α.

4.2.1.1 **Επισκόπηση** (Παράρτημα Α, Στιγμιότυπο 1. Επισκόπηση)

Ποια είναι η υπό εξέταση επεξεργασία;

Στην συγκεκριμένη περίπτωση η επεξεργασία προσωπικών δεδομένων που εκτελείται, δημιουργεί κατάλληλα αρχεία που χρησιμοποιούνται για την διεκπεραίωση της μισθοδοσίας και για την παραγωγή στατιστικών αξιολογήσεων της παραγωγικότητας και της οικονομικής κατάστασης της εταιρίας.

Ποιες είναι οι ευθύνες που συνδέονται με την επεξεργασία;

Ο "υπεύθυνος επεξεργασίας" είναι η εταιρεία, η οποία – διά του διοικητικού της συμβουλίου – λαμβάνει τις αποφάσεις επί της εν λόγω επεξεργασίας προσωπικών δεδομένων. Ο εκτελών την επεξεργασία είναι ένας εξουσιοδοτημένος συνεργάτης της Microsoft.

Όσον αφορά την κατανομή κρίσιμων για την επεξεργασία αρμοδιοτήτων εντός της εταιρείας, αρμόδιοι για τη μισθοδοσία είναι 4 υπάλληλοι του τμήματος προσωπικού και για την παραγωγή στατιστικών αξιολογήσεων είναι 3 υπάλληλοι του οικονομικού τμήματος.

Υπάρχουν πρότυπα που ισχύουν για την επεξεργασία;

Στην συγκεκριμένη επεξεργασία δεδομένων δεν εφαρμόζεται συγκεκριμένο πρότυπο επεξεργασίας ούτε υπάρχει κάποια πιστοποίηση προστασίας δεδομένων. Όσον αφορά τον κώδικα δεοντολογίας, είναι προαιρετικός και δεν ακολουθείται κάποιος – εξάλλου δεν έχει ακόμα υιοθετηθεί, από αρμόδια ένωση, κάποιος κώδικας δεοντολογίας σύμφωνα με το άρθρο 40 του ΓΚΠΔ, στο οποίο θα μπορούσε να είχε προσχωρήσει η εταιρεία.

4.2.1.2 Δεδομένα, Διαδικασίες και υποστηρικτικά στοιχεία (Παράρτημα Α, Στιγμιότυπο 2. Δεδομένα, Διαδικασίες και υποστηρικτικά στοιχεία)

Ποια προσωπικά δεδομένα υφίστανται επεξεργασία;

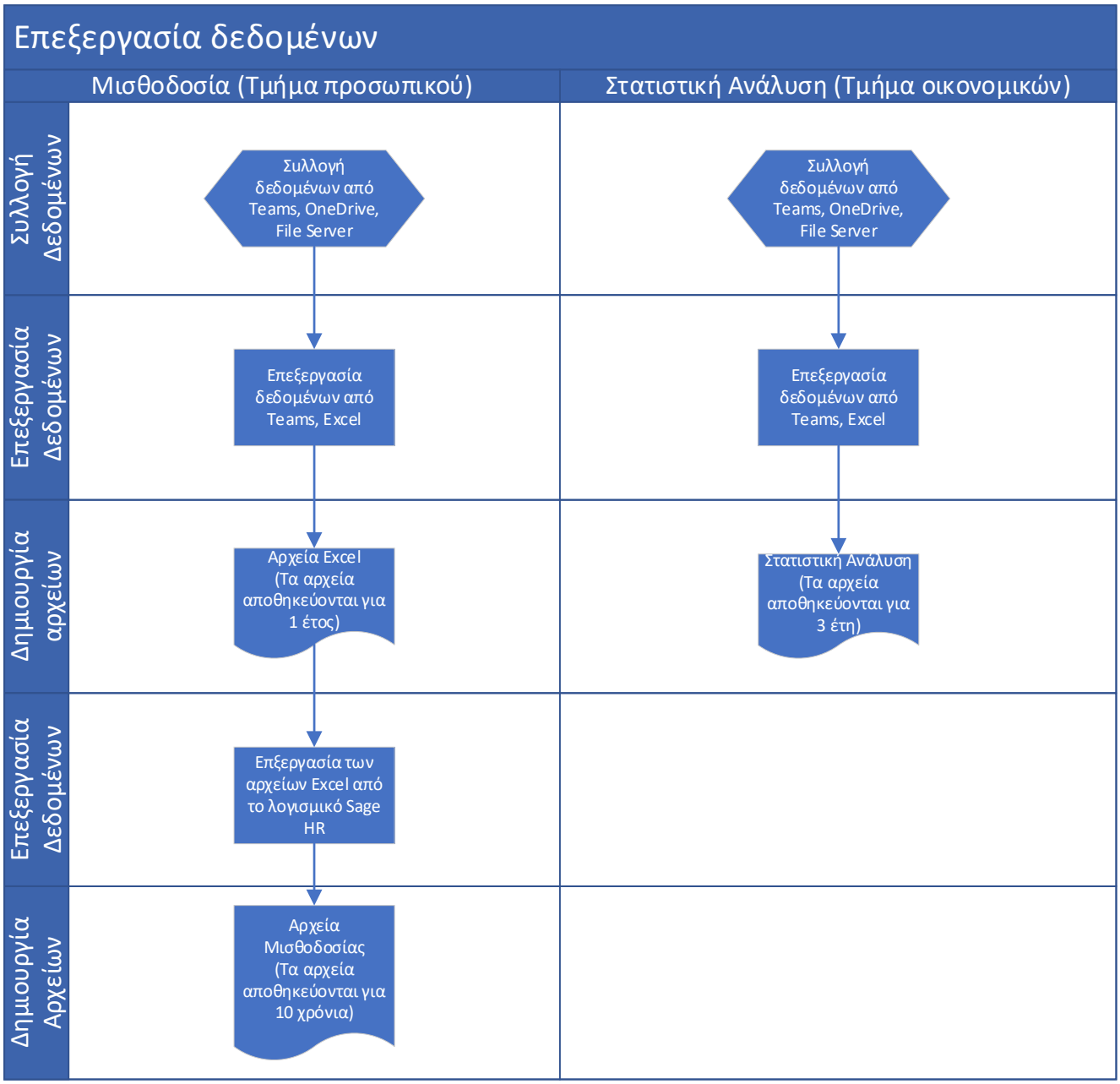
Για την μισθοδοσία θα επεξεργαστούν τα ακόλουθα προσωπικά και ευαίσθητα προσωπικά δεδομένα.

Προσωπικά δεδομένα: Ονοματεπώνυμο, διεύθυνση κατοικίας, ημερομηνία γέννησης, αριθμός τραπεζικού λογαριασμού, αριθμός ασφαλιστικού μητρώου, αριθμός φορολογικού μητρώου, φορολογική κλίμακα, ημέρες εργασίας, είδος βάρδιας.

Ευαίσθητα προσωπικά δεδομένα: θρησκεία, αναπηρική ταυτότητα, ημέρες ασθένειας του τρέχοντος μηνός, μέλος συνδικαλιστικού σωματείου.

Για τις στατιστικές αξιολόγησης θα επεξεργαστούν τα ακόλουθα προσωπικά δεδομένα: μισθός σε ευρώ, ημέρες εργασίας, ημέρες ασθένειας, χρόνος διαλείμματος, είδος βάρδιας.

Πώς λειτουργεί ο κύκλος ζωής των δεδομένων και των διαδικασιών;



Διάγραμμα Ροής 1. Περιγραφή της ροής της διαδικασίας της μισθοδοσίας και της στατιστικής ανάλυσης.

Ποια είναι τα στοιχεία που υποστηρίζουν τα δεδομένα;

Για την επεξεργασία των δεδομένων σε ηλεκτρονική μορφή χρησιμοποιούνται τα λογισμικά Microsoft Teams, Excel Online 365, Sage HR. Για την αποθήκευση χρησιμοποιούνται τα λογισμικά Microsoft Teams, OneDrive, virtual file Server Microsoft 2012r2, virtual SQL Server 2016. Τα συμβόλαια σε έντυπη μορφή αποθηκεύονται σε δωμάτιο του τμήματος προσωπικού, περιορισμένης πρόσβασης.

4.2.2 Θεμελιώδεις Αρχές νομιμότητας

4.2.2.1 Αναλογικότητα και Αναγκαιότητα (Παράρτημα Α, Στιγμιότυπο 3. Αναλογικότητα και αναγκαιότητα)

Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;

Η επεξεργασία με σκοπό την μισθοδοσία αποτελεί νομική υποχρέωση της εταιρίας και είναι η πλέον συνηθισμένη διαδικασία σε ένα εταιρικό περιβάλλον. Η στατιστικής φύσεως επεξεργασία, η οποία είναι μία εταιρική ανάγκη για τον υπολογισμό της παραγωγικότητας, θεωρείται απαραίτητη για τον σκοπό και τα έννομα συμφέροντα της εταιρίας. Η νομιμότητα των σκοπών είναι δεδομένη και στις δύο περιπτώσεις.

Ποια είναι η νομική βάση που καθιστά την επεξεργασία νόμιμη;

Η πρώτη επεξεργασία της μισθοδοσίας είναι αναγκαία λόγω της νομικής υποχρέωσης της εταιρίας απέναντι στους υπαλλήλους της. Συνεπώς, η νομική βάση έγκειται στο άρ. 6 παρ. 1 στοιχ. γ' του ΓΚΠΔ (δηλαδή «η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας»).

Οι στατιστικές αναλύσεις αποτελούν κομμάτια των εταιρικών ισολογισμών που και αυτοί αποτελούν νομικές υποχρεώσεις της εταιρίας και είναι απαραίτητοι για τη λειτουργία της. Η νομική βάση για τις εν λόγω αναλύσεις – αφού δεν προβλέπονται ρητά αυτές σε νόμο - έγκειται στο άρ. παρ. 1 στοιχ. στ' του ΓΚΠΔ (δηλαδή «η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας (…), 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 (…)»

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 («ελαχιστοποίηση των δεδομένων»);

Για τη διαδικασία της μισθοδοσίας, τα προσωπικά δεδομένα που συλλέγονται και επεξεργάζονται είναι τα αναγκαία για τον σωστό υπολογισμό του μισθού και προβλέπονται από νόμο του γερμανικού κράτους. Το περιεχόμενο των στατιστικών αναλύσεων ορίζεται από τον γενικό διευθυντή των οικονομικών. Τα συγκεκριμένα δεδομένα του ερωτήματος 1.2.1 συλλέγονται αυτά και μόνον αυτά και στη συνέχεια επεξεργάζονται. Θα ήταν σωστό να γινόταν έλεγχος στα μεγέθη που αναλύονται

στατιστικά, για να ελεγχθεί αν όντως υπάρχει ανάγκη συλλογής των συγκεκριμένων στοιχείων για την εξαγωγή αξιόπιστων αποτελεσμάτων.

Τα δεδομένα είναι ακριβή και ενημερωμένα;

Το τμήμα του προσωπικού δεν μπορεί να αλλάξει τα προσωπικά δεδομένα που επεξεργάζονται για την μισθοδοσία. Η ακρίβεια και η ενημέρωση είναι καθήκον του υπάλληλου σε τυχόν αλλαγές των δεδομένων του. Ωστόσο, παρέχεται σαφής ενημέρωση στους υπαλλήλους σχετικά με τις υποχρεώσεις τους για την παροχή στοιχείων που να είναι ακριβή.

Στις στατιστικές αναλύσεις πολλά δεδομένα προέρχονται από το σύστημα ελέγχου πρόσβασης και καταγραφής εργασιακού χρόνου, τα στοιχεία του οποίου είναι ακριβή.

Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;

Οι καταστάσεις μισθοδοσίας αποθηκεύονται για 10 χρόνια βάσει γερμανικού νόμου, τα αρχεία excel που αποτελούν τα δεδομένα του λογισμικού μισθοδοσίας αποθηκεύονται για 1 χρόνο και τα οι στατιστικές αναλύσεις για 3 χρόνια. Δεν υπάρχει κάποιο ενιαίο σχέδιο διαχείρισης της αποθήκευσης των δεδομένων.

4.2.2.2 Μέτρα για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων (Παράρτημα Α, Στιγμιότυπο 4. Μέτρα για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων)

Πώς ενημερώνονται τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία;

Στην επεξεργασία της μισθοδοσίας τα υποκείμενα λαμβάνουν κάθε μήνα σε έντυπη μορφή την μισθοδοσία τους. Στην επεξεργασία των στατιστικών αξιολογήσεων δεν προβλέπεται ενημέρωση των υποκειμένων. Τα υποκείμενα θα πρέπει να ενημερωθούν για την συγκεκριμένη διαδικασία.

Εάν ισχύει, πώς επιτυγχάνεται η συγκατάθεση των υποκειμένων των δεδομένων;

Δεν προβλέπεται καμία μορφή συγκατάθεσης των υποκειμένων των δεδομένων στις συγκεκριμένες επεξεργασίες. Όπως προαναφέρθηκε, οι νομική βάση της πρώτης επεξεργασίας είναι έννομη υποχρέωση και η δεύτερη είναι απαραίτητη για τους σκοπούς έννομων συμφερόντων της εταιρίας.

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους πρόσβασης και φορητότητας προσωπικών δεδομένων;

Οι εργαζόμενοι μπορούν να ενημερωθούν από τον υπεύθυνο προστασίας δεδομένων και να θέσουν τις ερωτήσεις τους σε προκαθορισμένες μέρες και ώρες κάθε εβδομάδα. Το τμήμα προσωπικού έχει οριστεί από τον υπεύθυνο της επεξεργασίας ως ο αρμόδιος για την επεξεργασία των αιτημάτων σχετικά με τα προσωπικά δεδομένα. Το τμήμα αυτό προσφέρει καθημερινά 2 ώρες για την εξυπηρέτηση αιτημάτων των υπαλλήλων, ώστε όλοι οι εργαζόμενοι να είναι σε θέση να ασκήσουν τα δικαιώματά τους, συμπεριλαμβανομένων και όσων προκύπτουν από τον ΓΚΠΔ. Δεν έχει γνωστοποιηθεί ότι το τμήμα προσωπικού οφείλει να απαντήσει σε κάθε αίτημα εντός 30 ημερών από την ημέρα υποβολής του.

Η φορητότητα προσωπικών δεδομένων στην συγκεκριμένη περίπτωση δεν έχει εφαρμογή (αφού η νομική βάση της επεξεργασίας δεν είναι ούτε το άρ. 6 παρ. 1 στοιχ. α' ούτε το άρ. 6 παρ. 1 στοιχ. β' του ΓΚΠΔ (βλ. άρθρο 20 αυτού σχετικά για το δικαίωμα φορητότητας).

