Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Εκτίμηση αντικτύπου ως προς την προστασία δεδομένων - Μελέτη περίπτωσης στο Δημόσιο Τομέα

Παναγιώτα Λεπίδα

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Νοέμβριος 2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Εκτίμηση αντικτύπου ως προς την προστασία δεδομένων - Μελέτη περίπτωσης στο Δημόσιο Τομέα

Παναγιώτα Λεπίδα

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 2021

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η παρούσα διπλωματική διατριβή διερευνά τους τρόπους διαχείρισης κινδύνων ασφαλείας στους φορείς της δημόσιας διοίκησης και προσανατολίζεται σε δύο κύριες κατευθύνσεις. Η πρώτη εστιάζει στην ανάδειξη όλων εκείνων του συνιστωσών που επηρεάζουν την ασφάλεια κατά την επεξεργασία προσωπικών δεδομένων σε ένα δημόσιο φορέα και στον τρόπο που διασφαλίζεται ότι η επεξεργασία είναι σύννομη ως προς το Γενικό Κανονισμό Προστασίας Δεδομένων. Η δεύτερη εστιάζει στον τρόπο υλοποίησης μιας ολοκληρωμένης εκτίμησης αντικτύπου των κινδύνων μιας επεξεργασίας προσωπικών δεδομένων και στις απαιτήσεις που πρέπει να έχει ο φορέας στην περίπτωση που επιλέγει ως εκτελών την επεξεργασία κάποιον εξωτερικό συνεργάτη. Μέσα από τη μελέτη εκτίμησης αντικτύπου προκύπτουν ερωτήματα που σχετίζονται με την ετοιμότητα ενός δημόσιου φορέα στην εκτέλεση επεξεργασίας προσωπικών δεδομένων μεγάλης κλίμακας, στα εχέγγυα που θα πρέπει να αναζητά σε περίπτωση συνεργασίας με εξωτερικό συνεργάτη και στον τρόπο που θα μπορεί να διασφαλίζει ανά πάσα στιγμή ότι η επεξεργασία των δεδομένων πραγματοποιείται με το μικρότερο δυνατό ρίσκο ως προς την πιθανότητα εμφάνισης κινδύνων. Τα αποτελέσματα της μελέτης οδηγούν σε κάποια ενδιαφέροντα συμπεράσματα ως προς τις απαιτήσεις σε θέματα ασφάλειας προσωπικών δεδομένων που επιβάλει ο ΓΚΠΔ και τις εγγυήσεις ως προς τη διαχείριση ασφάλειας των πληροφοριών που παρέχει το πρότυπο ασφάλειας δεδομένων ISO27001.

Για την ολοκλήρωση της διατριβής χρησιμοποιήθηκε ως οδηγός η μεθοδολογία διαχείρισης κινδύνων του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας ENISA, ενώ η μελέτη της εκτίμησης αντικτύπου πραγματοποιήθηκε με τη βοήθεια του λογισμικού PIA της Γαλλικής Αρχής Προστασίας Δεδομένων CNIL.

Summary

This thesis investigates the ways in which public organizations manage the security risks and is oriented in two fundamental areas. The first one focuses on highlighting the components affecting security while processing personal data and how to ensure that the procedure is lawful in terms of the General Data Protection Regulation. The second one focuses on how to implement a comprehensive Risk Impact Assessment while processing personal data and on the requirements that should be met in case of delegation to an external partner. Through the Privacy Impact Assessment study, different questions arise concerning the promptitude of a public organization to carry out large-scale operations of personal data processing, the conditions to be met while delegating to an external partner and how it can be ensured at all times that the data processing is carried out with the least possible risk. The results of the study lead to some interesting conclusions regarding the security requirements imposed by the GDPR and the guarantees provided by the ISO27001 data security standard. The risk management methodology used to complete the thesis, is the one proposed by the European Cybersecurity Agency ENISA , while the Privacy Impact Assessment study was carried out using the PIA software of the French Data Protection Authority CNIL.

Ευχαριστίες

Πρωτίστως, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Κωνσταντίνο Λιμνιώτη, για την πολύτιμη καθοδήγησή του και το χρόνο που μου αφιέρωσε κατά την εκπόνηση της παρούσας μεταπτυχιακής διατριβής.

Επίσης, οφείλω ένα μεγάλο ευχαριστώ στους φίλους, τους συναδέλφους και την οικογένειά μου για τη στήριξή τους.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Το πρώτο κεφάλαιο της παρούσας μεταπτυχιακής διατριβής, αποτελεί ένα εισαγωγικό κεφάλαιο στο οποίο θα παρουσιαστεί αρχικά το ερευνητικό ερώτημα που οδήγησε στη σύνταξη της διατριβής αυτής και στη συνέχεια, ο σκοπός, ο στόχος και η δομή της.

1.1 Εισαγωγή

Αδιαμφισβήτητο γεγονός είναι πως πλέον, στη σύγχρονη κοινωνία και το σύγχρονο τρόπο ζωής, σχεδόν το σύνολο των υπηρεσιών και των διαδικασιών βασίζονται στην επιστήμη της πληροφορίας και της τεχνολογίας. Τις τελευταίες δεκαετίες, η ραγδαία ανάπτυξη της τεχνολογίας και των ψηφιακών υπηρεσιών, έχει δημιουργήσει νέα δεδομένα στην ποιότητα ζωής, στην επιχειρηματικότητα, στις υπηρεσίες υγείας, στις μεταφορές και γενικά στους περισσότερους τομείς της καθημερινότητάς μας. Η βελτίωση στην ταχύτητα και την ποιότητα των παρεχόμενων υπηρεσιών γίνεται αντιληπτή καθημερινά, με την πλειοψηφία αυτών να μπορούν να ολοκληρωθούν μέσω ενός προσωπικού υπολογιστή ή μιας φορητής έξυπνης συσκευής. Ωστόσο, η συνεχής αύξηση του εύρους στο οποίο βρίσκει πλέον εφαρμογή η τεχνολογία της πληροφορίας και επικοινωνίας, έχει δημιουργήσει νέες υψηλότερες απαιτήσεις, σε τεχνολογικό εξοπλισμό, υπολογιστική ισχύ, αλλά και ασφάλεια. Η εκθετική αύξηση του όγκου της πληροφορίας που διακινείται και αποθηκεύεται προκειμένου να ολοκληρωθούν οι ηλεκτρονικές υπηρεσίες με αξιοπιστία, έχει προκαλέσει την απαίτηση για ασφαλή τεχνολογικά συστήματα, δίκτυα και υποδομές.

Οι δημόσιες υπηρεσίες και γενικά ο δημόσιος τομέας, δε θα μπορούσε να μείνει μακριά από την τεχνολογική αυτή εξέλιξη. Στο σύνολό της η δημόσια διοίκηση, στο πλαίσιο της ψηφιακής διακυβέρνησης και της μετάβασής της στη σύγχρονη ψηφιακή εποχή, διεκπεραιώνει πλέον όλο και περισσότερες διαδικασίες και συναλλαγές της, μέσω

ηλεκτρονικών υπηρεσιών. Το γεγονός αυτό έχει σαν αποτέλεσμα, αφενός μεν τη συνεχή αύξηση του αγαθού της πληροφορίας και αφετέρου την απαίτηση η πληροφορία αυτή να προστατευθεί με τον καλύτερο και ασφαλέστερο δυνατό τρόπο. Η πληροφορία πρέπει να προστατεύεται, διότι έχει αξία για το φορέα που την κατέχει όταν είναι έγκυρη, και σαν αγαθό που διακινείται και διαμοιράζεται κινδυνεύει να αλλοιωθεί και να χάσει την εγκυρότητά της άρα και την αξία της.

Μεταξύ των πληροφοριών που υφίστανται επεξεργασία είναι και τα προσωπικά δεδομένα, δηλαδή δεδομένα που αφορούν φυσικά πρόσωπα. Η προστασία τους αποτελεί θεμελιώδες ανθρώπινο δικαίωμα και είναι στενά συνυφασμένη με την έννοια της ιδιωτικότητας, αφού προσβολή στο δικαίωμα της προστασίας προσωπικών δεδομένων μπορεί να έχει σημαντικές επιπτώσεις στον πυρήνα της ιδιωτικής ζωής του ατόμου. Ακριβώς για αυτό, υπάρχει ένα αυστηρό νομικό πλαίσιο αναφορικά με την προστασία των προσωπικών δεδομένων: στην Ευρώπη είναι σε ισχύ, από το 2018, ο Γενικός Κανονισμός Προστασίας Δεδομένων, με σύνολο υποχρεώσεων για όσους επεξεργάζονται προσωπικά δεδομένα, αλλά και σύνολο δικαιωμάτων για όλους όσους τα προσωπικά τους δεδομένα υφίστανται επεξεργασία. Ο Γενικός Κανονισμός αποτέλεσε μία σημαντική τομή, αφού πληθώρα οργανισμών επένδυσε σε ενέργειες συμμόρφωσης με τις συναφείς υποχρεώσεις που απορρέουν από αυτόν. Παρόλα αυτά, πολλές εξ αυτών αποτελούν «προκλήσεις» - ιδιαίτερα δε για το Δημόσιο Τομέα, όπου συχνά δεν είναι εύκολο να δαπανηθούν οι αναγκαίοι πόροι, ενώ ταυτόχρονα το διακύβευμα από τη μη προστασία δεδομένων πολιτών είναι μεγάλο.

1.2 Ερευνητικό πρόβλημα

Ο Δημόσιος Τομέας (υπουργεία, δημόσιες υπηρεσίες, ΝΠΔΔ, ΟΤΑ, ανεξάρτητες Αρχές, κλπ.) διαχειρίζεται καθημερινά έναν πολύ μεγάλο όγκο πληροφορίας - προσωπικά δεδομένα, που αφορούν αφενός μεν τους πολίτες με τους οποίους πραγματοποιεί συναλλαγές και αφετέρου, τους υπαλλήλους που απασχολούνται σε αυτόν. Οι περισσότεροι από τους οργανισμούς του δημόσιου φορέα, εξαρτώνται σε πολύ μεγάλο βαθμό από την τεχνολογία της πληροφορικής, καθώς η αποθήκευση και επεξεργασία των δεδομένων στην πλειοψηφία τους γίνεται ηλεκτρονικά. Η διαχείριση των δεδομένων αυτών, πολλές φορές πραγματοποιείται με συνεργασία τρίτων (εξωτερικοί συνεργάτες),

οι οποίοι προσφέρουν στους φορείς τα κατάλληλα εργαλεία επεξεργασίας (λογισμικό, εφαρμογές και εξειδικευμένες υπηρεσίες).

Καθώς λοιπόν η ισχύουσα νομοθεσία επιβάλει στους δημόσιους φορείς να εξασφαλίζουν με κάθε τρόπο την προστασία των προσωπικών δεδομένων των πολιτών και του προσωπικού τους, κρίνεται απαραίτητο να μελετηθούν:

- αφενός μεν οι προϋποθέσεις που απαιτείται να πληροί ένας δημόσιος φορέας για να θεωρείται σύννομος ως προς την επεξεργασία των προσωπικών δεδομένων
- και αφετέρου, οι τρόποι και οι ενέργειες με τους οποίους μπορεί να εγγυηθεί την ακεραιότητα της επεξεργασίας, όταν αυτή εκτελείται αντ' αυτού εκ μέρους τρίτων

Οι παραπάνω προϋποθέσεις και ενέργειες, σχετίζονται τόσο με τις Πολιτικές Ασφάλειας των Πληροφοριών, όσο και με τη δυνατότητα του να εξασφαλίζεται ανά πάσα στιγμή η προσβασιμότητα, η εμπιστευτικότητα και η ακεραιότητα στα δεδομένα που επεξεργάζονται.

1.3 Σκοπός και Στόχος της διατριβής

Σύμφωνα με όσα αναφέρθηκαν προηγουμένως, για έναν δημόσιο οργανισμό ο οποίος συλλέγει, επεξεργάζεται, χρησιμοποιεί και διακινεί πληροφορίες και προσωπικά δεδομένα, είναι αναγκαία συνθήκη η Ασφάλεια και η Προστασία τους, προκειμένου να λειτουργεί απρόσκοπτα στο σύνολο των δραστηριοτήτων του.

Ο σκοπός της παρούσας μεταπτυχιακής διατριβής κινείται σε δύο άξονες. Ο πρώτος άξονας είναι να αναδειχθούν όλες οι συνιστώσες που επηρεάζουν την επεξεργασία των προσωπικών δεδομένων σε έναν δημόσιο φορέα και ο δεύτερος να γίνει μια πλήρη και ολοκληρωμένη εκτίμηση αντικτύπου ως προς την προστασία προσωπικών δεδομένων για τις περιπτώσεις όπου η επεξεργασία των δεδομένων πραγματοποιείται εκτός του φορέα μέσω συνεργατών. Η εκτίμηση αντικτύπου, για την οποία θα μπορούσε να ειπωθεί ότι αποτελεί γενίκευση μίας διαχείρισης κινδύνων ασφάλειας για τα προσωπικά δεδομένα, αποτελεί – εφόσον συντρέχουν συγκεκριμένες προϋποθέσεις - μία εκ των υποχρεώσεων που απορρέουν από το Γενικό Κανονισμό Προστασίας Δεδομένων.

Στόχος επομένως της μεταπτυχιακής διατριβής είναι να αποτελέσει έναν οδηγό για τη σωστή εφαρμογή των κανόνων που η Ευρωπαϊκή και Ελληνική νομοθεσία επιβάλλει ως προς την επεξεργασία των προσωπικών δεδομένων από έναν Δημόσιο Φορέα και να καταγραφούν όλες οι παράμετροι και τα κριτήρια που θα πρέπει να λαμβάνονται υπόψη από το σύνολο των ατόμων του φορέα που εμπλέκονται άμεσα με την επεξεργασία αυτή και πρέπει να επιλέξουν έναν εξωτερικό συνεργάτη με εχέγγυα για να την εκτελέσει. Ιδιαίτερα δε, η παρούσα διατριβή καταδεικνύει τα βήματα μίας ορθά εκπονηθείσας εκτίμησης αντικτύπου, για ένα ρεαλιστικό σενάριο κρίσιμης επεξεργασίας προσωπικών δεδομένων, για την οποία λαμβάνεται απόφαση να ανατεθεί σε εξωτερική συνεργαζόμενη εταιρεία.

1.4 Μεθοδολογία

Για την εκπόνηση της εκτίμησης αντικτύπου που καταγράφεται στα κεφάλαια 3 και 4 της παρούσας μεταπτυχιακής διατριβής, ακολουθήθηκε η εξής μεθοδολογία. Αρχικά, πραγματοποιήθηκε μια πρώτη ανάλυση κινδύνων του σεναρίου που επιλέχθηκε, σύμφωνα με τον οδηγό ENISA (ENISA n.d.), προκειμένου να αναδειχθούν κάποια μεγάλα θέματα ασφάλειας, τα οποία δεν ήταν δυνατόν να ξεπεραστούν άμεσα προκειμένου να ολοκληρωθεί η επεξεργασία με το αρχικό πλάνο. Στη συνέχεια, εκπονήθηκε μια δεύτερη ανάλυση κινδύνων, με την ίδια μεθοδολογία, αλλά σε άλλο περιβάλλον όπου οι κίνδυνοι περιορίστηκαν και η εκτέλεση της επεξεργασίας μπορούσε να ξεκινήσει άμεσα. Στη συνέχεια, καθώς το σενάριο απαιτεί διενέργεια ΕΑΠΔ, πραγματοποιείται με τη βοήθεια του ανοικτού λογισμικού PIA της Γαλλικής αρχής Προστασίας Δεδομένων (CNIL n.d.), η εκτίμηση αντικτύπου για τη συγκεκριμένη επεξεργασία. Στους κινδύνους που καταγράφονται κατά την εκτέλεση της ΕΑΠΔ, προτείνονται βελτιωτικά μέτρα, τα οποία χρησιμοποιούνται στο ίδιο λογισμικό, προκειμένου να αποτυπωθεί και χαρτογραφικά, το πως θα περιοριστεί μέσω των μέτρων η πιθανότητα εμφάνισης των κινδύνων.

1.5 Δομή της Εργασίας

Στο 2ο Κεφάλαιο της παρούσας μεταπτυχιακής διατριβής, θα παρουσιαστεί εν συντομία ο Γενικός Κανονισμός για την Προστασία των Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR 2016/679), οι αλλαγές που επιφέρει ως προς την επεξεργασία των δεδομένων, με

έμφαση στη Δημόσια Διοίκηση, ενώ στη συνέχεια θα γίνει αναφορά στο νόμο Ν.4624/2019 που καθορίζει τα μέτρα εφαρμογής του Κανονισμού και ενσωματώνει την Οδηγία 2016/680 της ΕΕ στην εθνική νομοθεσία.

Το 3ο Κεφάλαιο αποτελείται από τρεις βασικές ενότητες. Στο πρώτο μέρος αρχικά, θα παρουσιαστεί το σενάριο το οποίο θα αφορά η μελέτη περίπτωσης. Στη δεύτερη ενότητα θα παρουσιαστούν οι πιο σημαντικές παράμετροι που θα παίξουν καθοριστικό ρόλο στον τρόπο στον τρόπο με τον οποίο θα πραγματοποιηθεί η επεξεργασία. Η τρίτη κα τελευταία ενότητα, θα περιέχει την αξιολόγηση κινδύνων του σεναρίου που επιλέχθηκε. Μέσα από μια πρώτη αξιολόγηση κινδύνων για την εκτέλεση της επεξεργασίας, θα προκύψουν προβληματισμοί και εμπόδια που θα καταστήσουν απαγορευτική την εκτέλεση της επεξεργασίας από τον ίδιο τον οργανισμό, οπότε ο υπεύθυνος επεξεργασίας θα προσανατολιστεί στην εύρεση συνεργάτη με εχέγγυα για να τη διεκπεραιώσει. Για την περίπτωση αυτή θα πραγματοποιηθεί δεύτερη εκτενέστερη μελέτη αξιολόγησης κινδύνων, που θα αποτελέσει και τη βάση για τη διενέργεια της μελέτης εκτίμησης αντικτύπου που θα παρουσιαστεί στο 4ο Κεφάλαιο. Η μελέτη αυτή θα ολοκληρωθεί με τη βοήθεια του λογισμικού PIA της γαλλικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (CNIL). Στο τέλος του 4ου Κεφαλαίου θα καταγραφεί η πρόταση βελτιωτικών μέτρων για την αντιμετώπιση των κινδύνων και με τη βοήθεια του ίδιου λογισμικού θα εξαχθούν συμπεράσματα για την αποτελεσματικότητά τους.