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους διόρθωσης και διαγραφής;

Τα προσωπικά δεδομένα που σχετίζονται με την μισθοδοσία πρέπει βάσει γερμανικού νόμου να φυλάσσονται για 10 χρόνια. Δυνατή είναι η διαγραφή των προσωπικών δεδομένων του συστήματος ελέγχου πρόσβασης και καταγραφής εργασιακού χρόνου μετά από συνεννόηση με το τμήμα προσωπικού.

Η διόρθωση προσωπικών δεδομένων γίνεται μέσω του τμήματος προσωπικού σε προκαθορισμένες ώρες και μέρες. Δεν έχει γνωστοποιηθεί ότι το τμήμα προσωπικού οφείλει να απαντήσει σε κάθε αίτημα εντός 30 ημερών από την ημέρα υποβολής του.

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους περιορισμού και εναντίωσης;

Όμοια με τον προηγούμενο ερώτημα το τμήμα προσωπικού είναι προσβάσιμο καθημερινά για την άσκηση των δικαιωμάτων των υποκειμένων. Δεν έχει γνωστοποιηθεί ότι το τμήμα προσωπικού οφείλει να απαντήσει σε κάθε αίτημα εντός 30 ημερών από την ημέρα υποβολής του.

Οι υποχρεώσεις των εκτελούντων την επεξεργασία προσδιορίζονται σαφώς και διέπονται από σύμβαση;

Υπάρχει σύμβαση με εξουσιοδοτημένο συνεργάτη της Microsoft.

Σε περίπτωση μεταφοράς δεδομένων εκτός της Ευρωπαϊκής Ένωσης, τα προσωπικά δεδομένα προστατεύονται επαρκώς;

Δεν προβλέπεται καμία μεταφορά προσωπικών δεδομένων.

4.2.3 Κίνδυνοι

4.2.3.1 Προγραμματισμένα ή υπάρχοντα μέτρα (Παράρτημα Α, Στιγμιότυπο 5. Προγραμματισμένα ή υπάρχοντα μέτρα)

Ελαχιστοποίηση του αριθμού των δεδομένων προσωπικού χαρακτήρα

Τα δεδομένα που συλλέγονται για σκοπούς μισθοδοσίας είναι απολύτως απαραίτητα βάσει νομικών υποχρεώσεων – συνεπώς δεν τίθεται ζήτημα περαιτέρω ελαχιστοποίησης των δεδομένων. Αναφορικά με την επεξεργασία για στατιστικούς σκοπούς, θα πρέπει να ελεγχθεί αν η συλλογή των προσωπικών δεδομένων του ερωτήματος 1.2.1 είναι αναγκαία για την επεξεργασία.

Μέτρο λογικής πρόσβασης

Η πολιτική ασφάλειας των κωδικών αποτελείται από 2 σκέλη, του τοπικού δικτύου και του cloud.

Στο τοπικό δίκτυο η πολιτική ασφάλειας των κωδικών πρέπει να πληροί τους κάτωθι όρους:

- Ο κωδικός αποτελείται από τουλάχιστον 10 χαρακτήρες και πρέπει να περιέχει το λιγότερο έναν αριθμό, ένα κεφαλαίο γράμμα και ένα ειδικό σύμβολο
- Η ανανέωση του κωδικού γίνεται κάθε 2 μήνες
- Ο Κωδικός απαγορεύεται να περιέχει τους 2 προηγούμενους κωδικούς
- Ο λογαριασμός κλειδώνει μετά από 3 αποτυχημένες προσπάθειες.

Στο cloud χρησιμοποιούνται οι ίδιοι κωδικοί και προστίθεται ένα επιπλέον επίπεδο ασφάλειας, το λεγόμενο 2-factor authentication. Η συγκεκριμένη διαδικασία εφαρμόζεται μόνο στα εταιρικά κινητά, οπότε δεν έχουν όλοι οι υπάλληλοι πρόσβαση σε αυτήν την υπηρεσία.

Η Office 365 δημιουργεί για κάθε αυθεντικοποίηση ενός χρήστη έναν δεύτερο κωδικό που στέλνεται μέσω εφαρμογής στο εταιρικό κινητό του χρήστη. Η αυθεντικοποίηση δεν εκτελείται αν ο χρήστης δεν δώσει και τους 2 κωδικούς.

Καταστολή κακόβουλου λογισμικού

Η εταιρία εφαρμόζει ένα σύστημα προστασίας 4 επιπέδων.

1. Σε όλους τους υπολογιστές και τους Servers είναι εγκατεστημένο Antivirus που ενημερώνεται καθημερινά.
2. Όλα τα email πριν φτάσουν στο δίκτυο ελέγχονται από το σύστημα Email Security.
3. Το σύνολο του δικτύου προστατεύεται από 3 firewalls που είναι προγραμματισμένα με τις βέλτιστες πολιτικές προστασίας και λειτουργούν με ενημερωμένα firmware.
4. Το Security and Compliance της Microsoft προστατεύει τα δεδομένα που βρίσκονται στο cloud.

Διαχείριση σταθμών εργασίας

Οι σταθμοί εργασίας ακολουθούν τις πολιτικές ασφάλειας κωδικών του domain controller, οι οποίες ορίζουν:

- Μεγάλο μήκος κωδικού με επιπλέον πολυπλοκότητα χαρακτήρων
- Απαγόρευση εγκατάστασης λογισμικού
- αυτόματο logout μετά από 3 λεπτά αδράνειας
- αυτόματη εγκατάσταση και ενημέρωση του antivirus
- εφαρμογή bit locker για την κρυπτογράφηση του σκληρού δίσκου του υπολογιστή
- ενημέρωση του λογισμικού windows 10 μέσω ασφαλούς πολιτικής του WSUS Server

Αντίγραφα ασφαλείας

Η πολιτική των αντιγράφων ασφαλείας είναι αρκετά ασφαλής. Αρχικά τα αντίγραφα των virtual Servers αλλά και του cloud domain αποθηκεύονται στον backup Server. Στη συνέχεια αυτά τα αντίγραφα αντιγράφονται σε 2 διαφορετικά data repositories και μαγνητικές κασέτες μεγάλης χωρητικότητας. Εφαρμόζεται δηλαδή η γνωστή βέλτιστη πολιτική «3,2,1» των αντιγράφων ασφάλειας, που σημαίνει τρία αντίγραφα, δύο εκ των οποίων ηλεκτρονικά σε διαφορετικά μέρη και ένα σε μαγνητικά μέσα. Τέλος, οι virtual Servers αποθηκεύονται ανά δύο ώρες και το cloud domain μία φορά την ημέρα.

Συντήρηση και Λειτουργική ασφάλεια

Τα λογισμικά Dameware και SysAid εκτελούν hardware monitoring στους clients του δικτύου και σε περίπτωση εύρεσης κάποιους προβλήματος τότε η συσκευή ελέγχεται.
Οι ενημερώσεις του λειτουργικού συστήματος εγκαθίστανται βάσει της εφαρμοζόμενης πολιτικής του WSUS. Οι ενημερώσεις ασφάλειας έχουν πάντα προτεραιότητα. Η εγκατάσταση πρώτα γίνεται σε δοκιμαστικό περιβάλλον και μετά σε πραγματικό.

Ασφάλεια δικτύου

Στο τοπικό δίκτυο είναι εγκατεστημένο το λογισμικό PRTG, το οποίο κάνει Network Monitoring που ανακαλύπτει τυχόν ύποπτες κινήσεις δεδομένων στο δίκτυο που μπορεί να αποτελούν ενδείξεις κάποιου είδους κυβερνοεπίθεσης. Στο cloud, η Microsoft προσφέρει το module Security and Compliance. Το module αυτό περιλαμβάνει υπηρεσίες όπως το threat management. Μέσω του threat management δημιουργούνται πολιτικές ανίχνευσης και αντιμετώπισης κινδύνου.

Σε αυτό το σημείο πρέπει να αναφερθεί ότι ενώ στο τοπικό δίκτυο οι χρήστες έχουν πρόσβαση μόνο μέσω υπολογιστών που είναι ενταγμένοι στον domain controller, κάτι αντίστοιχο δεν ισχύει και για την cloud πλατφόρμα. Εκεί κάθε χρήστης μπορεί να συνδεθεί μέσω οποιασδήποτε συσκευής που έχει εγκατεστημένο έναν browser – ακόμα και από τον προσωπικό του χώρο.

Προστασία από πηγές κινδύνων πλην του ανθρώπου

Το δίκτυο αποτελείται από 2 esx-Servers. Όλοι οι virtual Servers σε περίπτωση που ο πρώτος esx-Server σταματήσει να λειτουργεί, τότε γίνεται fail over και οι virtual Servers υποστηρίζονται από τον δεύτερο esx ο οποίος βρίσκεται σε διαφορετικό κτίριο από τον πρώτο και με διαφορετική τροφοδοσία ρεύματος. Στη σπάνια περίπτωση που και οι 2 esx-Servers δεν λειτουργούν τότε εφαρμόζεται σχέδιο ανάκαμψης από καταστροφές (disaster recovery) όπου το σύνολο του δικτύου υποστηρίζεται από Server εξωτερικού service provider. Το δίκτυο είναι καλά προστατευμένο από όλα τα είδη των καταστροφών, φυσικών και μη.

Ασφάλεια τεχνολογικού υλικού - Έλεγχος φυσικής πρόσβασης

Η πρόσβαση στο Server room καθώς και στα τμήματα που κάνουν επεξεργασία προσωπικών δεδομένων είναι ελεγχόμενη με chip.

Η διαγραφή και απόσυρση hardware που φέρουν δεδομένα γίνεται από εγκεκριμένο εξωτερικό service provider που μετά την ασφαλή διαγραφή και την καταστροφή των μέσων, εκδίδει πιστοποιητικό.

Οργάνωση της πολιτικής προστασίας προσωπικών δεδομένων

Υπάρχει τριμελής επιτροπή που αποτελείται από τον διευθυντή του τμήματος πληροφορικής, τον διευθυντή του τμήματος προσωπικού και ένα μέλος του διοικητικού συμβουλίου που παρακολουθούν την διαδικασία της επεξεργασίας και προστασίας των δεδομένων στο σύνολό της. Καθήκον τους η βελτίωση των διαδικασιών σε περίπτωση σφάλματος.

Διαχείριση προσωπικού

Κατά την πρόσληψη ενός υπαλλήλου ακολουθείται συγκεκριμένη διαδικασία χορήγησης εξουσιοδότησης όπου τα δικαιώματα είναι προκαθορισμένα από την θέση του υπαλλήλου. Αλλαγής της εξουσιοδότησης ενός υπαλλήλου γίνεται μόνο με έγκριση του τμήματος πληροφορικής και του διευθυντή του τμήματος, στο οποίο ανήκει ο υπάλληλος. Κατά την αποχώρηση ενός υπαλλήλου ακολουθείται συγκεκριμένη διαδικασία απενεργοποίησης λογαριασμών και αφαίρεσης εξουσιοδότησης. Το πρότυπο εξουσιοδότησης που ακολουθείται είναι το IGAO (Identity – Group – Access - Object) που θεωρείται ένα από τα καλύτερα πρότυπα εξουσιοδότησης για μεσαίες επιχειρήσεις.

4.2.3.2 Αθέμιτη πρόσβαση στα δεδομένα – Απώλεια εμπιστευτικότητας

(Παράρτημα Α, Στιγμιότυπο 6. Απώλεια εμπιστευτικότητας)

Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα δεδομένων αν επέρχονταν ο κίνδυνος;

- Δυσκολία εύρεσης εργασίας
- Δυσκολία σε πρόσβαση χρηματοπιστωτικών υπηρεσιών
- Ψυχολογικό στρες

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

- Παράνομη πρόσβαση
- Ανθρώπινο λάθος
- Κακόβουλο λογισμικό

Ποιες είναι οι πηγές κινδύνου;

- Εξουσιοδοτημένος χρήστης
- Εισβολέας \ Κυβερνοεπίθεση

Ποια από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

- Μέτρο λογικής πρόσβασης
- Ασφάλεια δικτύου
- Διαχείριση σταθμών εργασίας
- Καταστολή κακόβουλου λογισμικού
- Συντήρηση και Λειτουργική ασφάλεια
- Διαχείριση προσωπικού

Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Για τον υπολογισμό των επιπτώσεων θα αξιοποιήσουμε τα αποτελέσματα της αξιολόγησης κινδύνου (ENISA) η οποία έχει ήδη εκπονηθεί. Στον πίνακα 2, το επίπεδο σημαντικότητας του κινδύνου έχει οριστεί ως μέτριο (Medium). Οι επιπτώσεις είναι υλικές και σε μεγάλο βαθμό διαχειρίσιμες και δεν προκαλούν σημαντικές δυσκολίες στις ζωές των υποκειμένων. Η μέτρια σημαντικότητα θα αντιστοιχηθεί με την «περιορισμένη» στην κλίμακα του λογισμικού PIA.

Πώς υπολογίζετε την πιθανότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Το μεγάλο πρόβλημα έγκειται στην επιτρεπόμενη πρόσβαση των χρηστών στην cloud πλατφόρμα μέσω συσκευών που δεν είναι ενταγμένες στον domain controller και δεν ακολουθούν τις πολιτικές ασφάλειας του δικτύου.

4.2.3.3 Ανεπιθύμητη τροποποίηση των δεδομένων – Απώλεια ακεραιότητας (Παράρτημα Α, Στιγμιότυπο 7. Απώλεια ακεραιότητας)

Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα δεδομένων αν επέρχονταν ο κίνδυνος;

- Αδυναμία κάλυψης πρώτων αναγκών
- Αδυναμία κάλυψης πληρωμών χρηματοπιστωτικών ιδρωμάτων
- Ψυχολογικό στρες

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

- Παράνομη πρόσβαση
- Ανθρώπινο λάθος
- Κακόβουλο λογισμικό

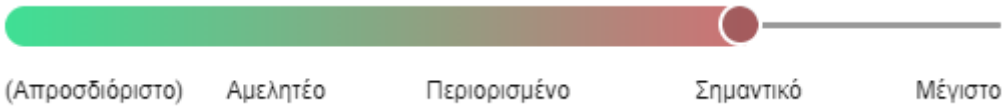
Ποιες είναι οι πηγές κινδύνου;

- Εξουσιοδοτημένος χρήστης
- Εισβολέας \ Κυβερνοεπίθεση

Ποια από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

- Μέτρο λογικής πρόσβασης
- Ασφάλεια δικτύου
- Διαχείριση σταθμών εργασίας
- Καταστολή κακόβουλου λογισμικού
- Συντήρηση και Λειτουργική ασφάλεια
- Διαχείριση προσωπικού

Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;



Η απώλεια ακεραιότητας προκαλεί σημαντικότερες συνέπειες από την απώλεια της εμπιστευτικότητας. Ένας μειωμένος μισθός που υπολογίστηκε λανθασμένα μπορεί να προκαλέσει υψηλό στρες, αδυναμία εξυπηρέτησης των πρώτων αναγκών αλλά και δανειακών πληρωμών. Στον πίνακα 2 της αξιολόγησης κινδύνου του Enisa ορίζεται η

απώλεια ακεραιότητας ως υψηλή. Η αντίστοιχη τιμή στην κλίμακα του λογισμικού PIA είναι η «σημαντική».