Στο 5ο και τελευταίο, που θα αποτελέσει τον επίλογο της εργασίας, θα παρουσιαστούν τα συμπεράσματα της Εκτίμησης Αντικτύπου που πραγματοποιήθηκε και θα αναλυθούν τα προσδοκόμενα αποτελέσματα της εφαρμογής των βελτιωτικών μέτρων που προτάθηκαν.

Κεφάλαιο 2
Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ)

Στο κεφάλαιο αυτό, θα γίνει μια παρουσίαση του πλαισίου προστασίας και αξιοποίησης των προσωπικών δεδομένων στην Δημόσια Διοίκηση σε σχέση με τον Γενικό Κανονισμό Προστασίας Δεδομένων. Επίσης, θα γίνει αναφορά, στις καινοτομίες που εισάγονται αλλά και στο ρόλο του υπεύθυνου επεξεργασίας δεδομένων στο δημόσιο τομέα.

2.1 Σύγχρονη ευρωπαϊκή νομοθεσία για τα προσωπικά δεδομένα

Στις 28 Ιανουαρίου 1981, το Συμβούλιο της Ευρώπης υπέγραψε τη Σύμβαση 108, κάνοντας την καθοριστική αρχή για την προστασία των προσωπικών δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης, καθώς η Σύμβαση αυτή αποτέλεσε την πρώτη νομικά δεσμευτική διεθνή πράξη που θεσπίστηκε στον τομέα της προστασίας των δεδομένων. Σκοπός της Σύμβασης 108 ήταν «η διασφάλιση για κάθε φυσικό πρόσωπο, του σεβασμού των δικαιωμάτων του και των θεμελιωδών ελευθεριών του, και ιδίως του δικαιώματός του στην ιδιωτική ζωή, έναντι της αυτοματοποιημένης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα» (Maciejewski 2021).

Στις 24 Οκτωβρίου 1995, εκδίδεται από το Ευρωπαϊκό Κοινοβούλιο η μέχρι πρόσφατα ισχύουσα «Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών» (European Parliament, Οδηγία για την προστασία δεδομένων

προσωπικού χαρακτήρα, ΕΕ 1995 L 281, σ. 31. 1995). Η Οδηγία 95/46/ΕΚ, αποσκοπούσε στην υλοποίηση και τη διεύρυνση των αρχών που διείπαν το δικαίωμα στην ιδιωτική ζωή και διατυπώνονταν ήδη στη Σύμβαση 108 (European Parliament και Fundamental Rights/Council of Europe, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων 2014).

Τον Απρίλιο του 2016 το Ευρωπαϊκό Κοινοβούλιο υπερψηφίζει το νέο Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ), ο οποίος στο άρθρο 94 καταργεί την Οδηγία 95/46/ΕΚ, εκσυγχρονίζοντας με τον τρόπο αυτό τη νομοθεσία της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων. Ο Κανονισμός αφορά στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και στην ελεύθερη κυκλοφορία των δεδομένων αυτών. Στο Άρθρο 51 του κανονισμού αναφέρεται ρητά πως κάθε κράτος μέλος της ΕΕ, καλείται να θεσπίσει σχετικές διατάξεις στο δίκαιό του, τις οποίες και πρέπει να κοινοποιήσει στην Επιτροπή το αργότερο μέχρι την 25η Μαΐου του 2018 (Άρθ.51 παρ. 4), ημερομηνία κατά την οποία τίθεται σε πλήρη εφαρμογή ο Κανονισμός. Βάσει αυτού του κανονισμού, κάθε επιχείρηση ή φορέας ιδιωτικός ή δημόσιος, που εδρεύει εντός ή εκτός της Ευρωπαϊκής Ένωσης και επεξεργάζεται προσωπικά δεδομένα που αφορούν σε άτομα που βρίσκονται εντός Ευρωπαϊκής Ένωσης ήταν υποχρεωμένη να συμμορφωθεί πλήρως με το νέο ΓΚΠΔ μέχρι την 25η Μαΐου του 2018.

Ως προς την ελληνική νομοθεσία, με αρκετή καθυστέρηση και μόλις στις 26 Αυγούστου του 2019, ψηφίζεται με τη διαδικασία του κατεπείγοντος ο Ν.4624/2019 περί «Προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα», θεσπίζοντας τα μέτρα εφαρμογής του ΓΚΠΔ.

2.2 Προστασία της Ιδιωτικότητας και των Προσωπικών Δεδομένων

Στο άρθρο 4 του ΓΚΠΔ, περιγράφεται αναλυτικά η πιο σημαντική έννοια που διαπραγματεύεται, αυτή των «δεδομένων προσωπικού χαρακτήρα». Σύμφωνα με τον ορισμό του Κανονισμού, ως "Δεδομένο προσωπικού χαρακτήρα» νοείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο

(«υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου" (European Parliament 2016)

Τέτοια δεδομένα μπορεί να είναι: ο αριθμός φορολογικού μητρώου, η ταχυδρομική διεύθυνση, ο αριθμός ταυτότητας κλπ. Στο σύγχρονο όμως κόσμο της τεχνολογίας και του διαδικτύου, η έννοια των προσωπικών δεδομένων φαίνεται να διευρύνεται αν αναλογιστεί κανείς το πλήθος των στοιχείων που συλλέγεται από κάθε ηλεκτρονική υπηρεσία προκειμένου αυτή να διεκπεραιωθεί ή τον τρόπο με τον οποίο τα ηλεκτρονικά ίχνη ενός χρήστη μπορούν να οδηγήσουν έπειτα από ειδική επεξεργασία στην ταυτοποίησή του. Όλα τα παραπάνω οδηγούν στο συμπέρασμα πως η ιδιωτικότητα των ατόμων η οποία είναι συνυφασμένη με το δικαίωμα στη μυστικότητα και την απομόνωση (on line dictionary Merriam-webster n.d.) φαίνεται να απειλείται και η σημασία της προστασίας των δεδομένων αυτών γίνεται επιτακτική, καθώς ο όγκος των δεδομένων που δημιουργούνται και αποθηκεύονται καθημερινά, εξακολουθεί να αυξάνεται με πρωτοφανείς ρυθμούς.

Ο ΓΚΠΔ ήρθε να προστατέψει το δικαίωμα της ιδιωτικότητας των πολιτών της Ευρωπαϊκής Ένωσης και να θεσπίσει κανόνες και προϋποθέσεις για την επεξεργασία και διακίνησή των δεδομένων που τους αφορούν, βάζοντας ακόμα μεγαλύτερους περιορισμούς στην επεξεργασία τους.

2.3 Βασικοί Ορισμοί και Αρχές του ΓΚΠΔ

Για το σκοπό του Κανονισμού, εισήχθησαν και περιεγράφηκαν στο Άρθρο 4 αρκετοί ορισμοί, συμπεριλαμβανομένων και αυτών του «Υποκειμένου των Δεδομένων» και των «Δεδομένων Προσωπικού Χαρακτήρα» (όπως αυτοί αναφέρθηκαν στην παράγραφο 2.2). Οι πιο σημαντικοί όροι, τους οποίους πραγματεύεται και οι οποίοι θα χρησιμοποιηθούν εκτενώς στην παρούσα μεταπτυχιακή διατριβή, είναι οι παρακάτω:

- **Υποκείμενο των δεδομένων:** το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου (European Parliament 2016)
- **Δεδομένα προσωπικού χαρακτήρα:** κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων) (European Parliament 2016)
- **Επεξεργασία:** κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή (European Parliament 2016)
- **Ψευδωνυμοποίηση των δεδομένων:** η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (European Parliament 2016)
- **Υπεύθυνος επεξεργασίας:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους (European Parliament 2016)

- **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 (European Parliament 2016)
- **Τρίτος:** οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα (European Parliament 2016)

Επιπλέον, στο άρθρο 5 του Κανονισμού, περιγράφονται με σαφήνεια, οι αρχές που πρέπει να διέπουν την επεξεργασία των προσωπικών δεδομένων και οι οποίες συνοψίζονται ως εξής:

1. Αρχή της Νομιμότητας: τα δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων ("νομιμότητα, αντικειμενικότητα και διαφάνεια")
2. Αρχή του Περιορισμού του Σκοπού: τα δεδομένα χρησιμοποιούνται μόνο για το σκοπό τον οποίο συλλέχθηκαν και δεν υποβάλλονται σε περαιτέρω επεξεργασία (η πλέον του σκοπού συλλογής επεξεργασία είναι αποδεκτή μόνο για σκοπούς αρχειοθέτησης που έχουν ως στόχο την εξυπηρέτηση του δημόσιου συμφέροντος)
3. Αρχή της Ελαχιστοποίησης των Δεδομένων: τα δεδομένα που συλλέγονται πρέπει να είναι τα απολύτως απαραίτητα για τους σκοπούς της επεξεργασίας
4. Αρχή της Ακρίβειας: τα δεδομένα θα πρέπει να είναι πάντα ακριβή και όταν χρειάζεται αν επικαιροποιούνται. Επιπλέον, πρέπει να λαμβάνονται όλα τα μέτρα για την άμεση διόρθωση ή και διαγραφή τους όταν εντοπιστεί ότι υπάρχει ανακρίβεια σε αυτά
5. Αρχή του Περιορισμού της Περιόδου Αποθήκευσης: η διάρκεια τήρησης των δεδομένων, θα πρέπει να περιορίζεται μόνο στο διάστημα για το οποίο απαιτείται έως την επίτευξη του σκοπού της επεξεργασίας (εξαίρεση αποτελούν οι περιπτώσεις συλλογής τους για στατιστικούς σκοπούς ή σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, καθώς επίσης και για σκοπούς ιστορικής ή επιστημονικής έρευνας)

6. Αρχή της Ακεραιότητας και Εμπιστευτικότητας: σύμφωνα με την αρχή αυτή, η επεξεργασία των δεδομένων θα πρέπει να διενεργείται με τρόπο τέτοιο που θα εγγυάται την ασφάλειά τους, δηλαδή την προστασία από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, καταστροφή, απώλεια ή φθορά
7. Αρχή της Λογοδοσίας: η αρχή της Λογοδοσίας περιγράφει την υποχρέωση του Υπεύθυνου επεξεργασίας να μπορεί να αποδείξει ανά πάσα στιγμή τη συμμόρφωση της επεξεργασίας ως προς τις παραπάνω αρχές που διέπουν τον Κανονισμό

Ένα πολύ βασικό κομμάτι της επεξεργασίας είναι και νομιμοποιητική της βάση. Το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ, προβλέπει τη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο βαθμό που «η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης». (European Data Protection Board 2019)

Ειδική αναφορά θα πρέπει να γίνει και στο Άρθρο 9 του Κανονισμού, στο οποίο εισάγεται η έννοια των προσωπικών δεδομένων “ειδικών κατηγοριών” (Ευαίσθητα Προσωπικά Δεδομένα). Στις κατηγορίες αυτές, ανήκουν δεδομένα που “αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό” (PRIVAZYPLAN gets your data protection on course n.d.) και για τις περιπτώσεις αυτές, απαγορεύεται ρητά η επεξεργασίας τους, εκτός από πολύ συγκεκριμένων εξαιρέσεων και υπό πολύ αυστηρές προϋποθέσεις.

2.4 Τα Δικαιώματα του Υποκειμένου των Δεδομένων

- ✓ ***Το δικαίωμα της ενημέρωσης (Άρθρα 12, 13 & 14):*** το Υποκείμενο των δεδομένων, έχει το δικαίωμα να ενημερώνεται με σαφήνεια και ακρίβεια για την

συλλογή και επεξεργασία των δεδομένων που το αφορούν. Η ενημέρωσή του πρέπει να παρέχεται δωρεάν και να είναι «συνοπτική, σαφής, διαφανή, κατανοητή και εύκολα προσβάσιμη» (Άρθρο 12). Επιπλέον, πρέπει να περιλαμβάνει πληροφορίες σχετικά με το σκοπό της επεξεργασίας, τις πηγές άντλησης και τις κατηγορίες των δεδομένων, καθώς και τους πιθανούς αποδέκτες της

- ✓ ***Το δικαίωμα πρόσβασης (Άρθρο 15):*** το Υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει γνώση για τα δεδομένα που επεξεργάζονται και να ζητήσει πρόσβαση σε αυτά
- ✓ ***Το δικαίωμα διόρθωσης (Άρθρο 16):*** το Υποκείμενο των δεδομένων έχει το δικαίωμα να «συμπληρώσει» ή να «διορθώσει» τα δεδομένα που το αφορούν, αν αντιληφθεί ότι είναι ελλιπή ή ανακριβή
- ✓ ***Το «δικαίωμα στη λήθη» (Άρθρο 17):*** το Υποκείμενο των δεδομένων, έχει το δικαίωμα να ζητήσει τη διαγραφή των δεδομένων που το αφορούν, υπό συγκεκριμένες προϋποθέσεις, όπως:
  - στην περίπτωση που τα δεδομένα έχουν υποβληθεί σε παράνομη επεξεργασία
  - όταν τα αυτά δεν είναι πλέον απαραίτητα ως προς το σκοπό για τον οποίο συλλέχθηκαν
  - όταν το Υποκείμενο ανακαλεί τη συγκατάθεσή του και δεν υφίστανται άλλη νομική βάση για επεξεργασία
- ✓ ***Το δικαίωμα στον περιορισμό της επεξεργασίας (Άρθρο 18):*** το Υποκείμενο των δεδομένων, έχει το δικαίωμα να ζητήσει τον περιορισμό της επεξεργασίας όταν:
  - τα δεδομένα έχουν υποβληθεί σε παράνομη επεξεργασία
  - αμφισβητεί την ακρίβειά τους
  - τα δεδομένα δε χρειάζονται πλέον για το σκοπό της επεξεργασίας
  - εκφράζει αντίρρηση στην επεξεργασία
- ✓ ***Το δικαίωμα στην φορητότητα (Άρθρο 20):*** το Υποκείμενο έχει το δικαίωμα, υπό συγκεκριμένες προϋποθέσεις, να αιτηθεί τη μεταφορά των δεδομένων του σε άλλον Υπεύθυνο επεξεργασίας ή να λάβει τα δεδομένα του σε συγκεκριμένη μορφή

- ✓ ***Το δικαίωμα αντίρρησης (Άρθρο 21):*** σε περίπτωση που δε θίγεται το δημόσιο συμφέρον και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, το Υποκείμενο έχει το δικαίωμα εναντίωσης στην επεξεργασία των δεδομένων του
- ✓ ***Το δικαίωμα αντίρρησης σε αποφάσεις που βασίζονται σε αυτοματοποιημένες διαδικασίες, συμπεριλαμβανομένης της κατάρτισης προφίλ (Άρθρο 22):*** το Υποκείμενο έχει επίσης το δικαίωμα να εναντιωθεί σε αποφάσεις που λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας που παράγει έννομα αποτελέσματα που το αφορούν

Τα ανωτέρω δικαιώματα μπορούν να υπόκεινται σε περιορισμούς υπό προϋποθέσεις – μία εκ των οποίων είναι ο περιορισμός να προβλέπεται ρητά σε νόμο (ο οποίος νόμος όμως θα πρέπει να σέβεται την ουσία του δικαιώματος της προστασίας των δεδομένων).

2.5 Τεχνολογικές λύσεις για την προστασία δεδομένων

Οι κανόνες που εισήγαγε ο ΓΚΠΔ έχουν εφαρμογή σε κάθε τύπου επεξεργασίας δεδομένων, ανεξάρτητα αν αυτή υλοποιείται μέσω τεχνολογικών εργαλείων ή όχι. Και στις δύο περιπτώσεις και προς διασφάλιση της συμμόρφωσης προς τον Κανονισμό, ο υπεύθυνος επεξεργασίας πρέπει να ακολουθεί πολιτικές και να εφαρμόζει κατάλληλα μέτρα που ανταποκρίνονται στις αρχές προστασίας των δεδομένων από το σχεδιασμό και εξ ορισμού (Data protection by design and by default) (Άρθρο 25 ΓΚΠΔ).

Στη σύγχρονη τεχνολογικά εποχή, η παραπάνω απαίτηση έχει άμεσο αντίκτυπο στην ανάπτυξη λύσεων λογισμικού και υλικού, καθώς τα μέτρα προστασίας πρέπει να τα εφαρμόζουν από τα πρώτα στάδια της επεξεργασίας και όχι στο τελευταίο βήμα της επεξεργασίας και κατά την κρίση τους, όπως είχαν τη δυνατότητα μέχρι και πριν την εφαρμογή του Κανονισμού (Προστασία δεδομένων από το σχεδιασμό)

Επιπλέον, ο υπεύθυνος επεξεργασίας επιβάλλεται πλέον εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας (Προστασία δεδομένων εξ ορισμού)

Τρεις από τις νέες τεχνικές λύσεις που εισάγει γι' αυτό το σκοπό ο ΓΚΠΔ, είναι οι τεχνικές της Ψευδωνυμοποίησης, της Ανωνυμοποίησης και της Κρυπτογράφησης.