Πώς υπολογίζετε την πιθανότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Το μεγάλο πρόβλημα έγκειται στην επιτρεπόμενη πρόσβαση των χρηστών στην cloud πλατφόρμα μέσω συσκευών που δεν είναι ενταγμένες στον domain controller και δεν ακολουθούν τις πολιτικές ασφάλειας του δικτύου.

4.2.3.4 Εξαφάνιση δεδομένων - Απώλεια διαθεσιμότητας (Παράρτημα Α, Στιγμιότυπο 8. Απώλεια διαθεσιμότητας)

Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα των δεδομένων σε περίπτωση επέλευσης του κινδύνου;

- Αδυναμία κάλυψης πρώτων αναγκών
- Αδυναμία κάλυψης πληρωμών χρηματοπιστωτικών ιδρωμάτων
- Ψυχολογικό στρες

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

- Ανθρώπινο λάθος
- Κακόβουλο λογισμικό
- Δολιοφθορά \ Καταστροφή

Ποιες είναι οι πηγές κινδύνου;

- Φυσικές καταστροφές
- Εξουσιοδοτημένος χρήστης
- Εισβολέας \ Κυβερνοεπίθεση

Ποια από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

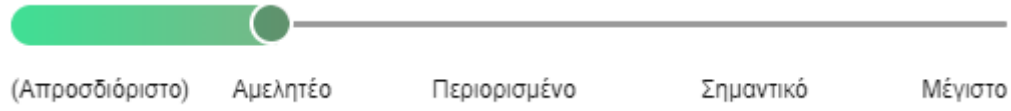
- Μέτρο λογικής πρόσβασης
- Ασφάλεια δικτύου

- Αντίγραφα ασφαλείας
- Καταστολή κακόβουλου λογισμικού
- Έλεγχος φυσικής πρόσβασης
- Προστασία από πηγές κινδύνων πλην του ανθρώπου

Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

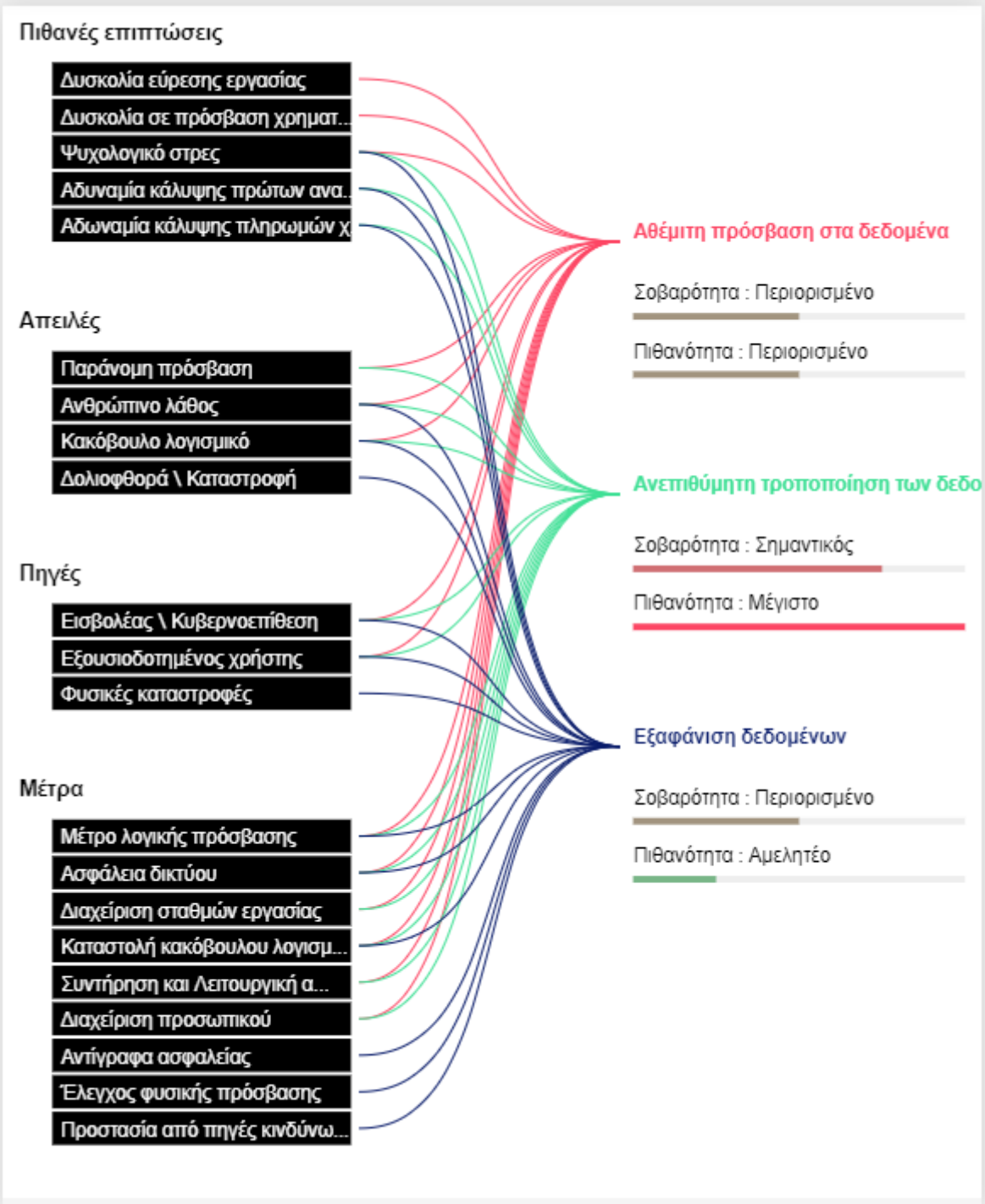
Από τον πίνακα 2 της αξιολόγησης του Enisa, η επικινδυνότητα της απώλειας της διαθεσιμότητας ορίζεται ως μέτρια. Η αυστηρή πολιτικής ασφάλειας φύλαξης αντιγράφων θα αντιμετωπίσει μία πιθανή απώλεια της διαθεσιμότητας. Στην κλίμακα του λογισμικού PIA θα αντιστοιχεί στην «περιορισμένη»

Πώς υπολογίζετε την πιθανότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;



Η πιθανότητα να είναι όλα τα αντίγραφα ασφάλειας προβληματικά ή μη προσβάσιμα και ταυτόχρονα τα δεδομένα στο cloud να είναι και αυτά μη προσβάσιμα είναι αμελητέα.

4.2.3.5 Επισκόπηση κινδύνων (Παράρτημα Α, Στιγμιότυπο 9. Επισκόπηση κινδύνων)



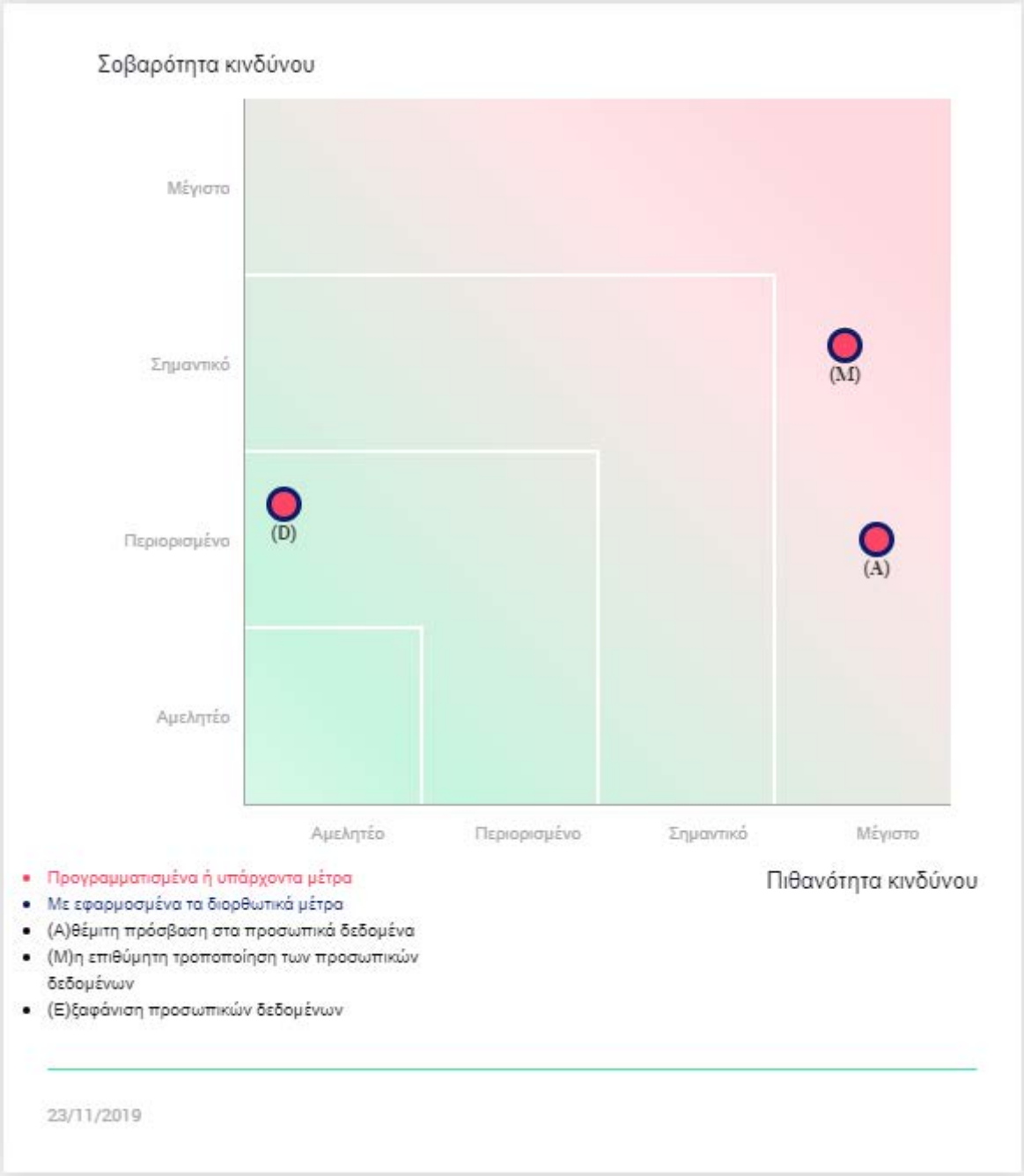
Διάγραμμα 1. Διάγραμμα επισκόπησης κινδύνων

Στο διάγραμμα 1, απεικονίζονται οι σχέσεις που έχουν οι 3 κίνδυνοι απώλειας με τις επιπτώσεις, τις απειλές, τις πηγές και τα μέτρα εναντίον των κινδύνων που έχουμε ορίσει στα προηγούμενα βήματα.

4.2.4 Επικύρωση

4.2.4.1 Χαρτογράφηση κινδύνων (Παράρτημα Α, Στιγμιότυπο 10. Χαρτογράφηση κινδύνων)

4.2.4.2



Διάγραμμα 2. Συνάρτηση πιθανότητας-σοβαρότητας κινδύνων

Όπως σωστά απεικονίζεται στο διάγραμμα 2, η σοβαρότητα της εξαφάνιση δεδομένων (D) είναι περιορισμένη λόγω της φύσης του συστήματος και ως προς την πιθανότητα είναι αμελητέα. Υψηλές πιθανότητες κινδύνων εμφανίζουν η αθέμιτη πρόσβαση (Α) και η ανεπιθύμητη τροποποίηση (Μ) λόγω των θεμάτων ασφάλειας που προαναφέρθηκαν

με διαφορετικά επίπεδα σημαντικότητας, με υψηλότερη την τροποποίηση των δεδομένων.

4.2.4.3 Σχέδιο Δράσης

Σε αυτό το σημείο το λογισμικό ζητάει από την ομάδα που εκτελεί την ΕΑΠΔ να επανελέξει όλα τα δεδομένα-απαντήσεις (Στιγμιότυπο 11. Αίτημα αξιολόγησης ανάλυσης), να επιλέξει τα σημεία όπου χρειάζονται βελτιώσεις (μπλε χρώμα) ή διορθώσεις (κόκκινο χρώμα) ή είναι ορθά (πράσινο χρώμα) και να καταγράψει βελτιωτικά μέτρα. Η λίστα με τα σημεία που ελέγχθηκαν (Στιγμιότυπο 13. Σχέδιο δράσης – Αξιολογημένα σημεία) είναι η ακόλουθη:

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

- Ελαχιστοποίηση του αριθμού των δεδομένων προσωπικού χαρακτήρα
- Μέτρο λογικής πρόσβασης
- Καταστολή κακόβουλου λογισμικού
- Διαχείριση σταθμών εργασίας
- Αντίγραφα ασφαλείας
- Συντήρηση και Λειτουργική ασφάλεια
- Ασφάλεια δικτύου
- Έλεγχος φυσικής πρόσβασης

- Προστασία από πηγές κινδύνων πλην του ανθρώπου
- Ασφάλεια τεχνολογικού υλικού
- Οργάνωση της πολιτικής προστασίας προσωπικών δεδομένων
- Διαχείριση προσωπικού

Κίνδυνοι

- Αθέμιτη πρόσβαση στα προσωπικά δεδομένα
- Ανεπιθύμητη τροποποίηση των προσωπικών δεδομένων
- Εξαφάνιση προσωπικών δεδομένων

4.2.4.4 Βελτιωτικά μέτρα

Κατά την διάρκεια της δοκιμαστικής περιόδου που το τμήμα πληροφορικής σχεδίαζε βελτιωτικά μέτρα παρατηρήθηκε μία σοβαρή αρνητική επίπτωση που προκλήθηκε από το κύριο πρόβλημα του υπάρχοντος συστήματος που είναι η απουσία καθολικής πολιτικής ασφάλειας των συσκευών που συνδέονται στη cloud πλατφόρμα. Οι χρήστες της office 365 άρχισαν να εγκαθιστούν το λογισμικό και στους προσωπικούς τους υπολογιστές επειδή κάθε άδεια επιτρέπει την εγκατάσταση σε 5 διαφορετικές συσκευές. Οι χρήστες άρχισαν να χρησιμοποιούν τις κλασσικές εφαρμογές όπως word, excel και OneDrive. Το αποτέλεσμα της χρήσης αυτής ήταν η αποθήκευση προσωπικών εγγράφων των χρηστών στο OneDrive. Οι λογαριασμοί OneDrive των χρηστών περιέχονται και αυτοί στο backup της πλατφόρμας. Ως αποτέλεσμα παρατηρήθηκε πρώτα η αφύσικη αύξηση του όγκου των δεδομένων των λογαριασμών OneDrive. Εξετάστηκαν κάποιοι λογαριασμοί και εντοπίστηκαν προσωπικά αρχεία των χρηστών όπως λογαριασμοί, αποδείξεις κ.α.. Το γεγονός αυτό σηματοδότησε την επείγουσα αλλαγή της πολιτικής χρήσης του λογισμικού από τους χρήστες αλλά και την αλλαγή της πολιτικής ασφάλειας της πρόσβασης στην πλατφόρμα.