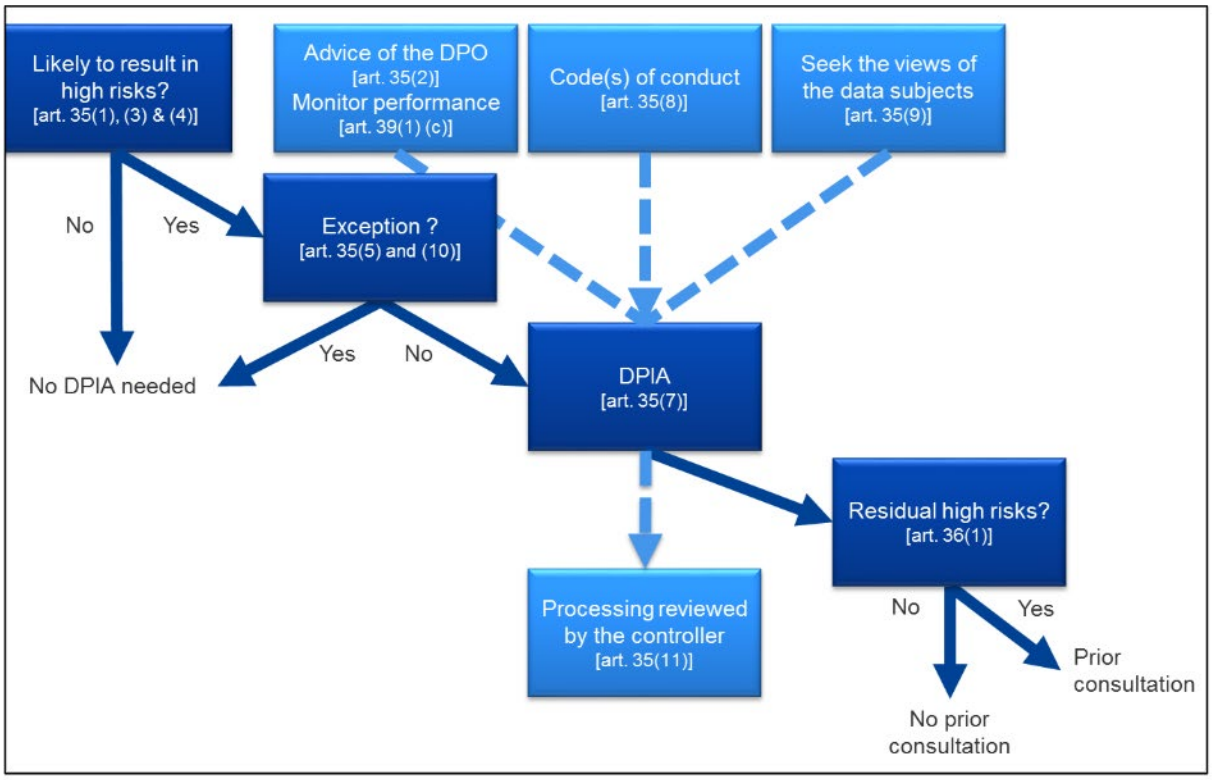
- ✓ **Ψευδωνυμοποίηση:** η διαδικασία αντικατάστασης της ταυτότητας του υποκειμένου των δεδομένων με τέτοιο τρόπο, ώστε να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώριση του υποκειμένου των δεδομένων (Δρ. Λουκάς 2017). Θα πρέπει ωστόσο να σημειωθεί ότι η επίτευξη της ανωνυμοποίησης δεν είναι πάντα μία εύκολη διαδικασία: ακόμα και η απαλοιφή αναγνωριστικών μπορεί να μην επαρκεί προκειμένου να επιτευχθεί ανωνυμοποίηση.
- ✓ **Ανωνυμοποίηση:** η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην είναι πλέον εφικτό τα ανωνυμοποιημένα δεδομένα να συσχετιστούν με το υποκείμενο των δεδομένων (Δρ. Λουκάς 2017)
- ✓ **Κρυπτογράφηση:** η διαδικασία κατά την οποία η αρχική πληροφορία «κείμενο» αναπαρίσταται σε μια εναλλακτική μορφή «κρυπτοκείμενο» το οποίο δεν είναι από μόνο του κατανοητό σε τρίτους

Και οι τρεις αυτές τεχνικές μπορούν να χρησιμοποιηθούν κατά το σχεδιασμό της επεξεργασίας, προκειμένου να δώσουν λύση στην προστασία της Ιδιωτικότητας τόσο κατά το σχεδιασμό, όσο και κατά την επεξεργασία.

2.6 Εκτίμηση Αντικτύπου και ο ρόλος του Υπεύθυνου Επεξεργασίας σε αυτή

Ένα από τα βασικά καθήκοντα του Υπεύθυνου Επεξεργασίας, όπως αυτά καταγράφονται στο Άρθρο 35 του κανονισμού, είναι και αυτό της "διενέργειας εκτίμησης του αντικτύπου των σχεδιαζόμενων πράξεων επεξεργασίας, όταν αυτές ενδέχεται να επιφέρουν υψηλό κίνδυνο ως προς τα δικαιώματα των υποκειμένων και την ασφάλεια των πληροφοριών (ΕΑΠΔ – Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων). Η Εκτίμηση Αντικτύπου διενεργείται πριν από την πράξη της επεξεργασίας και έχει ως στόχο τον εντοπισμό των κινδύνων των δεδομένων και την εύρεση κατάλληλων μέτρων περιορισμού των αντικτύπων στα δικαιώματα των υποκειμένων, ενώ παράλληλα αποτελεί σημαντικό εργαλείο για την εκπλήρωση της υποχρέωσης της λογοδοσίας.

Επομένως η Εκτίμηση Αντικτύπου αποτελεί ναι μεν μια "διαδικασία εμπέδωσης και απόδειξης συμμόρφωσης" του Φορέα που τη διενεργεί, ως προς τον Κανονισμό (Ομάδα Εργασίας του Άρθ.29 για την προστασία των Δεδομένων 2017) αλλά δε μπορεί να εξαλείψει την πιθανότητα εμφάνισης κινδύνου.



Εικόνα 1: Βασικές αρχές της ΕΑΠΔ κατά τον ΓΚΠΔ (Ομάδα Εργασίας του Άρθ.29 για την προστασία των Δεδομένων 2017)

Μια ΕΑΠΔ μπορεί να αφορά είτε απλά σε μια επιμέρους πράξη επεξεργασίας δεδομένων, είτε ακόμα και στην αξιολόγηση περισσότερων της μίας *παρόμοιων* πράξεων επεξεργασίας. Στην παράγραφο 3 του άρθρου 35 του ΓΚΠΔ, περιγράφονται οι περιπτώσεις όπου κρίνεται απαραίτητη η διενέργεια ΕΑΠΔ, και είναι οι εξής:

α. *"Περίπτωση συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο"*

β. *"Περίπτωση μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10"*

γ. *"Περίπτωση συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα"*

Η αναγκαιότητα στη διενέργεια ΕΑΠΔ, δεν περιορίζεται μόνο στις παραπάνω περιπτώσεις, αλλά πρέπει να λαμβάνει χώρα σε όσες περιπτώσεις επεξεργασίας ενέχεται να εμπεριέχουν υψηλό κίνδυνο ως προς την προστασία των προσωπικών δεδομένων, όπως και ρητά αναφέρεται στην παράγραφο 1 του άρθρου 35 του Κανονισμού.

2.7 Προσωπικά δεδομένα στη Δημόσια Διοίκηση

Ο Ν.4624/2019 εντάσσει στο πεδίο εφαρμογής του με τα Άρθρα 2 και 3, το σύνολο των δημόσιων φορέων, με τις διατάξεις του να εφαρμόζονται στην «*εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων Προσωπικού Χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης*» των φορέων αυτών. (Ν.4624/ 2019)

Επομένως, όλοι οι φορείς της Δημόσιας Διοίκησης, εμπίπτουν στις απαιτήσεις του ΓΚΠΔ, καθώς επεξεργάζονται μεγάλο όγκο δεδομένων προσωπικού χαρακτήρα, που προέρχονται είτε από το σύνολο των πολιτών με τους οποίους συναλλάσσονται, είτε από το προσωπικό το οποίο απασχολούν. Για το λόγο αυτό, κάθε δημόσια υπηρεσία οφείλει να είναι συμμορφωμένη με τις βασικές αρχές για τα προσωπικά δεδομένα, όπως αυτές περιγράφονται στο Άρθρο 5 του ΓΚΠΔ και αναφέρθηκαν προηγουμένως στην ενότητα 2.3.

Η ιδιαιτερότητα στο δημόσιο τομέα, έγκειται στο γεγονός, ότι οι σύγχρονες εφαρμογές ηλεκτρονικής διακυβέρνησης, που αναπτύχθηκαν στα πλαίσια του δημόσιου ψηφιακού μετασχηματισμού, διαχειρίζονται και διακινούν ένα πολύ μεγάλο όγκο πληροφορίων και δεδομένων προς τους φορείς της δημόσιας διοίκησης. Η πληροφορία των δεδομένων που

μπορεί να αντλήσει μια υπηρεσία από τα συστήματα αυτά (GovHub, ΑΑΔΕ, κλπ)[1] είναι μεγάλη και μπορεί να αφορά:

- Προσωπικές πληροφορίες πολιτών (ΑΦΜ, ΑΔΤ, Δ/νση κατοικίας, Τηλέφωνο, στοιχεία οχημάτων, περιουσιακά στοιχεία)
- Οικονομικά στοιχεία φυσικών και νομικών προσώπων (φορολογική ενημερότητα)
- Στοιχεία επιτηδευματιών (ΑΦΜ, δραστηριότητες, στοιχεία έδρας της επιχείρησης) κ.α.

Επειδή το σύνολο των πληροφοριών αυτών αποτελεί περιουσιακό στοιχείο του κράτους, υπάρχει πάντα το ζήτημα της ελεύθερης πρόσβασης σε αυτές και για το λόγο αυτό, η ανάγκη παρακολούθησης του σκοπού της συλλογής και επεξεργασίας αυτών κρίνεται απολύτως απαραίτητη.

2.8 Αιτήματα πολιτών προς τη Δημόσια Διοίκηση υπό τον ΓΚΠΔ

Τα φυσικά πρόσωπα (υποκείμενα των δεδομένων), για το σύνολο των δικαιωμάτων τους, όπως αυτά καθορίζονται στον ΓΚΠΔ[2], μπορούν να έρθουν σε επικοινωνία με κάθε δημόσιο φορέα ή υπεύθυνο επεξεργασίας αυτού, και να αιτηθούν ανάλογα την ενέργεια που επιθυμούν.

Εκτός όμως από τη νόμιμη άσκηση των δικαιωμάτων τους, οι πολίτες έχουν τη δυνατότητα διεκδίκησης αποζημίωσης εφόσον υπάρχει δημόσιος φορέας που έχει παραβιάσει τον ΓΚΠΔ, με συνέπεια να υποστούν υλική ζημία, ενώ η αξίωση αποζημίωσης γεννιέται άμεσα σε βάρος του άμεσα στον υπαίτιο δημόσιο φορέα ή με δικαστική προσφυγή στα αρμόδια εθνικά δικαστήρια του κράτους μέλους της Ευρωπαϊκής Ένωσης (Κυριαζόγλου 2019)

[1] Πλατφόρμες διαλειτουργικότητας http://aade.gr και http://govhub.gr
[2] Βλέπε παράγραφο 2.4

2.9 ΓΚΠΔ – Η Εφαρμογή του στους Δήμους – Σχέδιο Συμμόρφωσης

Όπως ήδη έχει αναφερθεί, από τις 25 Μαΐου 2018, που τέθηκε σε ισχύ ο Κανονισμός 2016/679, το σύνολο των φορέων της τοπικής αυτοδιοίκησης απαιτείται να είναι εναρμονισμένο με το νέο πλαίσιο. Οι Δήμοι, όντας το μεγαλύτερο και σημαντικότερο κομμάτι της τοπικής αυτοδιοίκησης, οφείλουν να έχουν ολοκληρώσει όλες τις απαραίτητες ενέργειες βάσει των οποίων θα αποδεικνύεται η συμμόρφωσή τους προς τις απαιτήσεις του ΓΚΠΔ και της προστασίας των προσωπικών δεδομένων που διαχειρίζονται.

Η υποχρέωση των Δήμων για συμμόρφωση, στα πλαίσια πάντα της λειτουργίας των υπηρεσιών τους και της εκτέλεσης των νόμιμων υποχρεώσεών τους, αφορά εκτός από τα δεδομένα πολιτών και «κάθε είδους προσωπικά δεδομένα που λαμβάνουν, διατηρούν, διαχειρίζονται, και εν γένει επεξεργάζονται κατά τη λειτουργία τους από τα ονοματεπώνυμα ως τα ευαίσθητα δεδομένα υγείας, είτε αυτά αφορούν σε διοικούμενους (φυσικά ή νομικά πρόσωπα) είτε σε υπαλλήλους των Δήμων» (Τασιόπουλος 2018). Επομένως, οφείλουν να ολοκληρώσουν το σύνολο των τεχνικών και οργανωτικών ενεργειών που αποδεικνύουν ότι έχουν ληφθεί από το φορέα τα κατάλληλα μέτρα προστασίας και διαχείρισης των προσωπικών και ευαίσθητων προσωπικών δεδομένων που διαχειρίζονται.

Η συμμόρφωση προς τον ΓΚΠΔ, απαιτεί επί της ουσίας από το φορέα – Δήμο, να προβεί ως νομική υποχρέωση, σε μια ολοκληρωμένη «Μελέτη Συμμόρφωσης». Οι ενέργειες που περιλαμβάνει μια τέτοια μελέτη, είναι οι εξής:

- ✓ Χαρτογράφηση (Data Mapping): το πρώτο μέρος σε μια Μελέτη Συμμόρφωσης, αποτελεί η αξιολόγηση της υφιστάμενης κατάστασης. Στο βήμα αυτό πρέπει να αναγνωριστούν και να καταγραφούν τα δεδομένα, οι ενέργειες επεξεργασίας, καθώς και το σύνολο των διαδικασιών συλλογής και αποθήκευσης των δεδομένων, προκειμένου να αξιολογηθεί η ετοιμότητα του φορέα ως προς τις απαιτήσεις του κανονισμού.
- ✓ Ανάλυση Κενών και Ελλείψεων (Gap Analysis): Επόμενο βήμα στη Μελέτη, είναι η Εκτίμηση των Ελλείψεων του φορέα. Στο βήμα αυτό πρέπει να εντοπιστούν οι

ελλείψεις του Δήμου αναφορικά με τις διαδικασίες επεξεργασίας και ασφάλειας των δεδομένων και να καταγραφούν σε ένα πίνακα ελλείψεων και αναγκών του φορέα.

- ✓ Ανάλυση Κινδύνων (Risk Analysis) & Εκτίμηση Αντικτύπου (Data Protection Impact Assesment): Ένα πολύ σημαντικό κομμάτι της μελέτης συμμόρφωσης, το οποίο ταυτίζεται γενικότερα και με την όλη φιλοσοφία του κανονισμού, είναι η καταγραφή της Εκτίμησης Αντικτύπου. Σκοπός της είναι ο έγκαιρος προσδιορισμός των κινδύνων ως προς την ιδιωτικότητα των δεδομένων, η εύρεση και αξιολόγηση κατάλληλων μέτρων προστασίας, καθώς και η επικύρωση και ενσωμάτωσή τους στην πολιτική μέτρων ασφαλείας του φορέα.
- ✓ Πολιτική Προστασίας: Σκοπός όλων του ανωτέρω ενεργειών, είναι η σύνταξη μιας κατάλληλης πολιτικής προστασίας, η οποία αφ' ενός θα αποδεικνύει τη συμμόρφωση του φορέα ως προς τον Κανονισμό και αφετέρου, θα διασφαλίζει την προάσπιση των δικαιωμάτων των υποκειμένων και τη βέλτιστη ασφάλεια των προσωπικών τους δεδομένων
- ✓ Αρχείο Δραστηριοτήτων Επεξεργασίας: είναι πλέον απαίτηση του Κανονισμού(βλ. άρθρο 30 αυτού), να τηρείται και ένα Αρχείο Δραστηριοτήτων Επεξεργασίας στο οποίο θα καταγράφεται το σύνολο των διαδικασιών που διενεργούνται από τις υπηρεσίες του φορέα - Δήμου και αφορούν σε προσωπικά δεδομένα.
- ✓ Εκπαίδευση Προσωπικού: στο πλαίσιο ευθύνης της διοίκησης του φορέα, είναι και η σωστή ενημέρωση και εκπαίδευση στο σύνολο του προσωπικού για όλες τις διαδικασίες συμμόρφωσης και την απαίτηση τήρησης των πολιτικών ασφάλειας και επεξεργασίας δεδομένων που έχουν υιοθετηθεί

Υπεύθυνος για την τήρηση των διαδικασιών που καταγράφονται στη Μελέτη Συμμόρφωσης του φορέα – Δήμου, καθίσταται ο Δήμος (ως νομικό πρόσωπο), που έχει το ρόλο, βάσει του ΓΚΠΔ, του Υπευθύνου. Επιπλέον, στον Υπεύθυνο Επεξεργασίας ανατίθεται η μέριμνα για την εκπαίδευση των υπαλλήλων και η μέριμνα για την επικαιροποίηση της Μελέτης όταν αυτό κρίνεται απαραίτητο.

Κεφάλαιο 3
Ανάλυση Κινδύνων

Στο 3ο κεφάλαιο της μεταπτυχιακής αυτής διατριβής (που αποτελεί και μελέτη περίπτωσης), θα παρουσιαστεί αναλυτικά όλη η ροή μιας Επεξεργασίας Δεδομένων που αφορά σε δημόσιο φορέα (μεγάλο Δήμο της ελληνικής επικράτειας) και εκτελείται από εξωτερικό συνεργάτη. Το κεφάλαιο ξεκινάει από την ανάλυση της υφιστάμενης κατάστασης και ακολουθεί μια πρώτη εκτίμηση ρίσκου με τη μεθοδολογία του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA). Ως συμπέρασμα της αρχικής εκτίμησης προκύπτει ότι οι παρούσες συνθήκες που επικρατούν στο Δήμο, σε συνδυασμό με τα μέτρα που θα πρέπει να ληφθούν προκειμένου να ολοκληρωθεί με ασφάλεια η επεξεργασία των προσωπικών δεδομένων, δεν είναι κατάλληλες για να προχωρήσει η διενέργεια της επεξεργασίας με ιδίους πόρους του φορέα. Λύση στο πρόβλημα δίνει η επιλογή κατάλληλου αναδόχου που θα υλοποιήσει το σύνολο της επεξεργασίας εκτός του οργανισμού. Ακολουθεί μια δεύτερη εκτίμηση ρίσκου για την περίπτωση που την επεξεργασία αναλαμβάνει εξωτερικός συνεργάτης και εν συνεχεία πραγματοποιείται μελέτη Εκτίμησης Αντικτύπου μέσω του λογισμικού PIA της γαλλικής Αρχής Προστασίας Δεδομένων (CNIL n.d.). Το κεφάλαιο ολοκληρώνεται με την καταγραφή μιας Ανάλυσης Κινδύνων Πληροφοριών και Πληροφοριακών Συστημάτων από την πλευρά του αναδόχου και Εκτελούντος την Επεξεργασία.

3.1 Περιγραφή της κατάστασης

Σε μεγάλο Δήμο της ελληνικής επικράτειας, μετά από έλεγχο που πραγματοποιήθηκε από αρμόδιο κρατικό όργανο, έγινε παρατήρηση ως προς την έλλειψη ενεργειών είσπραξης ενός μεγάλου ποσού βεβαιωμένων ανείσπρακτων ληξιπρόθεσμων οφειλών, που είναι καταγεγραμμένες στο πληροφοριακό σύστημα του Δήμου. Ο Δήμος αποφασίζει να προχωρήσει το συντομότερο δυνατό, σε εφαρμογή αναγκαστικών μέτρων είσπραξης

(αποστολή οφειλών στη ΔΟΥ, δέσμευση τραπεζικών λογαριασμών κα) βάσει κάποιων κριτηρίων που αποφάσισε η διοίκηση. Τα κριτήρια αυτά αφορούν: το ύψος και το είδος της οφειλής, αν η οφειλή αφορά φυσικό ή νομικό πρόσωπο, την ηλικιακή ομάδα των οφειλετών, την οικογενειακή τους κατάσταση και εισοδηματικά κριτήρια. Για την υλοποίηση του σχεδίου δράσης του Δήμου, γίνεται αντιληπτό ότι απαιτείται αρχικά, η επεξεργασία του συνόλου των δεδομένων των συναλλασσόμενων που τηρούνται στο φορέα και στη συνέχεια ο διαχωρισμός των οφειλετών ως προς τα κριτήρια που επιλέχθηκαν από τη διοίκηση για την εφαρμογή των μέτρων. Θα πρέπει να αναφερθεί επίσης, ότι ο τεχνολογικός εξοπλισμός του Δήμου δεν είναι ο πλέον σύγχρονος και η συντήρησή του δε γίνεται ακολουθώντας τις βέλτιστες τεχνικές ασφάλειας. Επίσης, λόγω κάποιων ειδικών συνθηκών (κινητικότητα υπαλλήλων), το ανθρώπινο δυναμικό στο φορέα είναι αποδυναμωμένο.

3.2 Παράμετροι της επεξεργασίας

Για τη σωστή εκτέλεση της επεξεργασίας των δεδομένων, πρέπει να ληφθούν υπόψη και κάποιες επιπλέον παράμετροι που μπορεί να επηρεάσουν τόσο τις αποφάσεις του φορέα ως προς την επεξεργασία, όσο και τη ροή της επεξεργασίας στη συγκεκριμένη περίπτωση και συνοψίζονται ακολούθως:

- Το ύψος και το είδος της οφειλής, καθώς και η κατηγορία του συναλλασσόμενου (φυσικό ή νομικό πρόσωπο), είναι δεδομένα τα οποία υπάρχουν ήδη ως πληροφορία στο αρχείο του Δήμου, οπότε η επεξεργασία ως προς τα αντίστοιχα κριτήρια μπορεί να πραγματοποιηθεί. Η ηλικιακή ομάδα, η οικογενειακή κατάσταση και το εισόδημα των οφειλετών όμως, αποτελούν δεδομένα που δε βρίσκονται πάντα στην κατοχή του φορέα. Πώς θα γίνει επομένως η αναζήτηση των συγκεκριμένων δεδομένων; Ο Δήμος σε αυτή την περίπτωση έχει τη δυνατότητα να ζητήσει από τους πολίτες να προσκομίσουν τα αντίστοιχα δεδομένα ή να τα αναζητήσει από τρίτα συστήματα που διασυνδέεται (όπως για παράδειγμα το Μητρώο Πολιτών, προκειμένου να εντοπίσει την ηλικία και την οικογενειακή κατάσταση ή ακόμα και τους πλησιέστερους συγγενείς αν πρόκειται για οφειλή που έχει βεβαιωθεί σε άτομο που έχει αποβιώσει)
- Τα περισσότερα δεδομένα που θα επεξεργαστούν είναι ενσωματωμένα στο πληροφοριακό σύστημα του Δήμου. Υπάρχουν όμως και αρκετά που βρίσκονται

αποθηκευμένα σε φυσικό αρχείο στις εγκαταστάσεις του φορέα, οπότε θα πρέπει να ληφθεί υπόψη η επεξεργασία και αυτού του αρχείου.

- Τα δεδομένα που θα αναλυθούν για να προκύψουν τα εισοδηματικά κριτήρια που θέλει ο Δήμος, περιέχουν ευαίσθητες προσωπικές πληροφορίες (δεδομένα υγείας, αναπηρίες κλπ.)

3.3 Ανάλυση της Επεξεργασίας

Ο Υπεύθυνος επεξεργασίας, ο οποίος στη συγκεκριμένη περίπτωση είναι ο ίδιος ο φορέας, (Δήμος), και βάσει των αρμοδιοτήτων που καθορίζει ο Κανονισμός, οφείλει αρχικά να ερευνήσει αν απαιτείται διενέργεια "Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων" (ΕΑΠΔ) για τη συγκεκριμένη επεξεργασία. Γνωρίζοντας τις περιπτώσεις για τις οποίες η διενέργεια της εκτίμησης αντικτύπου είναι υποχρέωση (περιπτώσεις της παραγράφου 3 του άρθρου 35) και όπως αυτές αναφέρθηκαν και στην παράγραφο 2.6 της παρούσας διατριβής, μπορούμε να πούμε ότι η συγκεκριμένη επεξεργασία εμπίπτει στις περιπτώσεις αυτές που απαιτούν εξορισμού διενέργεια ΕΑΠΔ, διότι αφορά περίπτωση *μεγάλης κλίμακας επεξεργασίας δεδομένων και ευαίσθητων προσωπικών δεδομένων.*

Λόγω των ειδικών συνθηκών που επικρατούν στο Δήμο (απουσία σύγχρονου και ασφαλούς τεχνολογικού εξοπλισμού, καθώς και έλλειψη ανθρώπινου δυναμικού) γίνεται αντιληπτό ότι υπάρχει πιθανότητα να μη μπορεί να εκτελεστεί άμεσα και με ασφάλεια η επεξεργασία των προσωπικών δεδομένων. Για το λόγο αυτό, αποφασίζεται να πραγματοποιηθεί μια αρχική εκτίμηση, που θα καταδείξει αν ο Δήμος έχει τα μέσα και τους πόρους να ανταποκριθεί αυτοτελώς και με ασφάλεια στη διενέργεια της επεξεργασίας.

3.3.1 Αξιολόγηση κινδύνων με τη μεθοδολογία ENISA (Η επεξεργασία λαμβάνει χώρα στο Φορέα)

Η μεθοδολογία αξιολόγησης κινδύνων ENISA, αποτελεί ένα σύνολο κατευθυντήριων γραμμών, προκειμένου να αξιολογηθεί στην πράξη ο κίνδυνος που ενέχει για τα δικαιώματα και τις ελευθερίες των υποκείμενων μια ενέργεια Επεξεργασίας Δεδομένων.

Το τελευταίο βήμα της μεθοδολογία, προσανατολίζεται στην ορθή επιλογή τεχνικών και οργανωτικών μέτρων κατάλληλων να περιορίσουν τους κινδύνους που εντοπίστηκαν.

Βήμα_1: Ορισμός της Επεξεργασίας και του πλαισίου της

Στο πρώτο βήμα της αξιολόγησης, καταγράφονται τα δεδομένα προς επεξεργασία, ο σκοπός της, το υποκείμενο των δεδομένων, τα μέσα που θα χρησιμοποιηθούν στην εκτέλεση της επεξεργασίας, του τελικούς παραλήπτες, καθώς και το χώρο που θα πραγματοποιηθεί η συγκεκριμένη διαδικασία. Τα δεδομένα αυτά καταγράφονται στον Πίνακα που ακολουθεί.

ΠΕΡΙΓΡΑΦΗ ΕΠΕΞΕΡΓΑΣΙΑΣ: Ανάλυση οφειλών πολιτών προς το Δήμο	
Προσωπικά δεδομένα προς επεξεργασία	Προσωπικά στοιχεία (όνομα, επίθετο, φύλο, ηλικία, διεύθυνση, τηλέφωνο), ΑΦΜ, περιουσιακή κατάσταση, οικονομικά στοιχεία οφειλών, στοιχεία εισοδήματος, δεδομένα υγείας
Σκοπός επεξεργασίας	Ανάλυση των οφειλών των δημοτών και κατηγοριοποίησή τους βάσει συγκεκριμένων κριτηρίων
Υποκείμενο δεδομένων	Το σύνολο των δημοτών του φορέα
Μέσα επεξεργασίας	Τμήμα Εσόδων του Δήμου
Παραλήπτες δεδομένων	Δήμος
Που λαμβάνει χώρα η επεξεργασία	Εσωτερικά, στις εγκαταστάσεις του Δήμου

Πίνακας 1: Περιγραφή Επεξεργασίας: Ανάλυση οφειλών πολιτών προς το Δήμο

Βήμα_2: Αξιολόγηση Επιπτώσεων

Στο δεύτερο βήμα της μεθοδολογίας, πρέπει να αξιολογηθεί βάσει μιας συγκεκριμένης κλίμακας (low, medium, high, very high) ο αντίκτυπος που θα έχει στο υποκείμενο της επεξεργασίας πιθανή απώλεια στην Εμπιστευτικότητα, στην Ακεραιότητα και τη Διαθεσιμότητα των προσωπικών δεδομένων που επεξεργάζονται.

Απώλεια Εμπιστευτικότητας

Η Εμπιστευτικότητα αφορά την προστασία των πληροφοριών (προσωπικών δεδομένων) από μη εξουσιοδοτημένη αποκάλυψή (ανάγνωση) τους. Στα πλαίσια της συγκεκριμένης επεξεργασίας, Απώλεια Εμπιστευτικότητας μπορεί να προκύψει είτε από πιθανή ακούσια αποκάλυψη του εισοδήματος, ή δεδομένων υγείας σε τρίτους, είτε από

πιθανή πρόσβαση στα δεδομένα κάποιου τρίτου, μέσω ψηφιακής υποκλοπής δεδομένων. Μια τέτοια απώλεια εκθέτει το υποκείμενο σε συνέπειες, όπως η ταλαιπωρία που προκύπτει από τη δημοσιοποίηση των προσωπικών του δεδομένων, ή και η πιθανή στόχευσή του σε επιθέσεις κλοπής. Ιδιαίτερη όμως προσοχή θα πρέπει να δοθεί στην περίπτωση όπου η Απώλεια Εμπιστευτικότητας σχετίζεται με τα ευαίσθητα δεδομένα υγείας (ασθένειες, ιατρικές πληροφορίες) που τηρούνται στο πληροφοριακό σύστημα. Πιθανή απώλεια των δεδομένων αυτών μπορεί να εκθέσει το υποκείμενο σε κοινωνικό στιγματισμό και να υποχρεώσει το Δήμο σε καταβολή υψηλών προστίμων. Για τους λόγους αυτούς η Απώλεια εμπιστευτικότητας θα μπορούσε να τεθεί στο επίπεδο διαβάθμισης **VERY HIGH**.

Απώλεια Ακεραιότητας των πληροφοριών

Η Ακεραιότητα των πληροφοριών αφορά την προστασία των πληροφοριών από μη εξουσιοδοτημένη μεταβολή (τροποποίηση & διαγραφή) τους. Στα πλαίσια της επεξεργασίας των στοιχείων των δημοτών, πιθανή Απώλεια Ακεραιότητας των πληροφοριών, ενδέχεται να υποβάλλει τα υποκείμενα σε ταλαιπωρία, αν χρειαστεί να υποβάλλουν εκ νέου τα στοιχεία τους στον οργανισμό, είτε στην περίπτωση που προκύψει λανθασμένη κατηγοριοποίησή τους ως προς την εφαρμογή των μέτρων είσπραξης από το Δήμο και τους επιβληθεί κάποιο δυσβάσταχτο για την περίπτωσή τους, οικονομικό μέτρο αναγκαστικής είσπραξης (πχ δέσμευση τραπεζικού λογαριασμού). Με τα δεδομένα αυτά, η Απώλεια Ακεραιότητας των πληροφοριών θα μπορούσε να τεθεί στο επίπεδο διαβάθμισης **HIGH**.

Απώλεια Διαθεσιμότητας των πληροφοριών

Η Διαθεσιμότητα των πληροφοριών, αφορά τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης στις πληροφορίες (είτε για "ανάγνωση" είτε για "μεταβολή"), χωρίς εμπόδια ή καθυστερήσεις. Στα πλαίσια της συγκεκριμένης επεξεργασίας, πιθανή Απώλεια Διαθεσιμότητας των πληροφοριών μπορεί να έχει ως αποτέλεσμα την αδυναμία ικανοποίησης των δικαιωμάτων των πολιτών εφόσον τα ασκήσουν. Για το λόγο αυτό, ο αντίκτυπος της Απώλειας Διαθεσιμότητας των πληροφοριών θα μπορούσε να τεθεί στο επίπεδο διαβάθμισης **HIGH**.

Ο παρακάτω πίνακας συνοψίζει την προαναφερθείσα ανάλυση.

ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ (Ι)		
Εμπιστευτικότητα	**Ακεραιότητα**	**Διαθεσιμότητα**
ΠΟΛΥ ΥΨΗΛΗ	ΥΨΗΛΗ	ΥΨΗΛΗ
Συνολική Αξιολόγηση Επιπτώσεων:		**ΠΟΛΥ ΥΨΗΛΗ**

Ως Συνολική Αξιολόγηση των επιπτώσεων καθορίζεται το υψηλότερο επίπεδο διαβάθμισης που εντοπίστηκε. Επομένως, ο συνολικός αντίκτυπος σε αυτή τη συγκεκριμένη περίπτωση εκτιμάται ως **ΠΟΛΥ ΥΨΗΛΟΣ**.

Βήμα_3: Πιθανότητα εμφάνισης Απειλών

Στο βήμα αυτό αποτυπώνονται οι απειλές που σχετίζονται με το συνολικό περιβάλλον της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και αξιολογείται η πιθανότητα εμφάνισής τους. Οι τέσσερεις κύριοι τομείς αξιολόγησης του περιβάλλοντος επεξεργασίας αφορούν:

- *Το δίκτυο και τους τεχνικούς πόρους (υλικό και λογισμικό)*
- *Τις διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων*
- *Τα διαφορετικά τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας*
- *Στον τομέα και την κλίμακα της επεξεργασίας*

Δίκτυο & Τεχνικοί Πόροι:

Για να αξιολογηθεί η πιθανότητα εμφάνισης απειλής μέσω Δικτύου και Τεχνικών πόρων, πρέπει να απαντηθούν τα εξής ερωτήματα:

1. ***Πραγματοποιείται οποιοδήποτε μέρος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω του διαδικτύου;***

   Η πλειοψηφία των δεδομένων που θα επεξεργαστούν είναι ψηφιακά και καταχωρημένα στο πληροφοριακό σύστημα του οργανισμού το οποίο είναι προσβάσιμο διαδικτυακά, αλλά μόνο μέσω δικτύου Intranet (syzefxis). Σε κάποιο χρήστη που το επιθυμεί, μπορεί να δοθεί η δυνατότητα διενέργειας της επεξεργασίας μέσω του διαδικτύου και της εφαρμογής remote desktop .

2. ***Είναι δυνατή η παροχή πρόσβασης σε εσωτερικό αρχείο δεδομένων προσωπικού χαρακτήρα μέσω του διαδικτύου;***

   Στις εγκαταστάσεις του φορέα, η πιθανότητα να έχει κάποιος απομακρυσμένη πρόσβαση στα δεδομένα είναι μεγάλη, είτε αυτή πραγματοποιείται μέσω διαδικτύου, είτε μέσω Intranet.

3. ***Είναι το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα διασυνδεδεμένο με άλλο εξωτερικό ή εσωτερικό πληροφοριακό σύστημα ή υπηρεσία;***

   Γενικά η ύπαρξη διασύνδεσης με τρίτα συστήματα και υπηρεσίες, πάντα ενέχει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης λόγω πιθανών τρωτών σημείων στα πληροφοριακά συστήματα. Σε ότι αφορά την επεξεργασία εντός του φορέα, το σύστημα επεξεργασίας είναι διασυνδεδεμένο με τρίτα πληροφοριακά συστήματα και υπηρεσίες. Αυτό συμβαίνει για τους εξής λόγους: αρχικά, το δίκτυο Intranet στο οποίο ανήκει ο Δήμος, διασυνδέει πολλούς διαφορετικούς φορείς με διαφορετικά πληροφοριακά συστήματα. Επιπλέον οι κόμβοι διαλειτουργικότητας που έχουν δοθεί προς χρήση στους δημόσιους φορείς, επιτρέπουν σε πολλές εξωτερικές διαδικτυακές κρατικές υπηρεσίες να επικοινωνούν μέσω web services με τους φορείς που το επιθυμούν.

4. ***Μπορούν μη εξουσιοδοτημένα άτομα να έχουν εύκολα πρόσβαση στο περιβάλλον του συστήματος επεξεργασίας δεδομένων;***

   Πάντα το φυσικό περιβάλλον είναι μια πολύ σημαντική πτυχή της ασφάλειας, που αν δε διασφαλιστεί επαρκώς μπορεί να θέσει σε κίνδυνο οποιαδήποτε επεξεργασία. Ο κίνδυνος επομένως μη εξουσιοδοτημένης πρόσβασης υπάρχει πάντα.

5. ***Το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα έχει σχεδιαστεί, υλοποιηθεί ή συντηρείται χωρίς να ακολουθεί τις σχετικές βέλτιστες πρακτικές;***

   Το σύστημα επεξεργασίας των δεδομένων εντός του φορέα, και σε ότι αφορά την αξιοπιστία του υλικού, δεν θεωρείται ότι ακολουθεί τις βέλτιστες πρακτικές. Ο

τεχνικός εξοπλισμός είναι σχετικά παλιός και δεν συντηρείται σύμφωνα με τις βέλτιστες πρακτικές.