Η μόνη λύση απαιτούσε την εγκατάσταση της premium έκδοσης του online Azure Server. Η έκδοση αυτή έδωσε τη δυνατότητα στο τμήμα πληροφορικής να ορίσει καινούρια πολιτική ασφάλειας πρόσβασης, σύμφωνα με την οποία η αυθεντικοποίηση εκτελείται μόνο αν η συσκευή είναι ενταγμένη στον local domain controller και ακολουθεί την πολιτική ασφάλειας του controller. Η συγκεκριμένη λύση αποτελεί σημαντική βελτίωση των τομέων Ασφάλεια δικτύου, Αθέμιτη πρόσβαση στα προσωπικά δεδομένα και Ανεπιθύμητη τροποποίηση των προσωπικών δεδομένων. Οι χρήστες πλέον μπορούν να συνδεθούν στην πλατφόρμα μόνο μέσω ελεγμένων συσκευών και μόνο σε αυτές μπορούν να εγκατασταθεί.

Διάρκεια αποθήκευσης

Σχεδιασμός ενιαίας πολιτικής της αποθήκευσης δεδομένων από το τμήμα πληροφορικής για μία πιο διαφανή οργάνωση των αποθηκευμένων δεδομένων, προσωπικών και μη.

Πληροφορίες για τα υποκείμενα των δεδομένων

Τα υποκείμενα πρέπει να ενημερωθούν για τον σκοπό της δεύτερης επεξεργασίας των στατιστικών αξιολογήσεων.

Δικαιώματα πρόσβασης, φορητότητας , διόρθωσης, διαγραφής, περιορισμού και εναντίωσης

Τα υποκείμενα πρέπει να ενημερωθούν ότι τα αιτήματά τους πρέπει να απαντώνται εντός 30 ημερών από την μέρα υποβολής (ακόμα και αν δεν μπορούν να ικανοποιηθούν, πρέπει να υπάρξει τεκμηριωμένη απάντηση εντός αυτού του χρονικού διαστήματος). Οι διαδικασίες άσκησης των δικαιωμάτων τους λειτουργούν.

Ελαχιστοποίηση του αριθμού των δεδομένων προσωπικού χαρακτήρα

Θα πρέπει να γίνει έλεγχος της αναγκαιότητας των δεδομένων στην επεξεργασία των στατιστικών αναλύσεων.

Μέτρο λογικής πρόσβασης

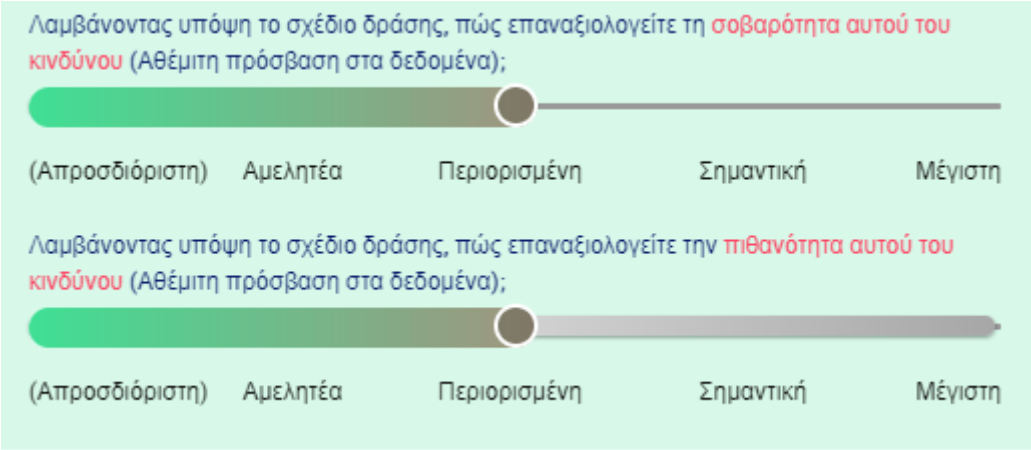
Χορήγηση εταιρικού κινητού, το οποίο ακολουθεί την πολιτική ασφάλειας του domain controller, σε όλους τους χρήστες που επεξεργάζονται προσωπικά δεδομένα και χρήση της εφαρμογής office για τη multifactor αυθεντικοποίηση για επιπλέον ασφάλεια.

Ασφάλεια δικτύου

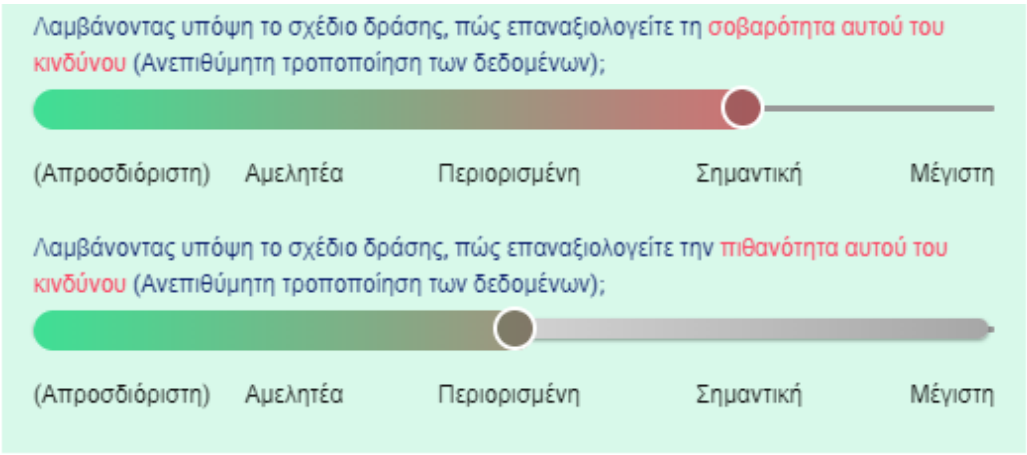
Εφαρμογή της καινούριας πολιτικής του Azure Online.

4.2.4.5 Εφαρμογή βελτιωτικών μέτρων

Η εφαρμογή των μέτρων και κυρίως της καινούριας πολιτικής του Azure Online επηρεάζουν σημαντικά τις πιθανότητες της εμφάνισης των κινδύνων. Πιο συγκεκριμένα, η πιθανότητα απώλειας της εμπιστευτικότητας θα περιοριστεί και από «μέγιστη» θα μειωθεί σε «περιορισμένη» και η σοβαρότητα κινδύνου θα παραμείνει σταθερή.



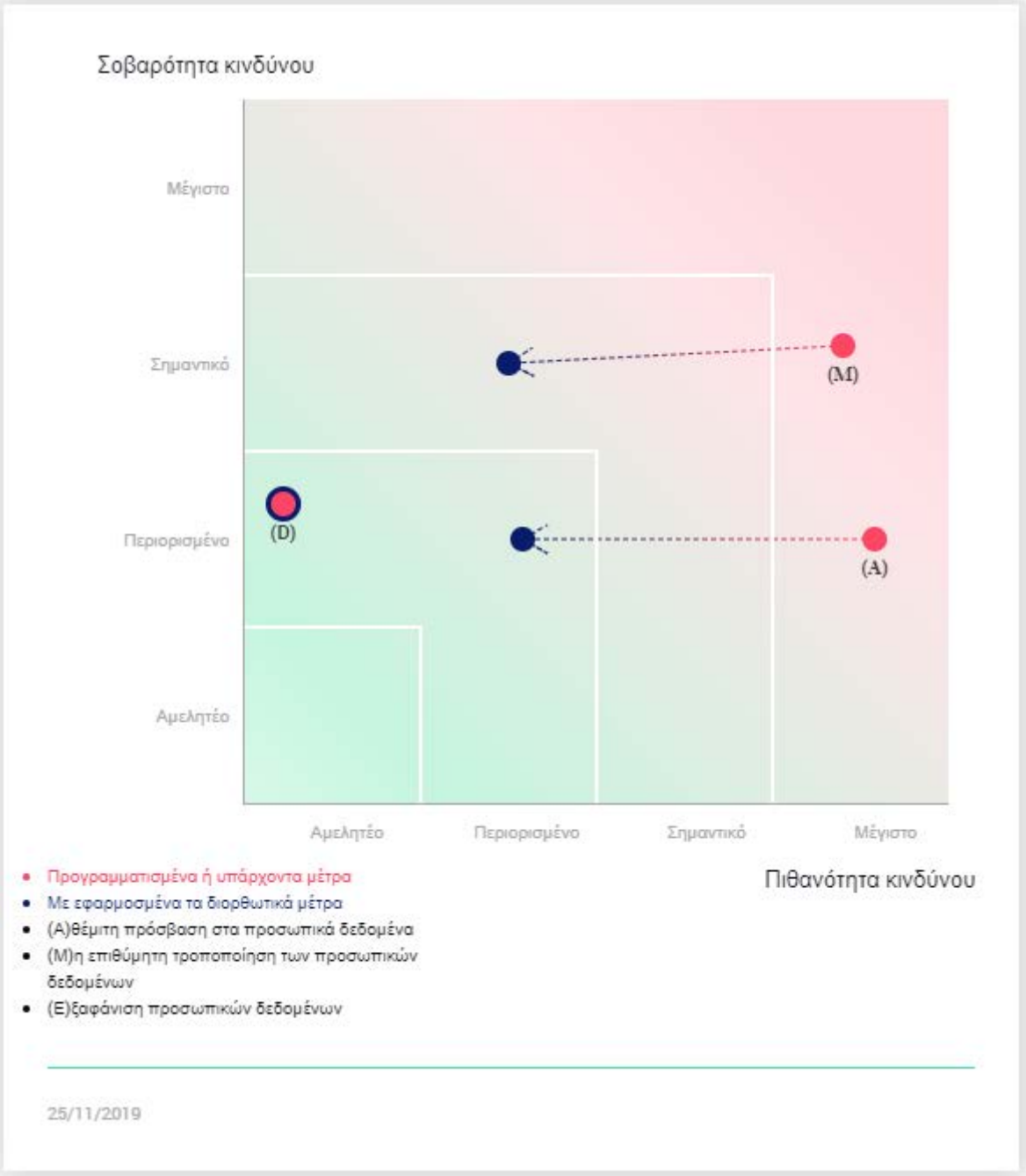
Όσον αφορά την απώλεια της ακεραιότητας, η πιθανότητα ομοίως θα υποχωρήσει από «μέγιστη» σε «περιορισμένη» και η σοβαρότητα του κινδύνου θα παραμείνει υψηλή.



Τα μέτρα δεν επηρεάζουν την σοβαρότητα της απώλειας της διαθεσιμότητας και η πιθανότητα εμφάνισής παραμένει «αμελητέα».

4.2.4.6 Χαρτογράφηση κινδύνων μετά την εφαρμογή των μέτρων

(Στιγμιότυπο 12. Χαρτογράφηση κινδύνων μετά την εφαρμογή των βελτιωτικών μέτρων.)



Διάγραμμα 3. Συνάρτηση πιθανότητας-σοβαρότητας κινδύνων μετά την εφαρμογή βελτιωτικών μέτρων.

Στο διάγραμμα 3 παρατηρούμε ότι οι πιθανότητες της αθέμιτης πρόσβασης και της ανεπιθύμητης τροποποίησης μειώνονται ενώ η σοβαρότητα κινδύνου δεν παρουσιάζει μεταβολή. Η σοβαρότητα του κινδύνου δεν επηρεάζεται από τα μέτρα αλλά ορίζεται αρχικά με βάση τη μελέτη του συνολικού συστήματος επεξεργασίας.

Το τελικό στάδιο είναι εκείνο της απόφασης για την έγκριση της επεξεργασίας ή της αρνητικές γνωμοδότησης (Στιγμιότυπο 14. Επικύρωση της ΕΑΠΔ).

Κεφάλαιο 5ο
Επίλογος

Η παρούσα διατριβή πραγματεύτηκε τη διαδικασία εκτίμησης αντικτύπου προστασίας προσωπικών δεδομένων, επί ενός ρεαλιστικού σεναρίου επεξεργασίας προσωπικών δεδομένων το οποίο είναι ευρέως διαδεδομένο (αξιοποίηση υπολογιστικού νέφους), για δύο διαφορετικούς σκοπούς επεξεργασίας.

Στο πλαίσιο αυτό, δεδομένου ότι τμήμα της εκτίμησης αντικτύπου αποτελεί ουσιαστικά μία διαχείριση κινδύνων ασφάλειας, αξιοποιήθηκε μια αρχικώς εκπονηθείσα τέτοια διαχείριση, η οποία αποσκοπεί ακριβώς στην ασφάλεια προσωπικών δεδομένων. Με αυτόν τον τρόπο, εκτιμάται ότι διευκολύνεται σημαντικά η εκπόνηση εκτίμησης αντικτύπου στο σύνολό της

5.1 Συμπεράσματα

Το αρχικό συμπέρασμα της διπλωματικής διατριβής είναι ότι τα αποτελέσματα της εκτίμησης κινδύνου ασφάλειας μιας επεξεργασίας προσωπικών δεδομένων μπορούν να λειτουργήσουν ως βάση για την εκτίμησης αντικτύπου σχετικά με τα προσωπικά δεδομένα της ίδιας επεξεργασίας. Ουσιαστικά, η εκτίμηση κινδύνων ασφάλειας είναι ένα υποσύνολο της εκτίμησης αντικτύπου και το γεγονός αυτό οφείλεται στο μεγάλο εύρος της έρευνας που απαιτεί η ΕΑΠΔ.

Ενδιαφέρον παρατηρείται και στην ταυτόχρονη ανάλυση δύο επεξεργασιών με διαφορετικούς σκοπούς. Όταν δύο διαφορετικές επεξεργασίες με διαφορετικούς σκοπούς, οι οποίοι σχετίζονται με νομικές υποχρεώσεις και έννομα συμφέροντα, εκτελούνται από το ίδιο υπολογιστικό σύστημα και χρησιμοποιούν την ίδια βάση δεδομένων, εμφανίζουν σχεδόν όμοιες επισφάλειες – ιδίως δε ως προς την ασφάλεια της επεξεργασίας. Αυτό συνεπάγεται μεγάλη ομοιότητα στα μέτρα που θα ληφθούν για τη βελτίωση της ασφάλειας αλλά στα μέτρα συμμόρφωσης ως προς τον ΓΚΠΔ ενδέχεται να υπάρξουν διαφορές.

Τέλος, η επεξεργασία προσωπικών δεδομένων στο υπολογιστικό νέφος (cloud) παρουσιάζει αρκετά κενά ασφάλειας. Η απώλεια ακεραιότητας και η απώλειας

εμπιστευτικότητας είναι οι βασικές αρχές ασφάλειας που βάλλονται. Η πρόσβαση στην πλατφόρμα πρέπει να οργανωθεί με αυστηρές πολιτικές ασφάλειας που θα ελαχιστοποιούν τον αριθμό των χρηστών και των συσκευών που θα έχουν πρόσβαση.

Η παρούσα διατριβή μπορεί να αποτελέσει βάση αναφοράς για οποιονδήποτε φορέα καλείται να πραγματοποιήσει, λόγω της σχετικής νομικής υποχρέωσης που απορρέει από το ΓΚΠΔ, εκτίμηση αντικτύπου προστασίας δεδομένων για επεξεργασίες συναφείς με αυτές που μελετήθηκαν στην παρούσα διατριβή. Εξάλλου, οι εν λόγω επεξεργασίες είναι εξαιρετικά πιθανό, λόγω της φύσης τους, να πραγματοποιούνται αντιστοίχως από πάρα πολλούς υπευθύνους επεξεργασίας.

5.2 Θέματα μελλοντικής έρευνας

Αρκετά ενδιαφέρουσα θα ήταν η εφαρμογή της μεθοδολογίας που αναλύεται στο Κεφάλαιο 3ο, χρησιμοποιώντας διαφορετικά εργαλεία διαχείρισης κινδύνου και εκτίμησης αντικτύπου. Για παράδειγμα, τα αποτελέσματα του συνδυασμού της χρήσης της διαχείρισης κινδύνου Octave [10] με το πρότυπο της εκτίμησης αντικτύπου της αγγλικής επιτροπής πληροφόρησης [11] θα μπορούσαν να συγκριθούν με τα αποτελέσματα της συγκεκριμένης διπλωματικής εργασίας, με σκοπό την οριοθέτηση της εφαρμογής μιας εκτίμησης αντικτύπου, αφού δεν ορίζεται αυστηρά από τον Γενικό Κανονισμό.

Η διεπαφή (interface) του λογισμικού PIA- Εκτίμηση αντικτύπου, το οποίο αξιοποιήθηκε στο πλαίσιο της παρούσας διατριβής, αφήνει σημαντικά περιθώρια βελτίωσης, δεδομένου ότι το λογισμικό είναι ανοιχτού κώδικα. Ανάμεσα στις θεματικές ενότητες «Θεμελιώδεις Αρχές» και «Κίνδυνοι» θα μπορούσε αρχικά να εισαχθεί μία καινούρια ενότητα αφιερωμένη στα μέτρα. Μία τέτοια ενότητα θα συμπεριλάμβανε τα μέτρα που αφορούν την άσκηση των δικαιωμάτων των υποκειμένων, που ανήκουν στις «Θεμελιώδεις Αρχές», και τα μέτρα ασφάλειας του υπολογιστικού συστήματος, που ανήκουν στην ενότητα «Κίνδυνοι». Παράλληλα, θα πρέπει ο χρήστης να έχει την ικανότητα, να αξιολογεί κάθε μέτρο ξεχωριστά όσον αφορά την αποτελεσματικότητά του και να αντιστοιχεί το μέτρο στις βασικές κατηγορίες ασφάλειας πληροφοριακών συστημάτων που είναι η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Όταν το μέτρο έχει χαμηλή βαθμολογία, θα πρέπει να απαιτείται η περιγραφή των κινδύνων που απορρέουν και η αξιολόγησή τους.

Στη συνέχεια, στην ενότητα «Κίνδυνοι» σκόπιμο είναι να εμφανίζονται οι κίνδυνοι λόγω χαμηλής βαθμολογίας κάποιοι μέτρου και θα πρέπει επίσης να προβλεφθεί και η ανεξάρτητη δημιουργία κινδύνων που δεν απορρέουν από κάποιο υπάρχον μέτρο. Κάθε κίνδυνος θα πρέπει να αντιστοιχίζεται σε βασική αρχή ασφάλειας και να βαθμολογείται η σοβαρότητα και η πιθανότητα εμφάνισής του.

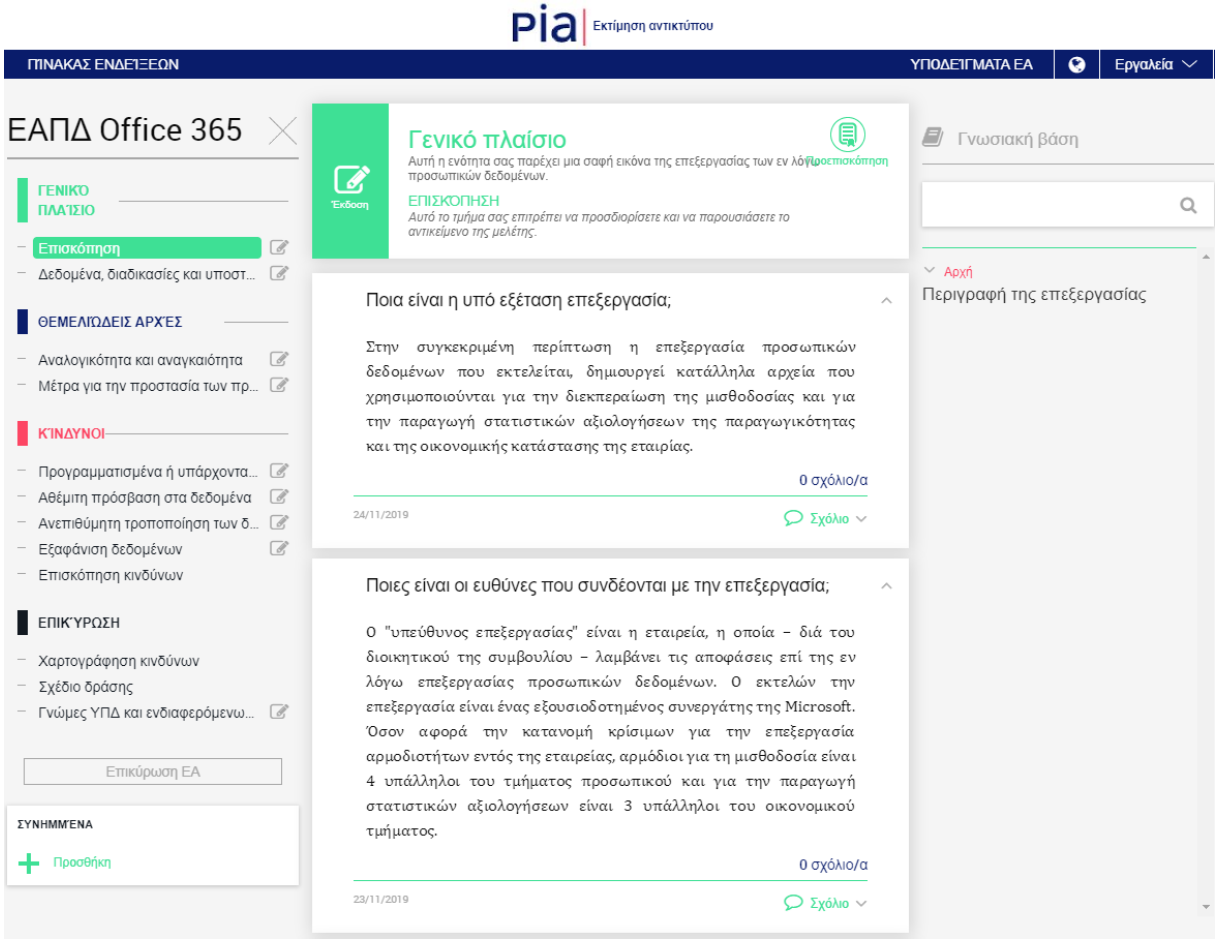
Η αξιολόγηση της απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας θα πρέπει να σχεδιαστούν σε καινούρια ενότητα με όνομα «Αξιολόγηση». Στο συγκεκριμένο Interface θα μπορούσε να γίνει εισαγωγή μιας τέταρτης παραμέτρου, της εγκυρότητας, επειδή αφενός αποτελεί βασική αρχή στην επεξεργασία δεδομένων και αφετέρου προβλέπεται και από τον Γενικό Κανονισμό. Ο χρήστης θα μπορεί να βλέπει ποια μέτρα και ποιοι κίνδυνοι αντιστοιχούν σε ποιες βασικές αρχές ασφάλειας. Επίσης θα πρέπει να έχει τη δυνατότητα στην καινούρια ενότητα να αξιολογήσει αυτόνομα σε γενικότερα πλαίσια τις αρχές της ασφάλειας , η οποία βαθμολογία θα αποτελεί την τρίτη παράμετρο.

Η συνολική αξιολόγηση θα είναι ο συνδυασμός της αξιολόγησης των μέτρων, των κινδύνων και της αυτόνομης βαθμολογία της ενότητας «Αξιολόγηση». Αν και το σύστημα φαντάζει πολύπλοκο, η αξιολόγηση εξαρτάται από περισσότερες σχετικές παραμέτρους, γεγονός που την δίνει μεγαλύτερη ακρίβεια.