Έχοντας σαν αναφορά τα παραπάνω ερωτήματα που θέτει η μεθοδολογία ENISA μπορεί να γίνει μια πρώτη καταγραφή των ευπαθειών και απειλών που σχετίζονται με το Δίκτυο και τους Τεχνικούς Πόρους και είναι οι εξής:

#	Αιτία/Ευπάθεια	Απειλή
1	Δυνατότητα απομακρυσμένης εκτέλεσης της επεξεργασίας (remote desktop)	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου)
2	Δυνατότητα σύνδεσης κακόβουλου χρήστη στο πληροφοριακή σύστημα που εκτελείται η επεξεργασία μέσω του Intranet	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου), Κοινολόγηση προσωπικών δεδομένων
3	Δυνατότητα διασύνδεσης του πληροφοριακού συστήματος με άλλα, μέσω δικτύου	Διαδικτυακή πρόσβαση μη εξουσιοδοτημένου χρήστη, Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου), Κοινολόγηση προσωπικών δεδομένων
4	*Έλλειψη περιορισμών στη χρήση εφαρμογών διαμοιρασμού αρχείων (πχ dropbox, onedrive κλπ)*	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου)
5	Δυνατότητα να εισέλθουν στο χώρο επεξεργασίας και άτομα που δε σχετίζονται με αυτή	Κοινολόγηση προσωπικών δεδομένων (λόγω αμέλειας κλειδώματος του υπολογιστή κατά την απουσία του εκτελούντος της επεξεργασία), Πρόσβαση μη εξουσιοδοτημένου χρήστη (απουσία ελέγχου εισόδου στο χώρο)
6	Παρωχημένος τεχνολογικός εξοπλισμός, που δε συντηρείται βάσει βέλτιστων πρακτικών	Απώλεια προσωπικών δεδομένων λόγω αστοχίας του τεχνολογικού εξοπλισμού
7	Δυνατότητα των χρηστών να διακόψουν τις αναβαθμίσεις του λειτουργικού και του antivirus	Μόλυνση του συστήματος από κακόβουλο λογισμικό με πιθανή συνέπεια την κοινολόγηση ή απώλεια των προσωπικών δεδομένων

Πίνακας 2: Ευπάθειες και απειλές που σχετίζονται με το Δίκτυο και τους Τεχνικούς Πόρους

Κάνοντας μια εκτίμηση των παραπάνω ευπαθειών που εντοπιστήκαν, μπορούμε να συμπεράνουμε ότι συνολικά, η πιθανότητα εμφάνισης απειλής που σχετίζεται με το Δίκτυο και τους Τεχνικούς Πόρους είναι **ΥΨΗΛΗ.**

Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων:

Για την αξιολόγηση της πιθανότητας απειλής σε αυτόν τον τομέα πρέπει να απαντηθούν τα εξής ερωτήματα:

1. ***Είναι οι ρόλοι και οι ευθύνες όσον αφορά την επεξεργασία των προσωπικών δεδομένων σαφώς καθορισμένοι;***

   Καθώς ο Δήμος είναι εναρμονισμένος με τις απαιτήσεις του ΓΚΠΔ, οι ρόλοι των εκτελούντων την επεξεργασία είναι καθορισμένοι

2. ***Είναι σαφώς καθορισμένο το ποιος θα κάνει χρήση του δικτύου, του συστήματος και των φυσικών πόρων εντός του οργανισμού που εκτελείται η επεξεργασία;***

   Χρήση του δικτύου, του πληροφοριακού συστήματος καθώς και των φυσικών πόρων γίνεται από τα σύνολο των εργαζομένων στο φορέα, επομένως δεν περιορίζεται μόνο στους εκτελούντες την επεξεργασία.

3. ***Επιτρέπεται στους εργαζόμενους να φέρνουν και να χρησιμοποιούν τις δικές τους συσκευές για να συνδεθούν στο σύστημα επεξεργασίας των προσωπικών δεδομένων;***

   Δεν υπάρχει κάποια πολιτική που να απαγορεύει τη χρήση εντός του οργανισμού, συσκευών που δεν ανήκουν στο φορέα

4. ***Επιτρέπεται στους εργαζόμενους να μεταφέρουν, να αποθηκεύουν ή να επεξεργάζονται με άλλο τρόπο δεδομένα προσωπικού χαρακτήρα εκτός των εγκαταστάσεων του οργανισμού;***

   Βάσει των απαιτήσεων του ΓΚΠΔ, οι εργαζόμενοι δεν επιτρέπεται να μεταφέρουν προσωπικά δεδομένα εκτός των εγκαταστάσεων του φορέα, παρόλα αυτά, σε περίπτωση που υπάρχει δόλος, μια τέτοια πιθανότητα δε μπορεί να αποκλειστεί.

5. ***Μπορούν οι δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα να διεξάγονται χωρίς δημιουργία αρχείων καταγραφής;***

   Στο Δήμο τηρείται Μητρώο Επεξεργασιών σύμφωνα με τους κανόνες συμμόρφωσης του ΓΚΠΔ σχετικά με το είδος της επεξεργασίας που μπορεί να λάβει χώρα στο φορέα. Μεμονωμένα όμως, οι καθημερινές δραστηριότητες επεξεργασίας διεξάγονται χωρίς δημιουργία αρχείων καταγραφής.

Έχοντας σαν αναφορά τα παραπάνω ερωτήματα, μπορούμε να γίνει μια πρώτη καταγραφή των ευπαθειών και απειλών που σχετίζονται με τις Διαδικασίες/Διεργασίες της επεξεργασίας και είναι οι εξής:

#	Αιτία/Ευπάθεια	Απειλή
1	Έλλειψη ελέγχου ως προς τη χρήση του δικτύου και των πόρων κατά την εκτέλεση της επεξεργασίας	Αστοχία συστήματος και αδυναμία ολοκλήρωσης της επεξεργασίας λόγω έλλειψης πόρων
2	Προσβολή του συστήματος από κακόβουλο λογισμικό που προήλθε από τη σύνδεση στο δίκτυο ήδη “μολυσμένης” προσωπικής συσκευής χρήστη (USB, Laptop κλπ.)	Απώλεια προσωπικών δεδομένων από κακόβουλο λογισμικό
3	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού μέσω αφαιρούμενων μέσων αποθήκευσης (USB, φορητός σκληρός δίσκος)	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού από κακόβουλο χρήστη
4	Έλλειψη μηχανισμού καταγραφής (logging)	Αλλοίωση ή διαγραφή των προσωπικών δεδομένων λόγω εισόδου μη εξουσιοδοτημένου χρήστη

Πίνακας 3: Ευπάθειες και απειλές που σχετίζονται με τις Διαδικασίες/Διεργασίες της επεξεργασίας

Η πιθανότητα εμφάνισης απειλής είναι **ΥΨΗΛΗ**, καθώς ναι μεν η συμμόρφωση με τον Κανονισμό, περιορίζει τον κίνδυνο ως προς τον καθορισμό ρόλων και αρμοδιοτήτων κατά την επεξεργασία, υπάρχει όμως έντονα ο κίνδυνος μεταφοράς δεδομένων εκτός οργανισμού και μη εξουσιοδοτημένης πρόσβασης στο σύστημα που θα εκτελεστεί η επεξεργασία.

Τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας:

Για την αξιολόγηση της πιθανότητας απειλής σε αυτόν τον τομέα πρέπει να απαντηθούν τα εξής ερωτήματα:

1. ***Πραγματοποιείται η επεξεργασία δεδομένων προσωπικού χαρακτήρα από μη καθορισμένο αριθμό υπαλλήλων;***

   Η επεξεργασία των δεδομένων πραγματοποιείται από τους υπαλλήλους που ανήκουν συγκεκριμένα στο τμήμα Εσόδων του Δήμου

2. ***Εκτελείται οποιοδήποτε μέρος της διαδικασίας επεξεργασίας δεδομένων από εργολάβο/συνεργάτη (εκτελών την επεξεργασία δεδομένων);***

   Θεωρείται ότι το σύνολο της επεξεργασίας θα υλοποιηθεί εντός του φορέα με ιδίους πόρους, επομένως οποιαδήποτε ενέργεια ελέγχεται πλήρως από τον υπεύθυνο επεξεργασίας του φορέα

3. ***Είναι οι υποχρεώσεις των μερών που εμπλέκονται στην επεξεργασία δεδομένων σαφώς καθορισμένες;***

   Οι υποχρεώσεις του εκτελούντος την επεξεργασία και του υπεύθυνου επεξεργασίας, οφείλουν να είναι σαφώς καθορισμένες, βάσει και των διατάξεων του άρθ. 60 του Ν.4624/2019

4. ***Είναι το προσωπικό που εμπλέκεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα εξοικειωμένο με θέματα ασφάλειας πληροφοριών;***

   Η συμμόρφωση του φορέα με το ΓΚΠΔ, προϋποθέτει ότι το σύνολο του προσωπικού του φορέα, είναι σωστά εκπαιδευμένο και ενημερωμένο σχετικά με θέματα ασφάλειας πληροφοριών

5. ***Τα πρόσωπα/μέρη που εμπλέκονται στην επεξεργασία δεδομένων αμελούν να αποθηκεύουν ή/και να καταστρέφουν με ασφάλεια τα δεδομένα προσωπικού χαρακτήρα;***

   Βάσει των όσων επιβάλει ο Κανονισμός σχετικά με το χρόνο ζωής των δεδομένων και την αναγκαιότητα τήρησή τους εντός των οργανισμών, είναι ξεκάθαρο ότι τα δεδομένα τηρούνται για συγκεκριμένο χρονικό διάστημα και διαγράφονται όταν πλέον έχει ολοκληρωθεί ο σκοπός της επεξεργασίας. Επειδή όμως η αμέλεια είναι

ανθρώπινος μη ελεγχόμενος παράγοντας, η πιθανότητα του να συμβεί δε μπορεί να αποκλειστεί.

#	Αιτία/Ευπάθεια	Απειλή
1	Έλλειψη ελέγχου ως προς τη χρήση του δικτύου και των πόρων κατά την εκτέλεση της επεξεργασίας	Αστοχία συστήματος και αδυναμία ολοκλήρωσης της επεξεργασίας λόγω έλλειψης πόρων
2	Αμέλεια καταστροφής του φυσικού αρχείου από τους χρήστες, ενώ έχει ολοκληρωθεί ο σκοπός επεξεργασίας του ή δε χρειάζεται για τους σκοπούς της επεξεργασίας	Έκθεση προσωπικών δεδομένων σε μη εξουσιοδοτημένα άτομα

Πίνακας 4: Ευπάθειες και απειλές που σχετίζονται με Τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας

Το εύρος της πιθανότητας εμφάνισης απειλής στον τομέα που σχετίζεται με τα "Τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας" είναι αρκετά περιορισμένο, λόγω της απαίτησης συμμόρφωσης του δημόσιου τομέα με το ΓΚΠΔ. Αυτό έχει σαν αποτέλεσμα οι διαδικασίες και υποχρεώσεις των εκτελούντων την επεξεργασία, να είναι σαφώς καθορισμένες. Παρόλα αυτά, η πιθανότητα εμφάνισης απειλής δεν εκμηδενίζεται, διότι πάντα παραμένει ο παράγοντας κινδύνου που προκύπτει από την ανθρώπινη αμέλεια. Η πιθανότητα εμφάνισης απειλής σε αυτό τον τομέα χαρακτηρίζεται ως **ΜΕΤΡΙΑ**.

Τομέας & Κλίμακα επεξεργασίας:

Για την αξιολόγηση της πιθανότητας απειλής σε αυτόν τον τομέα πρέπει να απαντηθούν τα εξής ερωτήματα:

1. ***Θεωρείτε ότι ο τομέας που δραστηριοποιείται ο φορέας είναι επιρρεπής σε κυβερνοεπιθέσεις;***

   Ο τομέας της δημόσιας διοίκησης στην Ελλάδα, έχει δεχθεί επιθέσεις κυβερνοεπίθεσης, με πιο γνωστή αυτή που πραγματοποιήθηκε τον Ιούλιο του 2020 και είχε ως στόχο το πληροφοριακό σύστημα ενός πού μεγάλου Δήμου της χώρας. Αποτέλεσμα της επίθεσης ήταν να μείνει πολλές μέρες εκτός λειτουργίας το πληροφοριακό σύστημα του Δήμου και να χαθούν πολλά ηλεκτρονικά αρχεία. Επιθέσεις στον ίδιο Δήμο, με διαρροή δεδομένων όπως επιστολές του δήμου προς πολίτες για ανείσπρακτες οφειλές με προσωπικά στοιχεία, ΑΦΜ, διευθύνσεις

ακινήτων πραγματοποιήθηκαν και τον Αύγουστο του 2021[3]. Επίσης, πολύ συχνή επίθεση προς τους δημόσιους φορείς, είναι η "μόλυνση" των τερματικών και των servers, με κακόβουλο λογισμικό που κρυπτογραφεί το σύνολο των δεδομένων, απαιτώντας στη συνέχεια λύτρα για την επαναφορά τους.

2. ***Έχει υποστεί ο φορέας οποιαδήποτε κυβερνοεπίθεση ή άλλου είδους παραβίαση της ασφάλειας τα τελευταία δύο χρόνια;***

   Ο server και τα τερματικά των χρηστών του Δήμου, τον προηγούμενο χρόνο μολύνθηκαν από ιό που μετακινήθηκε μέσω ηλεκτρονικού ταχυδρομείου και κρυπτογράφησε το σύνολο των δεδομένων του φορέα

3. ***Έχετε λάβει οποιεσδήποτε κοινοποιήσεις ή/και καταγγελίες σχετικά με την ασφάλεια του πληροφοριακού συστήματος που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων κατά το τελευταίο έτος;***

   Ο φορέας δεν έχει λάβει κάποια καταγγελία σχετικά με την ασφάλεια των πληροφοριακών του συστημάτων το τελευταίο έτος

4. ***Θεωρείτε η συγκεκριμένη επεξεργασίας, αποτελεί επεξεργασία δεδομένων μεγάλης κλίμακας;***

   Η συγκεκριμένη επεξεργασία, θεωρείτε επεξεργασία μεγάλης κλίμακας, καθώς αφορά δεδομένα και ευαίσθητα προσωπικά δεδομένα μεγάλου Δήμου της ελληνικής επικράτειας.

5. ***Υπάρχουν βέλτιστες πρακτικές ασφάλειας για τον συγκεκριμένο τομέα υπηρεσιών που δεν έχουν ακολουθηθεί επαρκώς;***

   Στο συγκεκριμένο φορέα, όπως και γενικά σε όλο το δημόσιο τομέα υπάρχει ως απαίτηση η συμμόρφωση με τον ΓΚΠΔ, οι οδηγίες του οποίου πράγματι εφαρμόζονται. Επιπλέον όμως, υπάρχει πληθώρα ενεργειών που θα μπορούσε να ακολουθήσει ο φορέας, κυρίως ως προς την ασφάλεια των πληροφοριακών του συστημάτων και τεχνολογικού εξοπλισμού

[3] https://www.protothema.gr/greece/article/1151035/hakers-htupisan-ton-dimo-thessalonikis-kai-dierreusan-2000-eggrafa/

Η πιθανότητα εμφάνισης απειλής είναι **ΥΨΗΛΗ**, καθώς αφορά σε μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων, εμπίπτει γενικότερα σε τομέα όπου τα τελευταία χρόνια έχει δεχθεί πληθώρα κυβερνοεπιθέσεων και πρόκειται να υλοποιηθεί σε πληροφοριακό σύστημα που βρίσκεται σε δίκτυο που έχει εμφανίσει σημεία τρωτότητας.

ΤΟΜΕΑΣ ΑΞΙΟΛΟΓΗΣΗ	**ΠΙΘΑΝΟΤΗΤΑ**	
	Διαβάθμιση	**SCORE**
Δίκτυο & Τεχνικοί Πόροι	☐ Χαμηλή	1
	☐ Μέτρια	2
	☒Υψηλή	3
Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων	☐ Χαμηλή	1
	☐ Μέτρια	2
	☒Υψηλή	3
Τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας	☐ Χαμηλή	1
	☒ Μέτρια	2
	☐Υψηλή	3
Τομέας & Κλίμακα επεξεργασίας	☐ Χαμηλή	1
	☐ Μέτρια	2
	☒Υψηλή	3
Συνολικό Άθροισμα Πιθανότητας Εμφάνισης Απειλής		**11**

Ακολουθώντας το πρότυπο ENISA, η πιθανότητα εμφάνισης απειλής συνολικά, χαρακτηρίζεται ως **ΥΨΗΛΗ**.

Συνολικό Άθροισμα Πιθανότητας Εμφάνισης Απειλής	**Επίπεδο Πιθανότητας Εμφάνισης Απειλής**
4 - 5	Χαμηλό
6 - 8	Μέτριο
9 - 12	Υψηλό

Βήμα_4: Αξιολόγηση Κινδύνου

Επίπεδο Επίπτωσης				
Πιθανότητα Εμφάνισης Απειλής		*Χαμηλό*	*Μέτριο*	*Υψηλό/Πολύ Υψηλό*
	Χαμηλό			
	Μέτριο			
	Υψηλό			☒

Βάσει της αξιολόγησης που πραγματοποιήθηκε στα δύο προηγούμενα βήματα, ο συνολικός κίνδυνος για τη συγκεκριμένη περίπτωση θεωρείται **ΥΨΗΛΟΣ** και κρίνεται απαραίτητη η υιοθέτηση απαραίτητων μέτρων ασφάλειας για τον μετριασμό/αποφυγή των κινδύνων που απειλούν τη διαδικασία της επεξεργασίας.

Βήμα_5: Υιοθέτηση Μέτρων Ασφάλειας

Καθώς ο μεγαλύτερος κίνδυνος που εμφανίζεται στο Δήμο αφορά τις εγκαταστάσεις και τον εξοπλισμό, τα μέτρα που επιβάλλεται να παρθούν αφορούν κυρίως:

- Νέο τεχνολογικό εξοπλισμό (server και τερματικά), για να ελαχιστοποιηθούν οι πιθανότητες αστοχίας του υλικού
- Κατάλληλο λογισμικό προκειμένου να δημιουργήσει ένα ασφαλές περιβάλλον επεξεργασίας των δεδομένων
- Προμήθεια συστημάτων παρακολούθησης (monitoring) της κίνησης του δικτύου προς αποφυγή κυβερνοεπιθέσεων
- Εγκατάσταση κάποιου συστήματος που θα παρέχει υπηρεσίες καταλόγου στο δίκτυο (πχ Active Directory)
- Εγκατάσταση συστήματος ελέγχου φυσικής πρόσβασης σε χώρους που περιέχουν εξοπλισμό (server room)
- Συστήματα προστασίας του εξοπλισμού (κλιματιστικά στο server room, αντικλεπτικά συστήματα κλπ.)