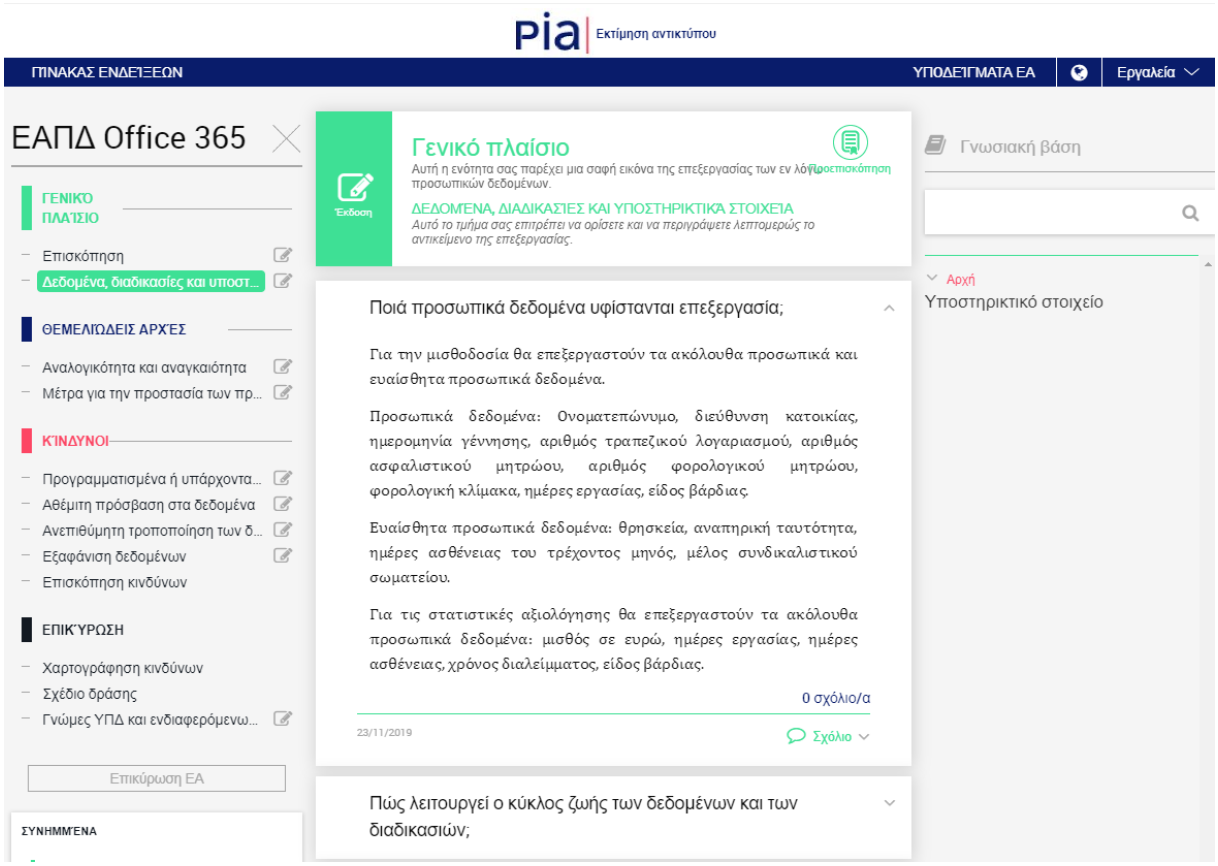
Παράρτημα Α

Στιγμιότυπα του λογισμικού PIA

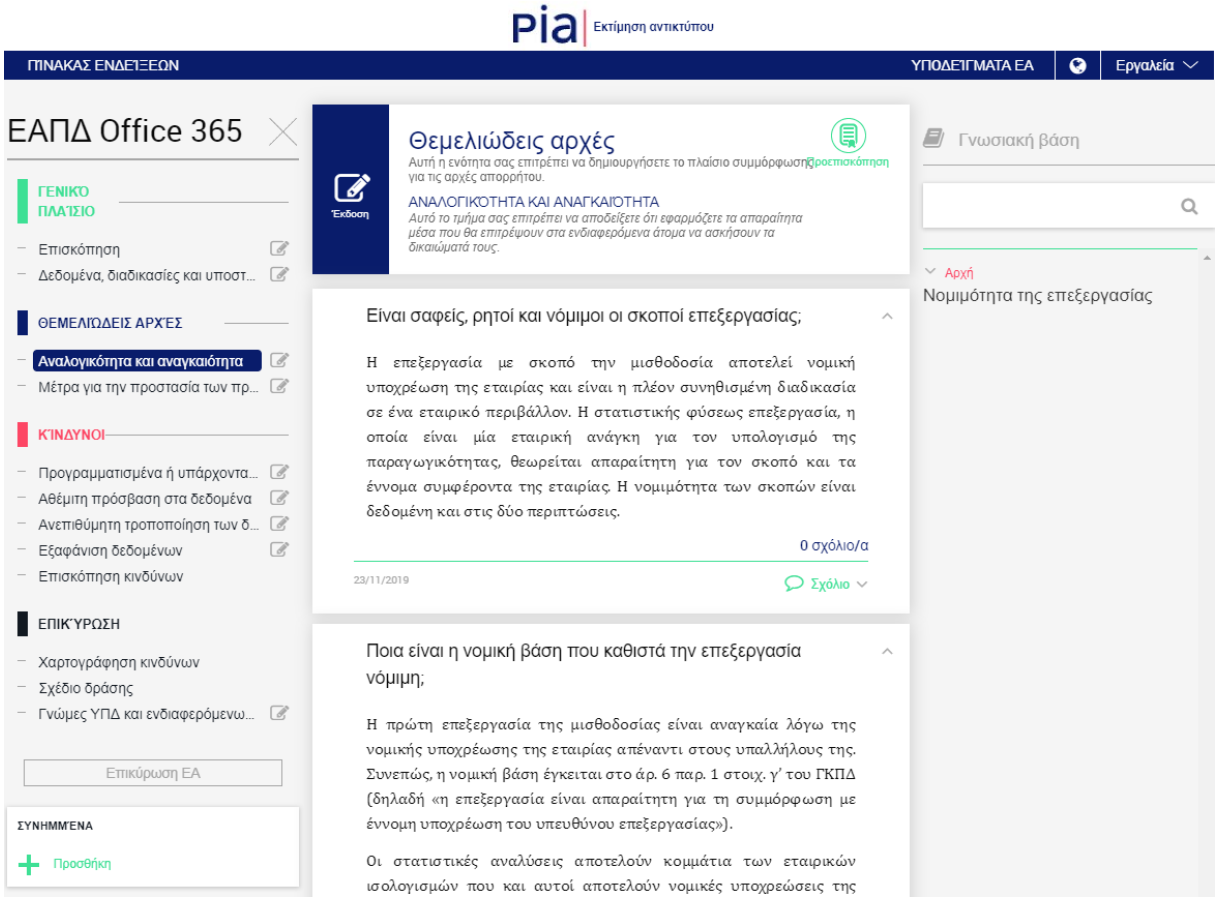
Α.1 Στιγμιότυπα



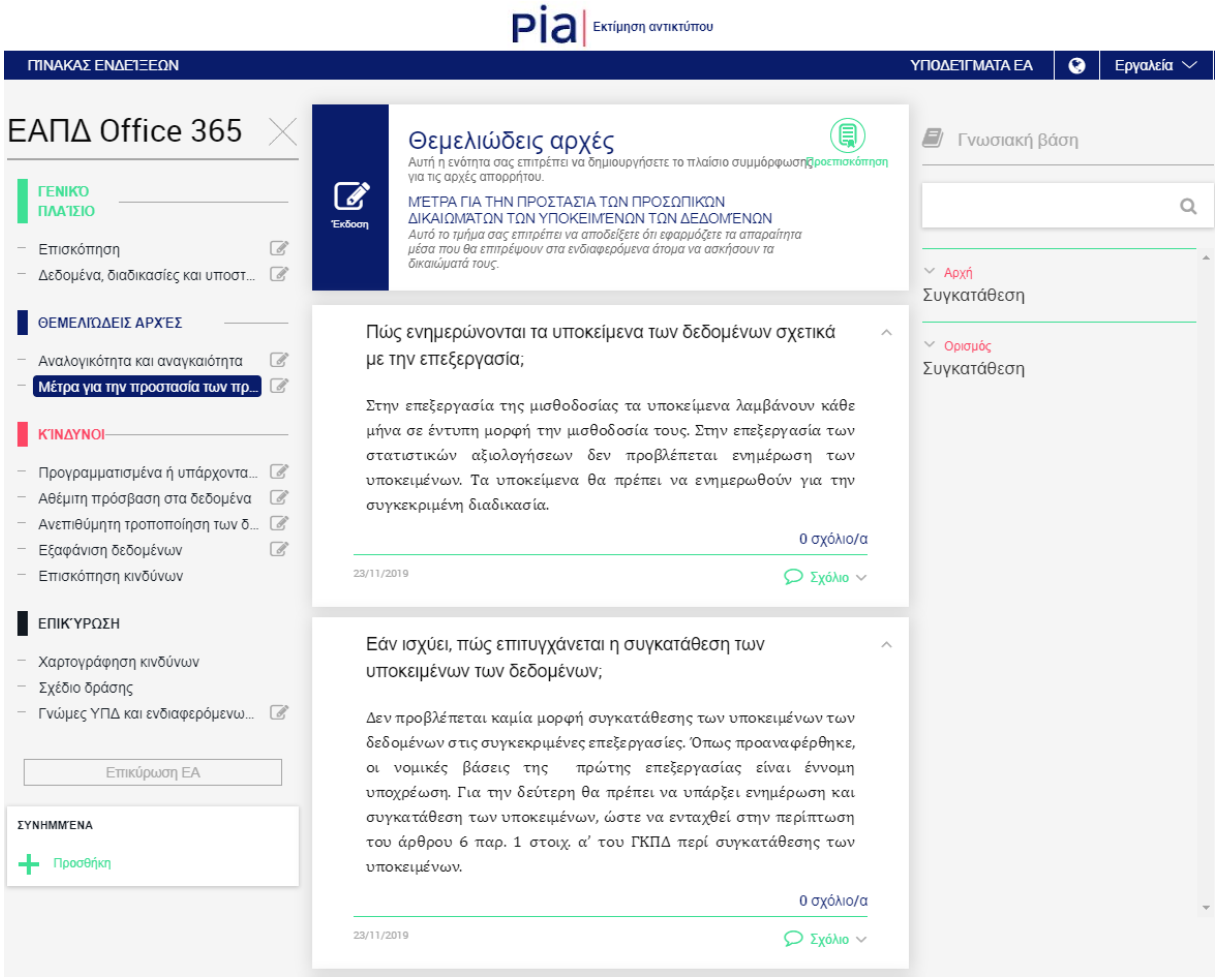
Στιγμιότυπο 1. Επισκόπηση.



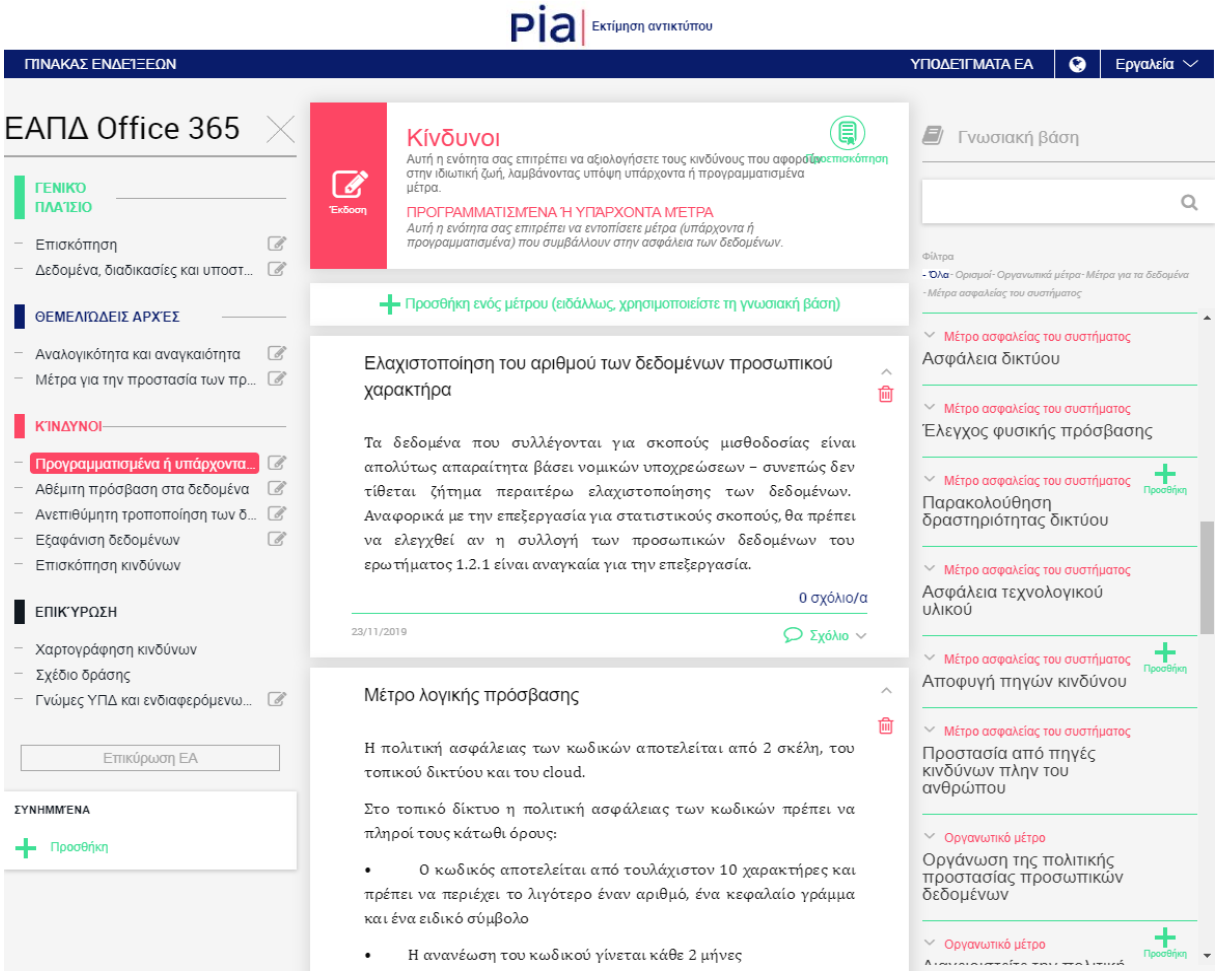
Στιγμιότυπο 2. Δεδομένα, Διαδικασίες και υποστηρικτικά στοιχεία.



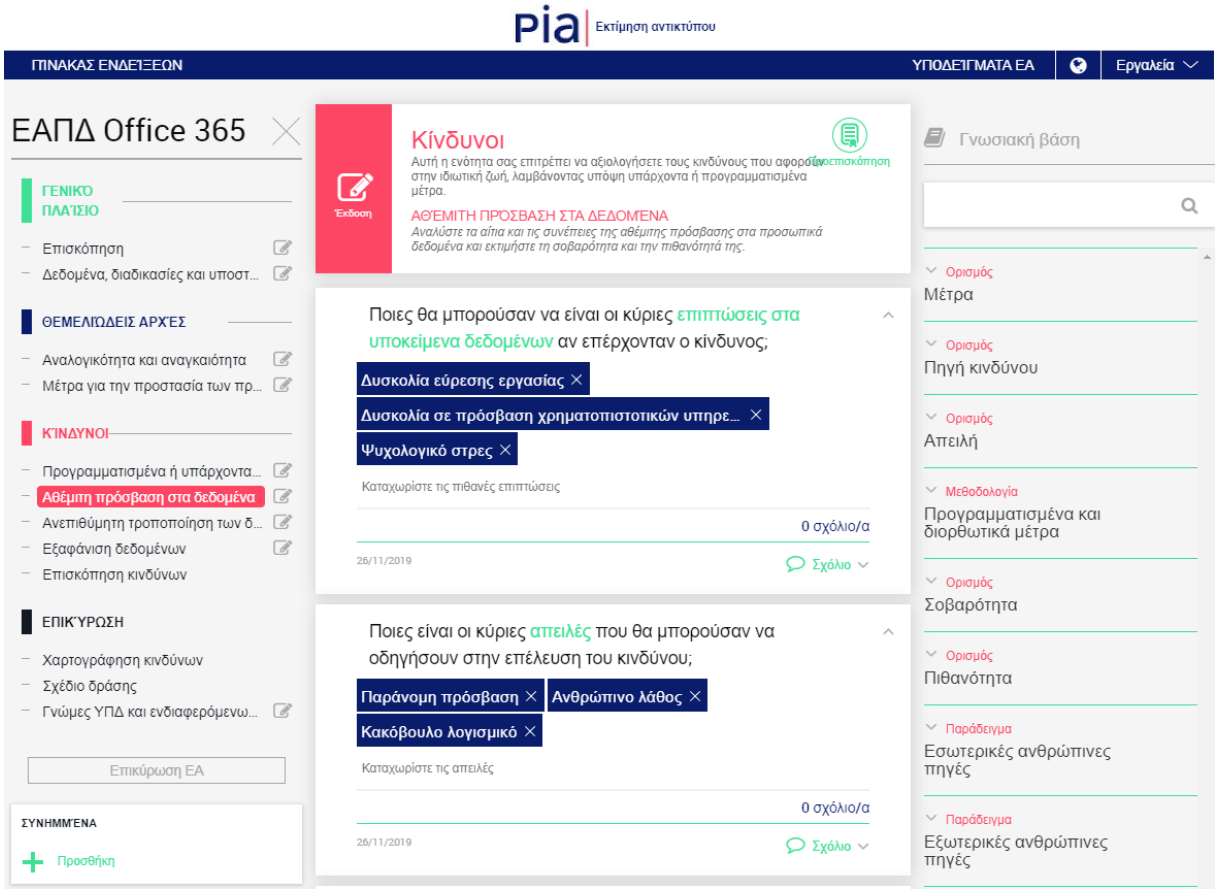
Στιγμιότυπο 3. Αναλογικότητα και αναγκαιότητα.



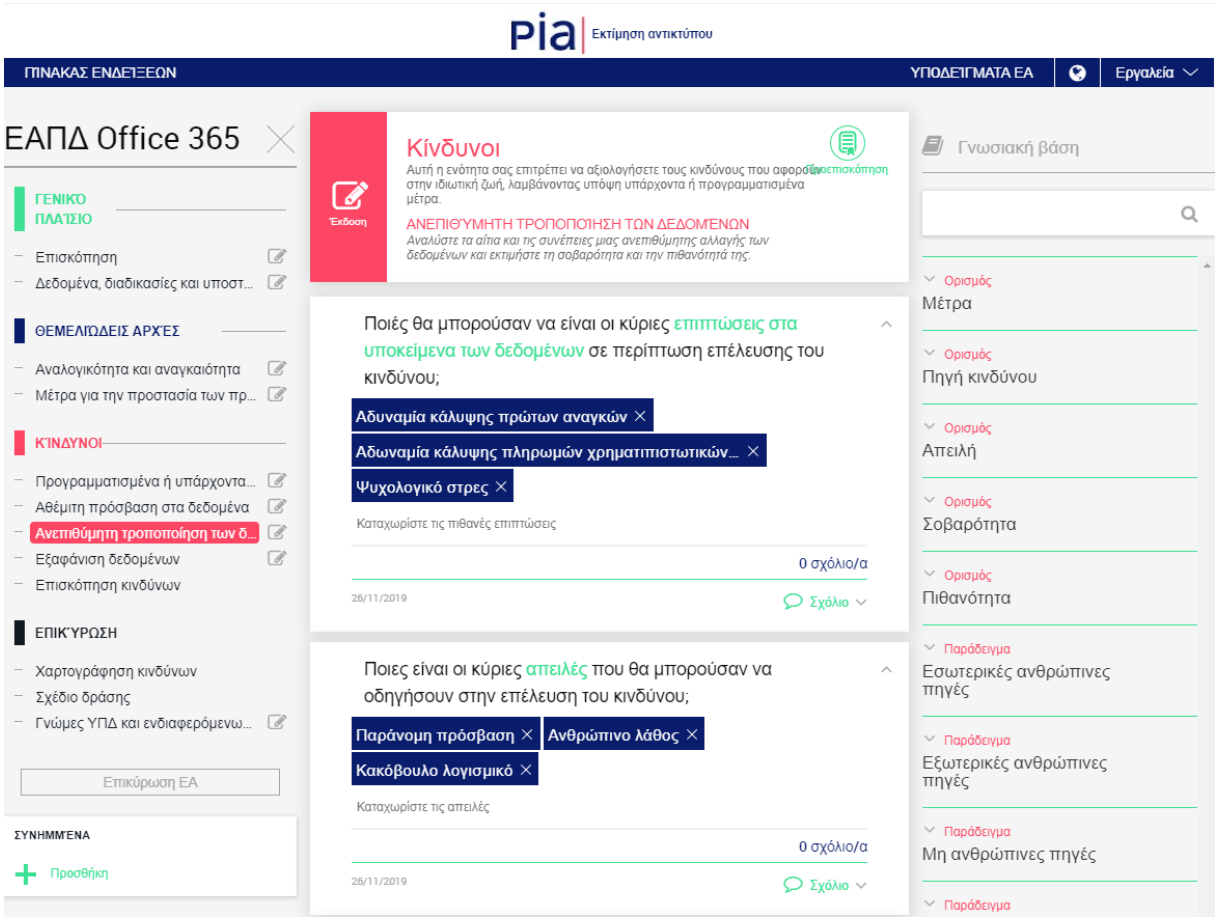
Στιγμιότυπο 4. Μέτρα για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων.



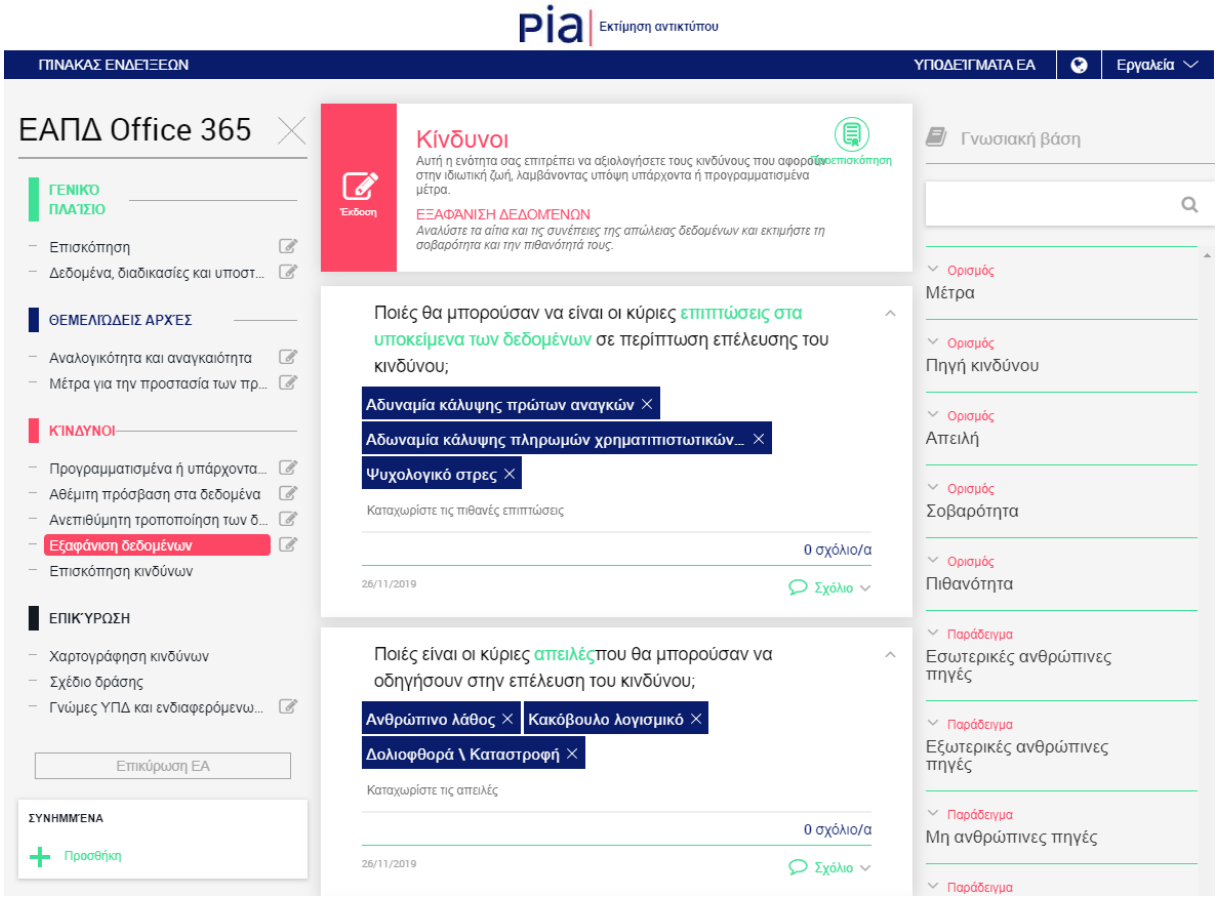
Στιγμιότυπο 5. Προγραμματισμένα ή υπάρχοντα μέτρα.



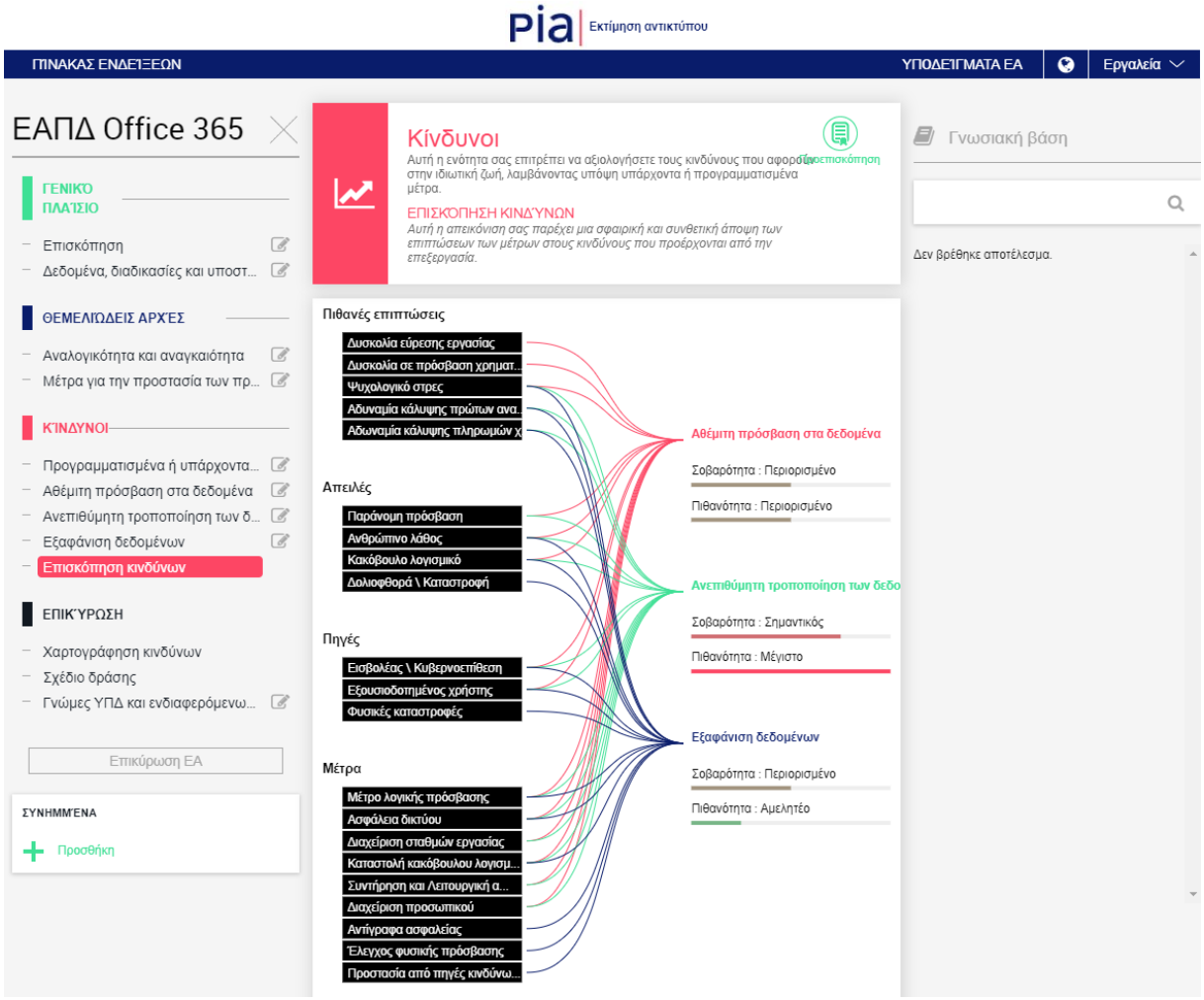
Στιγμιότυπο 6. Απώλεια εμπιστευτικότητας.



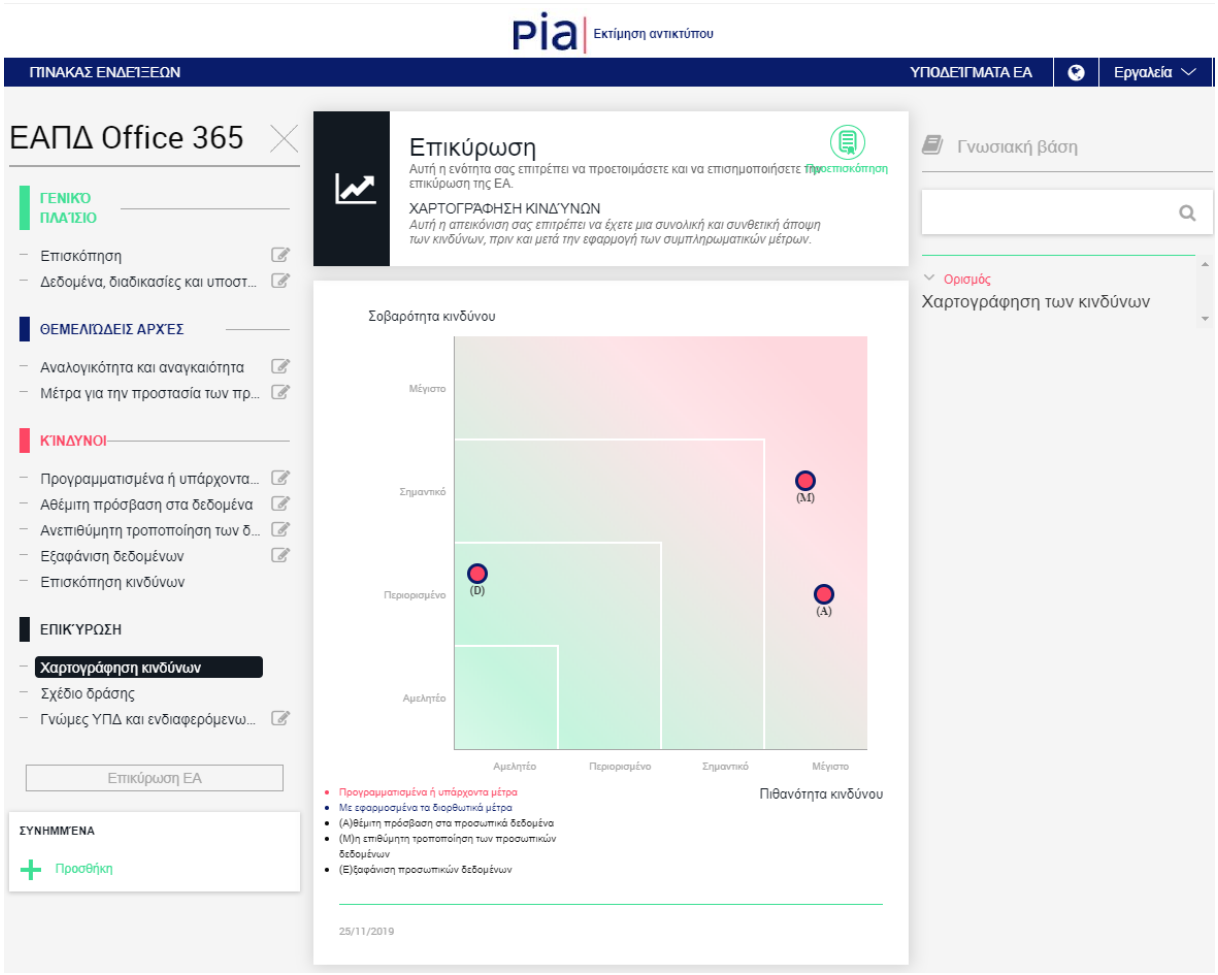
Στιγμιότυπο 7. Απώλεια ακεραιότητας.