Επιπλέον πρέπει να υιοθετηθούν και συγκεκριμένες πολιτικές που θα πρέπει να ακολουθούν οι χρήστες και θα αφορούν:

- Τη χρήση ασφαλών κωδικών πρόσβασης (password)
- Τη χρήση αφαιρούμενων μέσων αποθήκευσης
- Την ασφάλεια δικτύου και ασύρματου δικτύου του φορέα

Η υλοποίηση όλων των παραπάνω προτεινόμενων μέτρων προκειμένου να πραστατεύει μια επεξεργασία Υψηλού Κινδύνου, απαιτεί και πολύ μεγάλο χρηματικό κεφάλαιο (προμήθεια εξοπλισμού), αλλά και πολύ μεγάλο χρονικό διάστημα για να ολοκληρωθεί. Επιπλέον ο φορέας γνωρίζει πως οι διαδικασίες προμήθειας αγαθών στο δημόσιο τομέα είναι πολύ χρονοβόρες και το χρονοδιάγραμμα για την ολοκλήρωση της επεξεργασίας είναι περιορισμένο. Ένα επιπλέον πρόβλημα που φαίνεται να αποτελεί εμπόδιο στην πραγματοποίηση της επεξεργασίας από το φορέα, είναι και η έλλειψη ανθρώπινου δυναμικού. Επομένως, ο Δήμος, μη έχοντας την τεχνολογική υποδομή και το ανθρώπινο δυναμικό, να πραγματοποιήσει την επεξεργασία αυτή άμεσα και γρήγορα, αποφάσισε να αναζητήσει εξωτερικό συνεργάτη για να του αναθέσει τη συγκεκριμένη επεξεργασία.
Εφόσον ο φορέας έχει ήδη πραγματοποιήσει μια πρώτη ανάλυση των πιθανών κινδύνων της επεξεργασίας, έχει εντοπιστεί και τα σημεία εκείνα τα οποία χρειάζονται ιδιαίτερη προσοχή (ασφάλεια στις υποδομές, πολιτικές προστασίας δεδομένων, κατάλληλη κατάρτιση), επομένως η αναζήτηση του συνεργάτη πρέπει να πληροί πολύ συγκεκριμένα κριτήρια ασφάλειας. Γνωρίζοντας επίσης ότι μια πιστοποίηση ISO27001 σε έναν οργανισμό εξασφαλίζει πολύ μεγάλο επίπεδο ασφάλειας δεδομένων και διαδικασιών, έθεσε ως βασική προϋπόθεση στην αναζήτηση αναδόχου, τη συμμόρφωση με το συγκεκριμένο πρότυπο, καθώς επίσης και το να μην του έχει επιβληθεί στο παρελθόν καμία κύρωση από την Αρχή Προστασίας Προσωπικών Δεδομένων. Με τον τρόπο αυτό θεωρεί πως μπορεί να εξασφαλίσει μια πολύ καλή επιλογή ως προς έναν εξωτερικό συνεργάτη με εχέγγυα.

3.3.2 Αξιολόγηση κινδύνων με τη μεθοδολογία ENISA (Η επεξεργασία λαμβάνει χώρα εκτός οργανισμού)

Έχοντας προχωρήσει πλέον ο φορές σε συμφωνία με εξωτερικό συνεργάτη για την υλοποίηση της επεξεργασίας, πρέπει να πραγματοποιηθεί εκ νέου μια αξιολόγηση κινδύνων με τα νέα δεδομένα. Και σε αυτή την περίπτωση, όπως και στην αρχική, ακολουθείται η μεθοδολογία ENISA.

Βήμα_1: Ορισμός της Επεξεργασίας και του πλαισίου της

ΠΕΡΙΓΡΑΦΗ ΕΠΕΞΕΡΓΑΣΙΑΣ: Ανάλυση οφειλών πολιτών προς το Δήμο	
Προσωπικά δεδομένα προς επεξεργασία	Προσωπικά στοιχεία (όνομα, επίθετο, φύλο, ηλικία, διεύθυνση, τηλέφωνο), ΑΦΜ, περιουσιακή κατάσταση, οικονομικά στοιχεία οφειλών, στοιχεία εισοδήματος, δεδομένα υγείας
Σκοπός επεξεργασίας	Ανάλυση των οφειλών των δημοτών και κατηγοριοποίησή τους βάσει συγκεκριμένων κριτηρίων
Υποκείμενο δεδομένων	Το σύνολο των δημοτών του φορέα
Μέσα επεξεργασίας	Εξωτερικός συνεργάτης
Παραλήπτες δεδομένων	Δήμος
Που λαμβάνει χώρα η επεξεργασία	Εξωτερικά, στις εγκαταστάσεις του Εξωτερικού Συνεργάτη

Βήμα_2: Αξιολόγηση Επιπτώσεων

Η αξιολόγηση των Επιπτώσεων κατά την Απώλεια της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας των πληροφοριών, είναι ακριβώς η ίδια με την αξιολόγηση που προηγήθηκε προηγουμένως (στο Βήμα_2 της παραγράφου 3.3.1), όταν θεωρήθηκε ότι η επεξεργασία θα λάβει χώρα εντός του φορέα. Επομένως ο πίνακας που συνοψίζει την εκτίμηση των επιπτώσεων είναι ο παρακάτω.

ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ (ΙΙ)		
Εμπιστευτικότητα	**Ακεραιότητα**	**Διαθεσιμότητα**
ΠΟΛΥ ΥΨΗΛΗ	ΥΨΗΛΗ	ΥΨΗΛΗ
Συνολική Αξιολόγηση Επιπτώσεων:		**ΠΟΛΥ ΥΨΗΛΗ**

Ως Συνολική Αξιολόγηση των επιπτώσεων καθορίζεται το υψηλότερο επίπεδο διαβάθμισης που εντοπίστηκε. Επομένως, ο συνολικός αντίκτυπος και σε αυτή την περίπτωση εκτιμάται ως **ΠΟΛΥ ΥΨΗΛΟΣ**.

Βήμα_3: Πιθανότητα εμφάνισης Απειλών

Στο βήμα αυτό θα αποτυπωθούν ξανά οι απειλές που σχετίζονται με το συνολικό περιβάλλον της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, αλλά αυτή τη

φορά θα ληφθεί υπόψη ότι η επεξεργασία λαμβάνει χώρα σε έναν οργανισμό που ακολουθεί το πρότυπο ασφάλειας πληροφοριών ISO27001.

Δίκτυο & Τεχνικοί Πόροι:

Για να αξιολογηθεί η πιθανότητα εμφάνισης απειλής μέσω Δικτύου και Τεχνικών πόρων, πρέπει να απαντηθούν τα εξής ερωτήματα:

1. ***Πραγματοποιείται οποιοδήποτε μέρος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω του διαδικτύου;***

   Η πλειοψηφία των δεδομένων που θα επεξεργαστούν είναι ψηφιακά και καταχωρημένα σε πληροφοριακό σύστημα. Το σύστημα είναι προσβάσιμο διαδικτυακά για απομακρυσμένη επεξεργασία των δεδομένων από εξουσιοδοτημένα άτομα μέσω αποκλειστικής χρήσης προσωπικών κωδικών πρόσβασης. Η απομακρυσμένη επεξεργασία εκτελείται επικουρικά και δεν αποτελεί τον κύριο τρόπο επεξεργασίας των δεδομένων. Οι πολιτικές "Ασφάλειας Ασύρματης Επικοινωνίας", "Ασφάλειας Δικτύου" και "Χρήσης Internet" του ISO27001 που κατέχει ο συνεργάτης περιγράφουν τις διαδικασίες πρόσβασης μέσω διαδικτύου.

2. ***Είναι δυνατή η παροχή πρόσβασης σε εσωτερικό αρχείο δεδομένων προσωπικού χαρακτήρα μέσω του διαδικτύου;***

   Η απομακρυσμένη πρόσβαση στο σύστημα και τα δεδομένα είναι επιτρεπτή μόνο σε εξουσιοδοτημένους χρήστες και γίνεται μέσω κωδικών πρόσβασης όπως περιγράφεται στις πολιτικές "Ασφάλειας Ασύρματης Επικοινωνίας", "Ασφάλειας Δικτύου" και "Χρήσης Internet" κατά το ISO27001 του συνεργάτη. Επομένως η πρόσβαση σε εσωτερικά αρχεία δεδομένων μέσω διαδικτύου είναι εφικτή.

3. ***Είναι το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα διασυνδεδεμένο με άλλο εξωτερικό ή εσωτερικό πληροφοριακό σύστημα ή υπηρεσία;***

   Γενικά η ύπαρξη διασύνδεσης με τρίτα συστήματα και υπηρεσίες, πάντα ενέχει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης λόγω πιθανών τρωτών σημείων στα πληροφοριακά συστήματα. Το συγκεκριμένο πληροφοριακό σύστημα μπορεί

να αλληλοεπιδράσει και με τρίτα συστήματα ή υπηρεσίες (κόμβοι διαλειτουργικότητας GovHub και ΑΑΔΕ) μέσω WebServices.

4. ***Μπορούν μη εξουσιοδοτημένα άτομα να έχουν εύκολα πρόσβαση στο περιβάλλον του συστήματος επεξεργασίας δεδομένων;***

   Πρόσβαση στο σύστημα επεξεργασίας έχει το σύνολο των ατόμων στο οποίο έχει δοθεί η αντίστοιχη πρόσβαση. Η είσοδος γενικά στις εγκαταστάσεις του συνεργάτη, γίνεται μέσω συστήματος ταυτοποίησης (ID Badges) το οποίο επιτρέπει την πρόσβαση του χρήστη, μόνο σε συγκεκριμένους χώρους, ανάλογα την αρμοδιότητά του. Η είσοδος στο σύστημα επεξεργασίας των δεδομένων γίνεται μέσω ισχυρού κωδικού πρόσβασης. Πάντα όμως το φυσικό περιβάλλον είναι μια πολύ σημαντική πτυχή της ασφάλειας, που αν δε διασφαλιστεί επαρκώς μπορεί να θέσει σε κίνδυνο οποιαδήποτε επεξεργασία. Ο κίνδυνος επομένως μη εξουσιοδοτημένης πρόσβασης ενέχει πάντα, με την "Πολιτική Φυσικής Ασφάλειας" κατά ISO27001 του συνεργάτη να τον περιορίζει.

5. ***Το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα έχει σχεδιαστεί, υλοποιηθεί ή συντηρείται χωρίς να ακολουθεί τις σχετικές βέλτιστες πρακτικές;***

   Στις εγκαταστάσεις του εξωτερικού συνεργάτη, θεωρείται ότι το υλικό είναι βέλτιστα συντηρημένο και η πιθανότητα αστοχίας του περιορισμένες, καθώς ακολουθούνται οι πολιτικές ISO27001 ως προς την "Προστασία Hardware–Δεδομένων" και τον "Έλεγχο Τεχνικής Συμμόρφωσης". Ο κίνδυνος βέβαια αστοχίας του υλικού, είναι ένας παράγοντας που δε μπορεί να εξαλειφθεί.

Συνολικά επομένως, η πιθανότητα εμφάνισης απειλής είναι **ΥΨΗΛΗ**, καθώς: α) το σύστημα επεξεργασίας είναι προσβάσιμο διαδικτυακά, β) η φυσική παρουσία μη εξουσιοδοτημένου χρήστη δε μπορεί να αποκλειστεί και γ) η απομακρυσμένη πρόσβαση σε αυτό, έστω και από εξουσιοδοτημένα άτομα, ομοίως δε μπορεί να αποκλειστεί.

Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων:

Για την αξιολόγηση της πιθανότητας απειλής σε αυτόν τον τομέα πρέπει να απαντηθούν τα εξής ερωτήματα:

1. ***Είναι οι ρόλοι και οι ευθύνες όσον αφορά την επεξεργασία των προσωπικών δεδομένων σαφώς καθορισμένοι;***

   Εφόσον ο εκτελών την επεξεργασία έχει υιοθετήσει πολιτικές ασφάλειας για: α) τη "Διαχείριση Ασφάλειας σε Συμφωνίες με Πελάτες", β) την "Ασφάλεια Δεδομένων Προσωπικού Χαρακτήρα" και γ) τη "Συλλογή Χρήσης και Επεξεργασίας Προσωπικών Δεδομένων Πελατών", θεωρείται ότι οι ρόλοι και ευθύνες σχετικά με την επεξεργασία των προσωπικών δεδομένων είναι σαφώς καθορισμένοι.

2. ***Είναι σαφώς καθορισμένο το ποιος θα κάνει χρήση του δικτύου, του συστήματος και των φυσικών πόρων εντός του οργανισμού που εκτελείται η επεξεργασία;***

   Χρήση του δικτύου θεωρείται ότι θα γίνεται μόνο από εξουσιοδοτημένα άτομα, όπως αυτά καθορίζονται στην πολιτική προστασίας για τη Διαχείριση Πρόσβασης Χρηστών.

3. ***Επιτρέπεται στους εργαζόμενους να φέρνουν και να χρησιμοποιούν τις δικές τους συσκευές για να συνδεθούν στο σύστημα επεξεργασίας των προσωπικών δεδομένων;***

   Η πολιτική ασφάλειας α) "Ασύρματης Επικοινωνίας", β) "Δικτύου" και γ) "Αφαιρούμενων Αποθηκευτικών Μέσων", αποτρέπει τη σύνδεση και χρήση στο σύστημα επεξεργασίας, συσκευών που δεν ανήκουν στον εξοπλισμό του συνεργάτη

4. ***Επιτρέπεται στους εργαζόμενους να μεταφέρουν, να αποθηκεύουν ή να επεξεργάζονται με άλλο τρόπο δεδομένα προσωπικού χαρακτήρα εκτός των εγκαταστάσεων του οργανισμού;***

   Η πολιτική ασφάλειας "Αφαιρούμενων Αποθηκευτικών Μέσων", αποτρέπει την αποθήκευση δεδομένων σε φορητές μονάδες αποθήκευσης και περιορίζει την πιθανότητα μεταφοράς τους εκτός των εγκαταστάσεων του οργανισμού. Ο κίνδυνος αυτός όμως δε μπορεί να εξαλειφθεί σε περίπτωση κακόβουλης

ενέργειας, καθώς εξακολουθεί να υπάρχει δυνατότητα μεταφοράς κάποιων δεδομένων για παράδειγμα μέσω email. Επίσης, η δυνατότητα απομακρυσμένης πρόσβασης στο σύστημα επεξεργασίας μέσω διαδικτύου, δε μπορεί να αποκλείσει την περίπτωση μεταφοράς κάποιων δεδομένων εκτός του οργανισμού που εκτελείται η επεξεργασία

5. ***Μπορούν οι δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα να διεξάγονται χωρίς δημιουργία αρχείων καταγραφής;***
   Η σύνδεση οποιουδήποτε χρήστη στο σύστημα επεξεργασίας, απαιτεί σύνδεση με προσωπικούς κωδικούς, επομένως η απαίτηση ύπαρξης πολιτικής ασφάλειας α) "Ασύρματης Επικοινωνία", β) "Δικτύου" και γ) "Διαχείρισης πρόσβασης χρηστών", περιορίζει την απειλή μέσω των μηχανισμών καταγραφής (logging) και παρακολούθησης (monitoring)

Η πιθανότητα εμφάνισης απειλής είναι **ΜΕΤΡΙΑ**, καθώς ναι μεν οι προαπαιτούμενες πολιτικές ασφάλειας περιορίζουν τον κίνδυνο ως προς τον μη σωστό καθορισμό ρόλων και αρμοδιοτήτων, εξακολουθεί όμως να υπάρχει ο κίνδυνος μεταφοράς δεδομένων εκτός οργανισμού.

Τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας:
Για την αξιολόγηση της πιθανότητας απειλής σε αυτόν τον τομέα πρέπει να απαντηθούν τα εξής ερωτήματα:

1. ***Πραγματοποιείται η επεξεργασία δεδομένων προσωπικού χαρακτήρα από μη καθορισμένο αριθμό υπαλλήλων;***
   Όταν η πρόσβαση και επεξεργασία των προσωπικών δεδομένων είναι ανοικτή σε μεγάλο αριθμό ατόμων, τότε αυξάνονται και οι πιθανότητες παραβίασής τους, λόγω του ανθρώπινου παράγοντα. Στη συγκεκριμένη επεξεργασία δεν καθορίζεται με σαφήνεια το ποια άτομα χρειάζεται πραγματικά να έχουν πρόσβαση στα δεδομένα και την επεξεργασία.

2. ***Εκτελείται οποιοδήποτε μέρος της διαδικασίας επεξεργασίας δεδομένων από εργολάβο/συνεργάτη (εκτελών την επεξεργασία δεδομένων);***

Το σύνολο της επεξεργασίας υλοποιείται από εξωτερικό συνεργάτη. Όταν η επεξεργασία πραγματοποιείται από τρίτους, ο φορέας μπορεί να χάσει εν μέρει τον έλεγχο αυτών των δεδομένων. Είναι πολύ σημαντικό για το φορέα να επιλέγει αναδόχους που μπορούν να προσφέρουν υψηλό επίπεδο ασφάλειας και να καθορίζει από την αρχή και με σαφήνεια ποιο μέρος της επεξεργασίας ανατίθεται σε αυτούς, διατηρώντας ο ίδιος ένα υψηλό επίπεδο ελέγχου στη διαδικασία.

3. ***Είναι οι υποχρεώσεις των μερών που εμπλέκονται στην επεξεργασία δεδομένων σαφώς καθορισμένες;***
   Οι υποχρεώσεις του εκτελούντος την επεξεργασία είναι σαφώς καθορισμένες στη σύμβαση που συνάπτεται μεταξύ φορέα και εξωτερικού συνεργάτη. Όταν ο εκτελών την επεξεργασία δε έχει ενημερωθεί με σαφήνεια για τις υποχρεώσεις του, οι απειλές της κοινοποίησης των δεδομένων και της καταστροφής πολλές φορές σημαντικά αυξάνονται.

4. ***Είναι το προσωπικό που εμπλέκεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα εξοικειωμένο με θέματα ασφάλειας πληροφοριών;***
   Καθώς η επιλογή του συνεργάτη έχει γίνει με κριτήριο την ύπαρξη πιστοποίησης ISO27001, θεωρείται ότι το προσωπικό του είναι εξοικειωμένο με θέματα ασφάλειας πληροφοριών και κατάλληλα εκπαιδευμένο.

5. ***Τα πρόσωπα/μέρη που εμπλέκονται στην επεξεργασία δεδομένων αμελούν να αποθηκεύουν ή/και να καταστρέφουν με ασφάλεια τα δεδομένα προσωπικού χαρακτήρα;***
   Ο κίνδυνος απώλειας της ακεραιότητας των προσωπικών δεδομένων, από αμέλεια τήρησης για παράδειγμα αντιγράφου ασφαλείας, είναι πιθανή. Επίσης πιθανός είναι και ο κίνδυνος παραβίασης των προσωπικών δεδομένων λόγω έλλειψης μέτρων φυσικής προστασίας, όπως για παράδειγμα κλείδωμα του φυσικού αρχείου σε ερμάρια

Η πιθανότητα εμφάνισης απειλής είναι **ΥΨΗΛΗ**, καθώς υπάρχουν παράγοντες κινδύνου που δε μπορούν να περιοριστούν με κάποιο από τα μέτρα που έχουν παρθεί εξ αρχής.

Τομέας & Κλίμακα επεξεργασίας:

Για την αξιολόγηση της πιθανότητας απειλής σε αυτόν τον τομέα πρέπει να απαντηθούν τα εξής ερωτήματα:

1. ***Θεωρείτε ότι ο τομέας που δραστηριοποιείται ο φορέας είναι επιρρεπής σε κυβερνοεπιθέσεις;***

   Δεν είναι γνωστές περιπτώσεις εντός της Ελλάδας που να έχουν πραγματοποιηθεί κυβερνοεπιθέσεις ασφάλειας εν γένει στον τομέα των εταιρειών που δραστηριοποιούνται στην ανάπτυξη συστημάτων πληροφορικής. Παρόλα αυτά, ο οργανισμός στο πλαίσιο πιστοποίησης κατά ISO27001 έχει προβλέψει και ακολουθεί συγκεκριμένες πολιτικές προστασίας από κυβερνοεπιθέσεις

2. ***Έχει υποστεί ο φορέας οποιαδήποτε κυβερνοεπίθεση ή άλλου είδους παραβίαση της ασφάλειας τα τελευταία δύο χρόνια;***

   Ο οργανισμός δεν έχει υποστεί κάποιο σοβαρό περιστατικό κυβερνοεπίθεσης τα τελευταία δύο χρόνια. Η πιο συνηθισμένη απειλή είναι τα fishing emails τα οποία αποτρέπονται από το εγκατεστημένο λογισμικό προστασίας της ηλεκτρονικής αλληλογραφίας

3. ***Έχετε λάβει οποιεσδήποτε κοινοποιήσεις ή/και καταγγελίες σχετικά με την ασφάλεια του πληροφοριακού συστήματος που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων κατά το τελευταίο έτος;***

   Ο οργανισμός δεν έχει λάβει κάποια καταγγελία σχετικά με την ασφάλεια των πληροφοριακών του συστημάτων το τελευταίο έτος.

4. ***Θεωρείται η συγκεκριμένη επεξεργασία, επεξεργασία δεδομένων μεγάλης κλίμακας;***

   Η συγκεκριμένη επεξεργασία, θεωρείται επεξεργασία μεγάλης κλίμακας, καθώς αφορά προσωπικά και ευαίσθητα δεδομένα μεγάλου Δήμου της ελληνικής επικράτειας.

5. ***Υπάρχουν βέλτιστες πρακτικές ασφάλειας για τον συγκεκριμένο τομέα υπηρεσιών που δεν έχουν ακολουθηθεί επαρκώς;***

Ένα επιπλέον μέτρο ασφάλειας για τον οργανισμό, εκτός από το ISO27001 στο οποίο είναι ήδη πιστοποιημένος, θα ήταν και η συμμόρφωση ως προς τις απαιτήσεις του ΓΚΠΔ

Η πιθανότητα εμφάνισης απειλής είναι **ΜΕΤΡΙΑ**, καθώς αφορά ναι μεν σε μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων, αλλά ο κλάδος δραστηριοποίησης του οργανισμού, δε θεωρείται επιρρεπής σε κυβερνοεπιθέσεις. Αυτό από μόνο του βέβαια, δε μπορεί να εκμηδενίσει την πιθανότητα να συμβεί ένα περιστατικό κυβερνοεπίθεσης.

ΤΟΜΕΑΣ ΑΞΙΟΛΟΓΗΣΗ	**ΠΙΘΑΝΟΤΗΤΑ**	
	Διαβάθμιση	**SCORE**
Δίκτυο & Τεχνικοί Πόροι	☐ Χαμηλή	1
	☐ Μέτρια	2
	☒Υψηλή	3
Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων	☐ Χαμηλή	1
	☒ Μέτρια	2
	☐Υψηλή	3
Τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας	☐ Χαμηλή	1
	☐ Μέτρια	2
	☒Υψηλή	3
Τομέας & Κλίμακα επεξεργασίας	☐ Χαμηλή	1
	☒ Μέτρια	2
	☐Υψηλή	3
Συνολικό Άθροισμα Πιθανότητας Εμφάνισης Απειλής		**10**

Ακολουθώντας το πρότυπο ENISA, η πιθανότητα εμφάνισης απειλής συνολικά, χαρακτηρίζεται ως **ΥΨΗΛΗ**.

Συνολικό Άθροισμα Πιθανότητας Εμφάνισης Απειλής	**Επίπεδο Πιθανότητας Εμφάνισης Απειλής**
4 - 5	Χαμηλό
6 - 8	Μέτριο
9 - 12	Υψηλό

Βήμα_4: Αξιολόγηση Κινδύνου

Βάσει της αξιολόγησης που πραγματοποιήθηκε στα δύο προηγούμενα βήματα, ο συνολικός κίνδυνος για τη συγκεκριμένη περίπτωση θεωρείται Υψηλός.

		Επίπεδο Επίπτωσης		
		Χαμηλό	***Μέτριο***	***Υψηλό***
Πιθανότητα Εμφάνισης Απειλής	***Χαμηλό***			
	Μέτριο			
	Υψηλό			☒

Βήμα_5: Υιοθέτηση Μέτρων Ασφάλειας

Προκειμένου να περιοριστούν σε αποδεκτά επίπεδα οι προαναφερθείσες απειλές, ο Υπεύθυνος Επεξεργασίας θεωρεί ότι η υιοθέτηση των μέτρων που ακολουθούν θα επιφέρουν τα βέλτιστα αποτελέσματα.

#	*Απειλή*	*Μέθοδος Αντιμετώπισης*	*Δείκτης Παρακολούθησης*	*Στρατηγική Αντιμετώπισης*
1	*Διαδικτυακή πρόσβαση μη εξουσιοδοτημένου χρήστη*	*Αποφυγή*	*Monitoring της κίνησης προς το διαδίκτυο*	*Αφαίρεση της πρόσβασης στο διαδίκτυο από servers και τερματικά που επεξεργάζονται προσωπικά δεδομένα*
2	*Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου - email)*			
3	*Πρόσβαση στο σύστημα επεξεργασίας μη εξουσιοδοτημένου χρήστη*	*Πρόληψη*	*Καταγραφή πρόσβασης στα Log files*	*Αυθεντικοποίηση δύο παραγόντων κατά την πρόσβαση στο σύστημα του οργανισμού*
4	*Απώλεια εμπιστευτικότητας των δεδομένων, λόγω πρόσβασης μη εξουσιοδοτημένου χρήστη*	*Πρόληψη*	*Ισχυρός αλγόριθμος κρυπτογράφησης*	*Πλήρης κρυπτογράφηση δεδομένων στο δίσκο που βρίσκονται αποθηκευμένα τα προσωπικά δεδομένα*
5	*Φυσική πρόσβαση στο χώρο επεξεργασίας μη εξουσιοδοτημένου χρήστη*	*Πρόληψη*	*Συχνός έλεγχος στους χώρους επεξεργασίας για αρχεία που είναι εκτεθειμένα σε μη εξουσιοδοτημένους χρήστες*	*Φύλαξη του φυσικού αρχείου σε ερμάρια που ασφαλίζουν με κλειδαριές*

6	*Απώλεια ακεραιότητας των δεδομένων λόγω αμέλειας τήρησης αντιγράφων ασφαλείας*	*Αποφυγή*	*Καθημερινός έλεγχος ορθότητας του αντιγράφου ασφαλείας*	*Αυτοματοποιημένο σύστημα δημιουργίας αντιγράφων ασφαλείας*
7	*Απώλεια εμπιστευτικότητας και ακεραιότητας των δεδομένων, λόγω εμπλοκής μεγάλου αριθμού χρηστών*	*Πρόληψη*	*Καταγραφή πρόσβασης σε log files των*	*Σαφής καθορισμός εξ' αρχής του πλήθους των ατόμων που θα συμμετέχουν στην επεξεργασία*
8	*Απώλεια ελέγχου της ροής στη διαδικασία της επεξεργασίας, λόγω ανάθεσής της σε εξωτερικό συνεργάτη*	*Αποφυγή*	*Καθημερινή αναφορά από το συνεργάτη προς το φορέα στην οποία θα καταγράφεται το σύνολο των ενεργειών που πραγματοποιήθηκαν και τα αποτελέσματα*	*Καθορισμός στη σύμβαση του τρόπου παρακολούθησης της διαδικασίας από τον Υπεύθυνο Επεξεργασίας*
9	*Κυβερνοεπίθεση*	*Πρόληψη*	*Monitoring της εισερχόμενης προς το δίκτυο κίνησης μέσω διαδικτύου*	*Εγκατάσταση ειδικού λογισμικού παρακολούθησης του δικτύου*

Κεφάλαιο 4
Εκτίμηση αντικτύπου ως προς την προστασία δεδομένων

Μέσω της αυτόνομης μεθοδολογίας ENISA για τον εντοπισμό και τη διαχείριση κινδύνων ασφάλειας, μπορούν να προκύψουν τα τρωτά σημεία σε θέματα ασφαλείας μιας επεξεργασίας, τα οποία μπορούν να χρησιμοποιηθούν στη συνέχεια για την εκπόνηση της Μελέτης Εκτίμησης Αντικτύπου ως προς την προστασία των προσωπικών δεδομένων. Σαν εργαλείο για την διενέργεια της ΕΑ, μεταξύ των υπαρχόντων λογισμικών, επιλέχθηκε να χρησιμοποιηθεί το εργαλείο PIA της Γαλλικής Αρχής Προστασίας Δεδομένων CNIL και να ακολουθηθεί η ροή που προτείνεται μέσα από αυτό. Ο λόγος που επιλέχθηκε το εν λόγω λογισμικό, είναι επειδή πρόκειται για λογισμικό ανοιχτού κώδικα κατασκευασμένο από μια ανεξάρτητη κρατική αρχή, το οποίο προσφέρει πολλά εργαλεία οπτικοποίησης για την κατανόηση των κινδύνων και των επιπτώσεών τους. Επίσης, το λογισμικό PIA, περιλαμβάνει το σύνολο των νομικών σημείων που διασφαλίζουν τη νομιμότητα της επεξεργασίας και τα δικαιώματα των υποκειμένων των δεδομένων, σε όλα τα βήματα της μελέτης ΕΑ.

4.1 Διενέργεια Εκτίμησης Αντικτύπου με την εφαρμογή PIA της CNIL

4.1.1 Γενικό Πλαίσιο

Ποια είναι η υπό εξέταση επεξεργασία;

Μεγάλος Δήμος της ελληνικής επικράτειας αποφασίζει να προχωρήσει σε επεξεργασία του συνόλου των δεδομένων των συναλλασσόμενων που τηρούνται στα αρχεία του

(ψηφιακά και φυσικά) και που έχουν ληξιπρόθεσμες οφειλές, προκειμένου να τους κατηγοριοποιήσει ως προς συγκεκριμένα κριτήρια βάσει των οποίων θα εφαρμοσθούν και συγκεκριμένα μέτρα είσπραξης (αποστολή οφειλών στη ΔΟΥ, δέσμευση τραπεζικών λογαριασμών κα). Τα κριτήρια που έχουν επιλεχθεί, αφορούν: το ύψος και το είδος της οφειλής, αν η οφειλή αφορά φυσικό ή νομικό πρόσωπο, την ηλικιακή ομάδα των οφειλετών, την οικογενειακή τους κατάσταση και εισοδηματικά κριτήρια. Η συγκεκριμένη επεξεργασία πραγματοποιείτε από ανάδοχο συνεργάτη εκτός των εγκαταστάσεων του Δήμου.

Ποια είναι οι ευθύνες που συνδέονται με την επεξεργασία;

Οι ευθύνες που συνδέονται με την επεξεργασία μπορούν να διαχωριστούν σε δύο μέρη. Στις ευθύνες του Υπεύθυνου Επεξεργασίας και στις ευθύνες του Εκτελούντος την Επεξεργασία.

Για τον Υπεύθυνο Επεξεργασίας, δηλαδή το φορέα (Δήμος), οι ευθύνες που συνδέονται με την επεξεργασία είναι οι εξής:

- ✓ Να μεριμνά για την τήρηση των υποχρεώσεων που απορρέουν από το κανονιστικό πλαίσιο και τις ειδικότερες εθνικές νομικές διατάξεις σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα
- ✓ Να διενεργεί πριν την επεξεργασία, μελέτη εκτίμηση των επιπτώσεων των σχεδιαζόμενων ενεργειών
- ✓ Να παρακολουθεί καθ' όλη τη διάρκεια της επεξεργασίας, αν τηρούνται τα μέτρα προστασίας που θα διασφαλίσουν την ακεραιότητα των δεδομένων
- ✓ Να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό
- ✓ Να εφαρμόζει κατάλληλες πολιτικές προστασίας των προσωπικών δεδομένων

Για τον Εκτελούντα την Επεξεργασία (εξωτερικός συνεργάτης/ανάδοχος), οι ευθύνες που συνδέονται με την επεξεργασία είναι οι εξής:

- ✓ Να ενεργεί σε κάθε πράξη επεξεργασίας κατ’ εντολή του υπεύθυνου επεξεργασίας

- ✓ Να εξασφαλίζει ότι η επεξεργασία διενεργείται σύμφωνα με τις απαιτήσεις των κανονισμών
- ✓ Να διασφαλίζει την προστασία των δικαιωμάτων των υποκειμένων
- ✓ Να παρέχει στον υπεύθυνο επεξεργασίας όλες τις απαραίτητες πληροφορίες

Υπάρχουν πρότυπα που ισχύουν για την επεξεργασία;

Δεν υπάρχουν πρότυπα πιστοποίησης κατά το άρθρο 43 του GDPR, αλλά υπάρχει πρότυπο συμμόρφωσης ως προς το ISO 27001 για την προστασία των πληροφοριών.

Ποια προσωπικά δεδομένα υφίστανται επεξεργασία;

Στην περίπτωση που μελετάμε, υφίστανται επεξεργασία προσωπικά δεδομένα πολιτών, τα οποία είναι:

- ✓ Ονοματεπώνυμο
- ✓ Φύλο
- ✓ Διεύθυνση κατοικίας
- ✓ Τηλεφωνικός αριθμός
- ✓ Ημερομηνία γέννησης
- ✓ ΑΦΜ
- ✓ Διεύθυνση ηλεκτρονικού ταχυδρομείου
- ✓ Οικονομικά δεδομένα οφειλών προς το δήμο
- ✓ Περιουσιακά δεδομένα (Ε9)
- ✓ Στοιχεία εισοδήματος
- ✓ Δεδομένα υγείας

Πώς λειτουργεί ο κύκλος ζωής των δεδομένων και των διαδικασιών;

Τα προσωπικά δεδομένα συλλέγονται από το Δήμο και αποθηκεύονται είτε στο πληροφοριακό του σύστημα (η πλειοψηφία των δεδομένων) είτε ως φυσικό αρχείο. Ο εκτελών την επεξεργασία θα αντλήσει τα δεδομένα από το πληροφοριακό σύστημα, αλλά και από το φυσικό αρχείο όπου κρίνεται απαραίτητο. Η πληροφορία που προέρχεται από το φυσικό αρχείο και είναι απαραίτητη για την επεξεργασία, θα καταχωρηθεί και θα αποθηκευτεί στο σύστημα. Η επεξεργασία των δεδομένων γίνεται μέσω του ίδιου του πληροφοριακού συστήματος. Σε περίπτωση που υπάρχουν ελλιπή δεδομένα, ο ανάδοχος ενημερώνει τον υπεύθυνο επεξεργασίας, ο οποίος καλείται να αναζητήσει τα επιπλέον

στοιχεία απευθείας από τα υποκείμενα ή μέσω τρίτων συστημάτων (κόμβοι διαλειτουργικότητας) στα οποία έχει πρόσβαση σαν δημόσιος φορέας. Τα επιπλέον στοιχεία που έχει συλλέξει ο υπεύθυνος επεξεργασίας, τα αποστέλλει με ηλεκτρονική μορφή (excel) συγκεκριμένης γραμμογράφησης στον ανάδοχο, προκειμένου να εισαχθούν τα δεδομένα στο σύστημα. Αφού ολοκληρωθεί η επεξεργασία, δημιουργούνται αναφορές που αποθηκεύονται στο σύστημα (ως εγγραφές στη βάση δεδομένων), αλλά και αποστέλλονται στο Δήμο με μορφή excel. Η πληροφορία που έχει δημιουργηθεί σαν αποτέλεσμα της επεξεργασίας, παραμένει στο σύστημα για όσο διάστημα απαιτεί η κείμενη νομοθεσία.