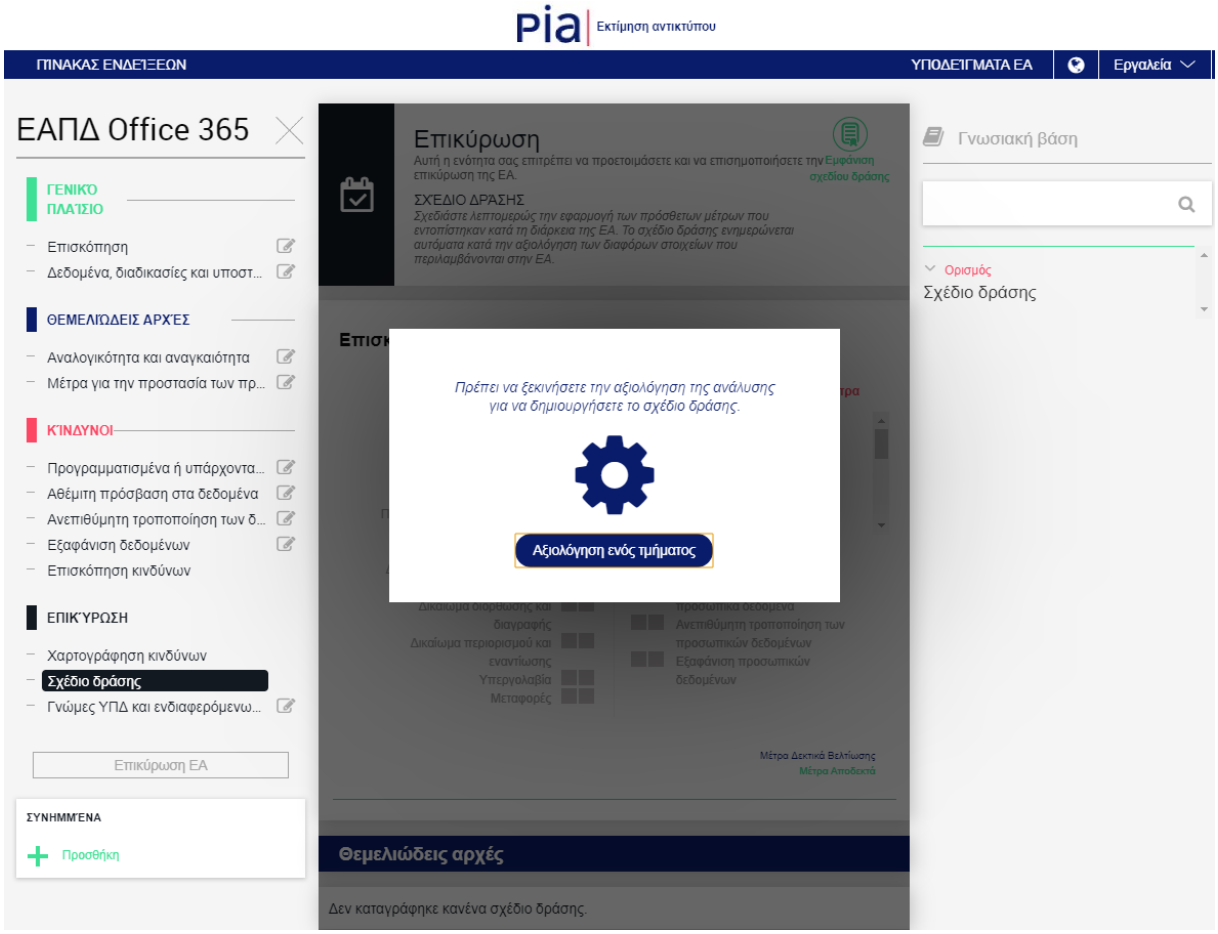
Στιγμιότυπο 8. Απώλεια διαθεσιμότητας.



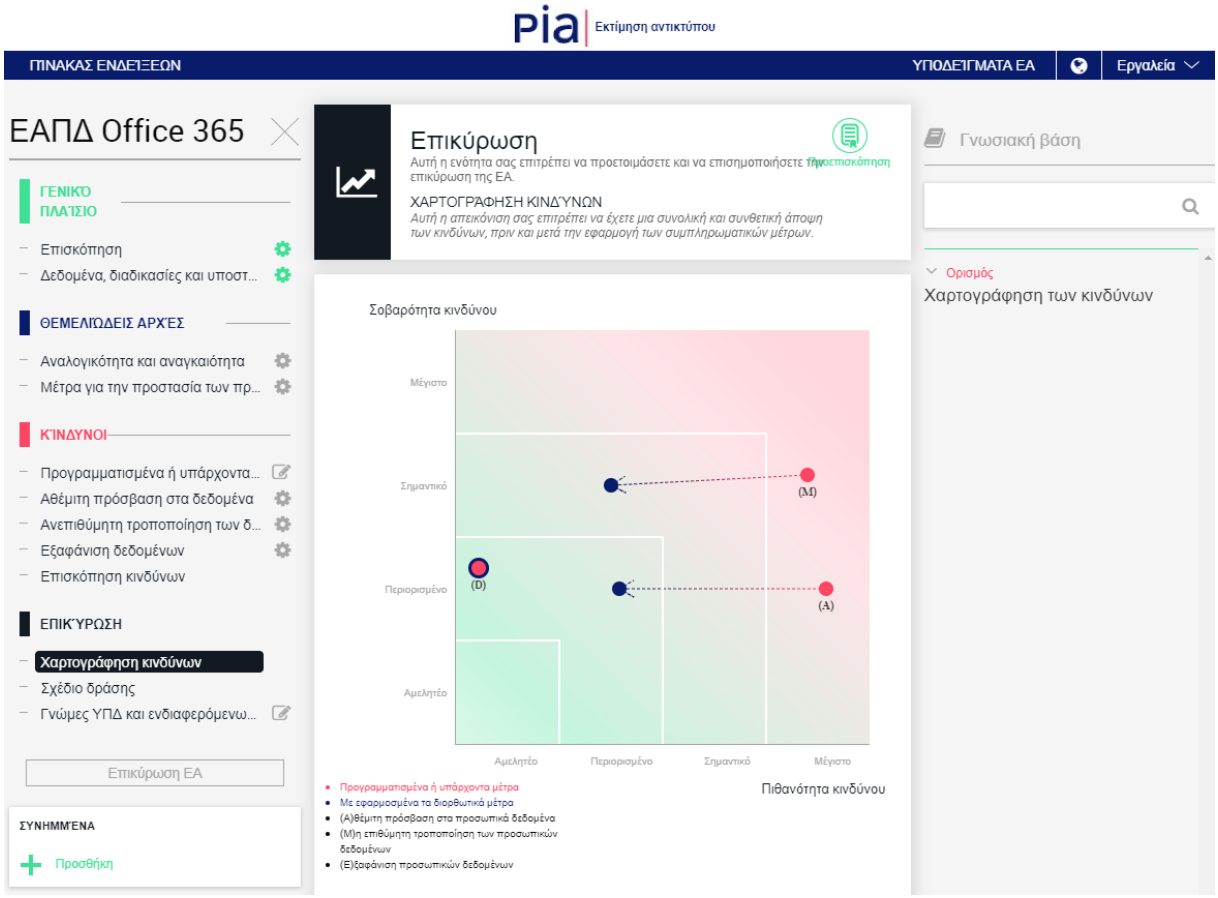
Στιγμιότυπο 9. Επισκόπηση κινδύνων.



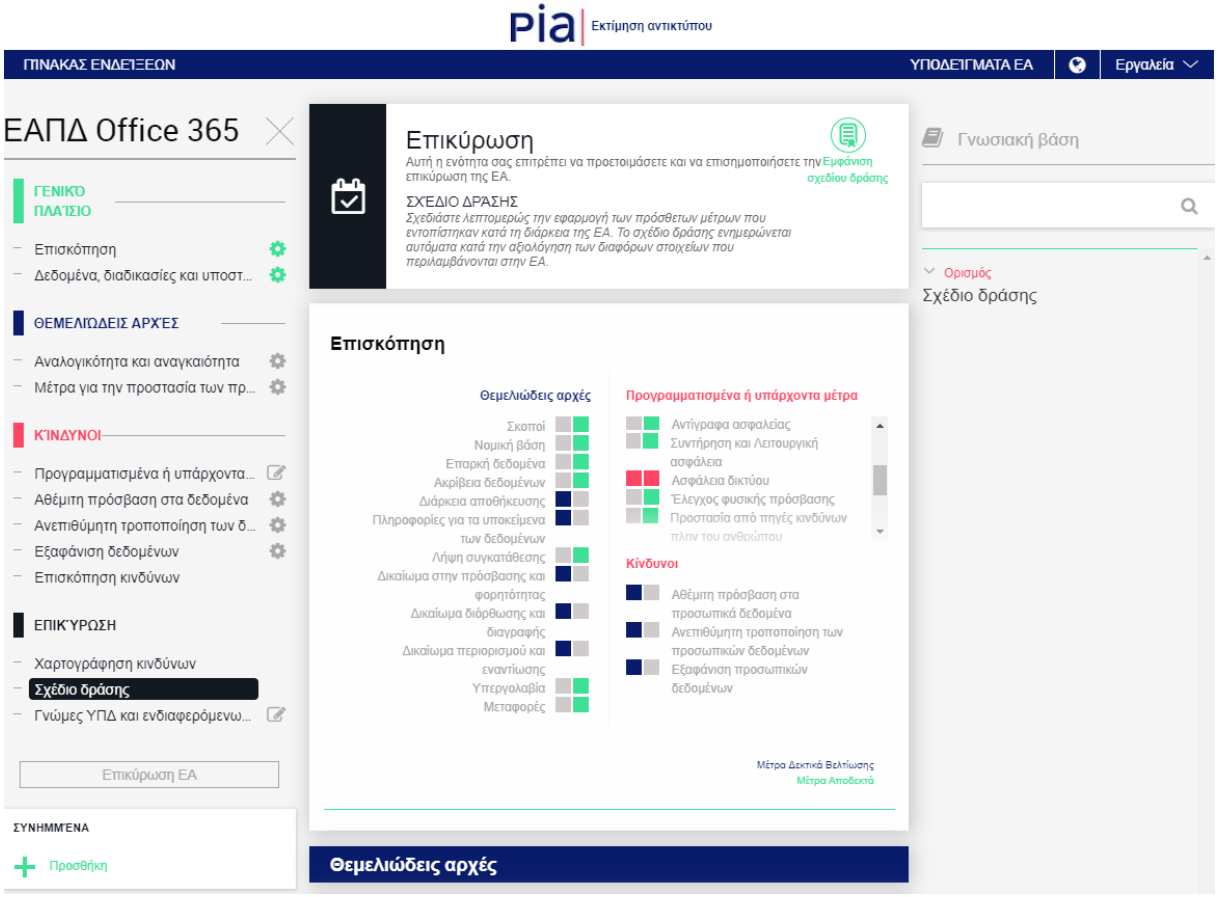
Στιγμιότυπο 10. Χαρτογράφηση κινδύνων.



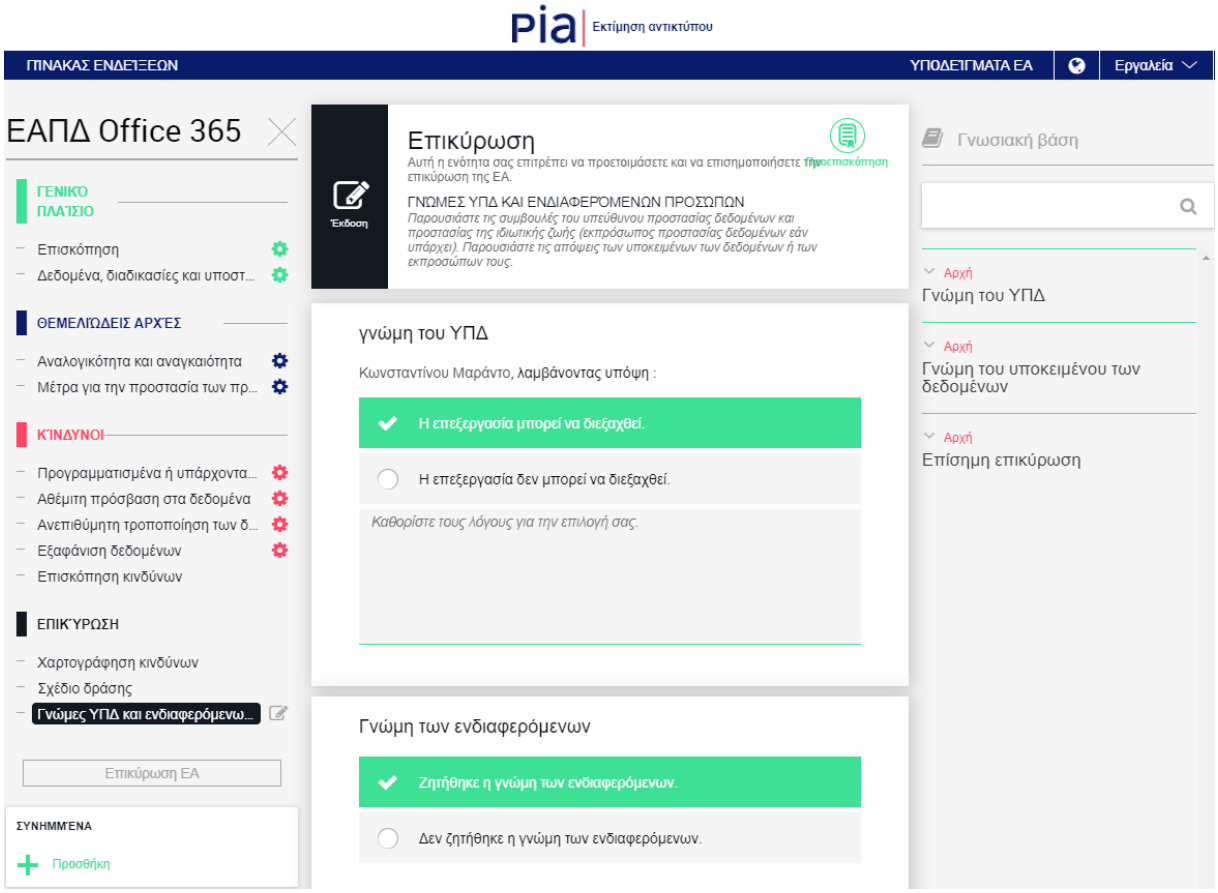
Στιγμιότυπο 11. Αίτημα αξιολόγησης ανάλυσης.



Στιγμιότυπο 12. Χαρτογράφηση κινδύνων μετά την εφαρμογή των βελτιωτικών μέτρων.



Στιγμιότυπο 13. Σχέδιο δράσης – Αξιολογημένα σημεία.



Στιγμιότυπο 14. Επικύρωση της ΕΑΠΔ.

Βιβλιογραφία

[1] European Union, '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 repeal- ing Directive 95/46/EC (General Data Protection Regulation)'.

[2] Enisa, 'Handbook on Security of Personal Data Processing'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing.

[3] CNIL, 'The open source PIA software helps to carry out data protection impact assesment | CNIL'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

[4] Merriam-Webster, 'Privacy | Definition of Privacy by Merriam-Webster'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.merriam-webster.com/dictionary/privacy.

[5] B. Schneier, 'A Revised Taxonomy of Social Networking Data - Schneier on Security'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.schneier.com/blog/archives/2010/08/a_taxonomy_of_s_1.html.

[6] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) - European Commission'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[7] European Commission, 'Guidelines on Data Protection Officers ('DPOs')'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. [Ημερομηνία πρόσβασης: 22-Νοεμβρίου-2019].

[8] Microsoft, 'End of support for Office 2010'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://support.office.com/en-us/article/end-of-support-for-office-2010-3a3e45de-51ac-4944-b2ba-c2e415432789.

[9] Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 'Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen', *Der Hessische Beauftragte für Datenschutz und Informationsfreiheit*. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und.

[10] Enisa, 'Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses)'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html.

[11] Information Commissioner's Office (ICO), 'How do we do a DPIA?', 23-Αυγούστου-2019. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://ico.org.uk/for-

organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/.