Ποια είναι τα στοιχεία που υποστηρίζουν τα δεδομένα;

Το λειτουργικό σύστημα στο οποίο πραγματοποιείται η επεξεργασία είναι Microsoft Windows 10. Η βάση δεδομένων του Δήμου είναι Oracle, ενώ η εφαρμογή λογισμικού που θα χρησιμοποιηθεί για την διεκπεραίωση της επεξεργασίας, είναι γραμμένη σε Sybase Powerbuilder 2017. Η σύνδεση στη βάση δεδομένων για την εκτέλεση ερωτημάτων (queries) ή την εισαγωγή δεδομένων που προέρχονται από το φυσικό αρχείο, γίνεται μέσω των εργαλείων Sybase Infomaker ή Quest Toad for Oracle. Δεδομένα της βάσης μπορεί να εξαχθούν και να επεξεργαστούν τοπικά σε υπολογιστές του δικτύου του εξωτερικού συνεργάτη, στη σουίτα Office της Microsoft (Excel)

4.1.2 Θεμελιώδεις Αρχές

Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;

Ο σκοπός της επεξεργασίας, δηλαδή η εφαρμογή μέτρων είσπραξης για τις ληξιπρόθεσμες οφειλές προς το δήμο, είναι απόλυτα σαφής, καθώς αποτελεί νόμιμο τρόπο είσπραξης οφειλών από την ταμειακή υπηρεσία του δήμου

Ποια είναι η νομική βάση που καθιστά την επεξεργασία νόμιμη;

Στο Άρθρο 6 παρ.1 στοιχ. γ' του GDPR αναφέρεται ότι: "*η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας*". Ειδικότερα, η εφαρμογή μέτρων είσπραξης για ανείσπρακτες ληξιπρόθεσμες οφειλές προς τους δήμους, αποτελεί μέρος του νομοθετικού διατάγματος Αριθ. 356 'Περί Κώδικος Εισπράξεως Δημοσίων Εσόδων'

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»);

Τα προσωπικά δεδομένα που παραχωρούνται στον ανάδοχο για επεξεργασία είναι επαρκή, συναφή και απολύτως απαραίτητα εν όψει του επιδιωκόμενου σκοπού, ο οποίος δε μπορεί να υλοποιηθεί με λιγότερα μέσα.

Τα δεδομένα είναι ακριβή και ενημερωμένα;

Προκειμένου να διασφαλιστεί η ποιότητα των δεδομένων, ο Δήμος καλείται να κοινοποιήσει στο συνεργάτη τα τελευταία επικυρωμένα δεδομένα του Δήμου (το backup με τις πιο επικαιροποιημένες μεταβολές). Αν βρεθούν ανακριβή στοιχεία (για παράδειγμα λάθος ΑΦΜ ή ΑΔΤ) μπορούν να ελεγχθούν βάσει της διασύνδεσης με τον κόμβο διαλειτουργικότητας

Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;

Επειδή πρόκειται για περίπτωση όπου η επεξεργασία των προσωπικών δεδομένων γίνεται βάσει έννομης υποχρέωσης, ο χρόνος τήρησης αυτών καθορίζεται με βάση τις επιταγές της νομοθεσίας, το χρονικό διάστημα κατά το οποίο μπορούν να διενεργηθούν έλεγχοι από τις αρμόδιες αρχές, τις προβλεπόμενες παραγραφές, αλλά και τα έννομα συμφέροντα του υποκειμένου των δεδομένων.

Πώς ενημερώνονται τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία;

Τα υποκείμενα των δεδομένων ενημερώνονται για την επεξεργασία μέσω ανακοινώσεων (ιστοσελίδα δήμου, πίνακας ανακοινώσεων κλπ.), αλλά και απ' ευθείας από τον υπεύθυνο επεξεργασίας, στην περίπτωση που αναζητηθούν επιπλέον δεδομένα

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

Καθώς νομική βάση της επεξεργασίας είναι η έννομη υποχρέωση του Δήμου για αναζήτηση τρόπων είσπραξης των ληξιπρόθεσμων οφειλών, δεν απαιτείται να αναζητηθεί η συγκατάθεση του συνόλου των υποκειμένων.

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

Στη συγκεκριμένη επεξεργασία, δεν έχει εφαρμογή το δικαίωμα της φορητότητας. Το υποκείμενα όμως, μπορούν να ασκήσουν το δικαίωμα της πρόσβασης των προσωπικών τους δεδομένων ανά πάσα στιγμή, με ανάλογο αίτημα προς το Δήμο, προκειμένου να λάβουν επιβεβαίωση αναφορικά με την επεξεργασία των δεδομένων τους. Η διαδικασία υποβολής των αιτημάτων γίνεται μόνο γραπτώς χρησιμοποιώντας συγκεκριμένο έντυπο "Αίτηση Άσκησης Δικαιωμάτων Υποκειμένων" και τα σχετικά αιτήματα αρχειοθετούνται για λόγους τεκμηρίωσης. Ο υπεύθυνος επεξεργασίας, προκειμένου να διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων, έχει προβλέψει η διαδικασία της αίτησης να μπορεί να γίνει είτε με φυσική παρουσία στο Δήμο, είτε ηλεκτρονικά με email, είτε μέσω αυτοματοποιημένης φόρμας υποβολής στην ιστοσελίδα του Δήμου.

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

Τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματα της διόρθωσης και διαγραφής ανά πάσα στιγμή, με έγγραφο αίτημα προς το Δήμο, το οποίο θα αξιολογηθεί και θα απαντηθεί. Η διαδικασία υποβολής των αιτημάτων γίνεται μόνο γραπτώς χρησιμοποιώντας συγκεκριμένο έντυπο "Αίτηση Άσκησης Δικαιωμάτων Υποκειμένων" και τα σχετικά αιτήματα αρχειοθετούνται για λόγους τεκμηρίωσης. Ο υπεύθυνος επεξεργασίας, προκειμένου να διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων, έχει προβλέψει η διαδικασία της αίτησης να μπορεί να γίνει είτε με φυσική παρουσία στο Δήμο, είτε ηλεκτρονικά με email, είτε μέσω αυτοματοποιημένης φόρμας υποβολής στην ιστοσελίδα του Δήμου.

Το δικαίωμα στη διόρθωση αφορά κάθε περίπτωση για την οποία το υποκείμενο αντιληφθεί ότι τα δεδομένα είναι ανακριβή ή ελλιπή. Ο Δήμος θα προβεί σε έλεγχο και σε περίπτωση διόρθωσης θα ενημερωθούν τα εμπλεκόμενα μέρη.

Το δικαίωμα στη διαγραφή παρέχεται όταν τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με το σκοπό τον οποίο συλλέχθηκαν και όταν δεν υπάρχει πλέον νομική υποχρέωση διατήρησής τους.

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

Τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματα του περιορισμού και της εναντίωσης ανά πάσα στιγμή, με έγγραφο αίτημα προς το Δήμο, το οποίο θα αξιολογηθεί και θα απαντηθεί. Η διαδικασία υποβολής των αιτημάτων γίνεται μόνο γραπτώς χρησιμοποιώντας συγκεκριμένο έντυπο "Αίτηση Άσκησης Δικαιωμάτων Υποκειμένων" και τα σχετικά αιτήματα αρχειοθετούνται για λόγους τεκμηρίωσης. Ο υπεύθυνος επεξεργασίας, προκειμένου να διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων, έχει προβλέψει η διαδικασία της αίτησης να μπορεί να γίνει είτε με φυσική παρουσία στο Δήμο, είτε ηλεκτρονικά με email, είτε μέσω αυτοματοποιημένης φόρμας υποβολής στην ιστοσελίδα του Δήμου.

Η άσκηση των δικαιωμάτων του περιορισμού και της εναντίωσης παρέχεται στην περίπτωση που δεν εμποδίζει την νομική υποχρέωση του Δήμου για την επεξεργασίας τους.

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

Σύμφωνα με την παράγραφο 3 του Άρθρου 28 του ΓΚΠΔ καθορίζεται ότι: "Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας." Για την εκτέλεση της επεξεργασίας επομένως, απαιτείται να υπογραφεί σύμβαση στην οποία αναφέρονται ρητά και οι υποχρεώσεις του εκτελούντος, οι οποίες είναι:

- ✓ Να επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας
- ✓ Να διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας
- ✓ Να λαμβάνει όλα τα απαιτούμενα μέτρα δυνάμει του άρθρου 32
- ✓ Να λαμβάνει υπόψη τη φύση της επεξεργασίας και να επικουρεί τον υπεύθυνο επεξεργασίας με τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την εκπλήρωση

της υποχρέωσής του να απαντά σε αιτήματα για άσκηση των προβλεπόμενων δικαιωμάτων των υποκειμένων

- ✓ Να συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τον Κανονισμό
- ✓ Να διαγράφει ή να επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα και αντίγραφα στον υπεύθυνο επεξεργασίας μετά το πέρας της επεξεργασίας
- ✓ Να επιτρέπει και να διευκολύνει τους ελέγχους που διενεργούνται από τον υπεύθυνο επεξεργασίας

Επιπλέον, για την εκτέλεση της επεξεργασίας, απαιτείται να υπογραφεί και σύμβαση Εχεμύθειας και Εμπιστευτικότητας μεταξύ του Δήμου και του εξωτερικού συνεργάτη (ΕΤΑΙΡΕΙΑ). Στη σύμβαση αναφέρονται ρητά και προσυπογράφονται από κοινού τα εξής:

- ✓ Η Εταιρεία εφαρμόζει τις πολιτικές και διαδικασίες που τηρεί στα πλαίσια το ολοκληρωμένου συστήματος ασφάλειας που εφαρμόζει για τα δεδομένα που επεξεργάζεται
- ✓ Η Εταιρεία δεν κοινοποιεί σε τρίτους δεδομένα που της γνωστοποιούνται κατά τη διάρκεια που λαμβάνει χώρα η επεξεργασία
- ✓ Η Εταιρεία αναλαμβάνει την υποχρέωση να τηρεί, λαμβάνει ή χρησιμοποιεί εμπιστευτικά στοιχεία, μόνο στα πλαίσια εκπλήρωσης της σύμβασης και ποτέ εγκρίσεως από το Δήμο

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

Η συγκεκριμένη επεξεργασία δε λαμβάνει χώρα οποιαδήποτε μεταφορά δεδομένων εκτός Ευρωπαϊκής Ένωσης

4.1.3 Κίνδυνοι – Προγραμματισμένα ή Υπάρχοντα Μέτρα

Καταστολή κακόβουλου λογισμικού

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη “Πολιτική Antivirus” στην οποία περιγράφονται τα εξής:

- ✓ Στο σύνολο των υπολογιστικών συστημάτων της εταιρείας είναι εγκατεστημένο κατάλληλο λογισμικό και την καταστολή κακόβουλων εφαρμογών (trojan, mallware, virus)
- ✓ Η Εταιρεία εξασφαλίζει ότι όλα τα συστήματα είναι ενημερωμένα με τις τελευταίες αναβαθμίσεις ασφαλείας των εφαρμογών αυτών
- ✓ Ο Διαχειριστής Δικτύου είναι υπεύθυνος για τον τακτικό έλεγχο των μηχανημάτων για ιούς και που θα πιστοποιούν ότι τα μηχανήματα δεν είναι μολυσμένα

Ασφάλεια δικτύου - Αποφυγή επιθέσεων μέσω δικτύου

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη "Πολιτική Ασφάλειας Δικτύου" προς αποφυγή επιθέσεων όπως Denial-of-Service, Unauthorized access attacks, Password attacks, Trojan horses, Network packet sniffers. Στην πολιτική αυτή περιγράφονται τα εξής:

- ✓ Το δίκτυο της Εταιρείας προστατεύεται από κατάλληλο λογισμικό Firewall
- ✓ Για την πρόσβαση στο δίκτυο της Εταιρείας απαιτείται Έλεγχος Ταυτότητας Δύο Παραγόντων
- ✓ Η πρόσβαση σε μη ασφαλή δίκτυα είναι απαγορευμένη βάσει των πολιτικών ασφάλειας που ακολουθούνται
- ✓ Αποφυγή "single points of failure" συστημάτων

Παρακολούθηση δραστηριότητας δικτύου

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη "Πολιτική Παρακολούθησης Δικτύου" στην οποία περιγράφονται και τα εξής:

- ✓ Η δραστηριότητα του δικτύου καταγράφεται μέσω ειδικών εφαρμογών (monitoring)
- ✓ Η πρόσβαση στις υπηρεσίες καταγράφονται και ελέγχονται από τεχνολογίες όπως TCP Wrappers
- ✓ Τα security logs θα πρέπει να παραμένουν διαθέσιμα στο δίκτυο για ένα εύλογο χρονικό διάστημα
- ✓ Εφαρμογή παρακολούθησης θυρών μέσω Port Scanning και συγκεκριμένα μέσω του εργαλείου Nmap

Ασφάλεια τεχνολογικού υλικού

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη "Πολιτική Ασφάλειας Hardware-Δεδομένων" και "Πολιτική Τεχνολογικού Εξοπλισμού" στις οποίες περιγράφονται τα εξής:

- ✓ Μόνο το προσωπικό της εταιρείας διαθέτει πρόσβαση στους χώρους των σταθμών εργασίας μέσω ειδικών κλειδιών πρόσβασης (tags)
- ✓ Σε κάθε τμήμα της εταιρείας υπάρχει συναγερμός για την προστασία του εξοπλισμού
- ✓ Πρόσβαση στους χώρους που είναι τοποθετημένοι οι κεντρικοί εξυπηρετητές (computer room) έχουν μόνο εξουσιοδοτημένα άτομα
- ✓ Στους χώρους της εταιρείας όπου βρίσκεται εγκατεστημένος εξοπλισμός, ελέγχονται πλήρως οι περιβαλλοντικές συνθήκες (θερμοκρασία, υγρασία) προκειμένου να μην επηρεάζεται η λειτουργία των εγκαταστάσεων
- ✓ Για τη φυσική προστασία του hardware από απότομες διακυμάνσεις του ηλεκτρικού ρεύματος χρησιμοποιούνται UPS

Προστασία από πηγές κινδύνων πλην του ανθρώπου

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη "Πολιτική Τεχνικής Ασφάλειας" στην οποία περιγράφονται τα εξής:

- ✓ Για την προστασία και διαφύλαξη της φυσικής ασφάλειας των αρχείων και των κτηριακών εγκαταστάσεων της εταιρείας, έχουν εγκατασταθεί πυροσβεστήρες και συστήματα πυρανίχνευσης σε πολλά σημεία
- ✓ Ο εξοπλισμός στον οποίο εκτελείται η επεξεργασία, είναι εγκατεστημένος χωροταξικά με τέτοιο τρόπο έτσι ώστε αν αποφεύγονται κίνδυνοι από φυσικά αίτια (πλημμύρα, υψηλή θερμοκρασία κλπ.)
- ✓ Επίσης, στην εταιρεία έχει υλοποιηθεί σχέδιο επιχειρησιακής συνέχειας και ανάκαμψης από φυσικές καταστροφές

Συντήρηση Εξοπλισμού

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη "Πολιτική Τεχνικής Ασφάλειας" στην οποία περιγράφονται τα εξής:

- ✓ Το τεχνικό τμήμα της εταιρείας ελέγχει σε τακτά χρονικά διαστήματα τον εξοπλισμό
- ✓ Αντικαθιστά τμήματα που παρουσιάζουν αλλοιώσεις και ενθαρρύνει τους χρήστες να αναφέρουν οποιαδήποτε προβλήματα μπορεί να εμφανιστούν στον εξοπλισμό και να οδηγήσουν σε πιθανή αστοχία
- ✓ Οι έλεγχοι που πραγματοποιούνται καταγράφονται σε σχετικό έντυπο Τεχνικών Ελέγχων (Check List)
- ✓ Οι έλεγχοι περιλαμβάνουν τόσο δοκιμές ασφάλειας όσο και λειτουργικά θέματα των εφαρμογών

Έλεγχος φυσικής πρόσβασης

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη "Πολιτική Φυσικής Ασφάλειας" στην οποία περιγράφονται τα εξής:

- ✓ Απαγορεύεται γενικά η είσοδος στο σύνολο των εγκαταστάσεων από μη εξουσιοδοτημένο άτομο
- ✓ Κάθε υπάλληλος έχει πρόσβαση μόνο στους χώρους του τμήματος στο οποίο ανήκει, καθώς και σε κάποιους κοινόχρηστους χώρους
- ✓ Απαγορεύεται οποιοδήποτε άτομο εκτός των υπαλλήλων της εταιρείας, να κυκλοφορεί στις εγκαταστάσεις χωρίς συνοδεία
- ✓ Κάθε τμήμα προστατεύεται σε περίπτωση διάρρηξης από αυτόνομο σύστημα συναγερμού

Περιορισμένη πρόσβαση σε αποσπώμενα μέσα αποθήκευσης

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη "Πολιτική Χρήσης Αφαιρούμενων Αποθηκευτικών Μέσων" στην οποία περιγράφονται τα εξής:

Οι χρήστες δε μπορούν να χρησιμοποιήσουν αποσπώμενα μέσα αποθήκευσης αν δεν υπάρχει ανάγκη και ποτέ χωρίς επίσημο αίτημα προς το τμήμα IT. Στο αίτημα, ο χρήσης θα πρέπει να αιτιολογεί απόλυτα το σκοπό της διακίνησης, το πλήθος των αρχείων προς μεταφορά και το χρόνο πρόσβασης

Αντίγραφα ασφαλείας

Σύμφωνα με το πρότυπο ασφάλειας πληροφοριών ISO27001, στην εταιρεία ακολουθείται συγκεκριμένη διαδικασία που αφορά τη "Διασφάλιση των Δεδομένων". Σύμφωνα με αυτή: η συχνότητα λήψης αντιγράφων ασφαλείας για κάθε σύστημα ορίζεται σύμφωνα με τα αποτελέσματα ανάλυσης Επιχειρηματικών Επιπτώσεων που αφορούν στο Maximum Data Loss και στο Recovery Point Objective. Το Recovery Point Objective προσδιορίζεται ανάλογα με τις επιχειρηματικές επιπτώσεις που έχει η απώλεια των δεδομένων, ενώ λαμβάνεται υπόψη ο χρόνος που χρειάζεται για την ανάκτηση ή δημιουργία αυτών. Η συχνότητα λήψης αντιγράφων ασφαλείας δεν θα πρέπει να είναι μικρότερη του Recovery Time Objective

4.1.4 Κίνδυνοι – Αθέμιτη πρόσβαση στα δεδομένα

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

- ✓ Κοινωνικός στιγματισμός
- ✓ Έκθεση του υποκειμένου σε κίνδυνο
- ✓ Ενόχληση του υποκειμένου από την κοινολόγηση των προσωπικών του δεδομένων
- ✓ Ψυχολογικό στρες
- ✓ Μείωση της εμπιστοσύνης ως προς τις διαδικασίες επεξεργασίας που ακολουθεί ο Δήμος

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

- ✓ Ανθρώπινο λάθος
- ✓ Κακόβουλο λογισμικό
- ✓ Ανθρώπινος δόλος

Ποιες είναι οι πηγές κινδύνου;

- ✓ Κακόβουλος χρήστης
- ✓ Εξωτερικός εισβολέας στο σύστημα
- ✓ Αμελής χρήστης

Ποια από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

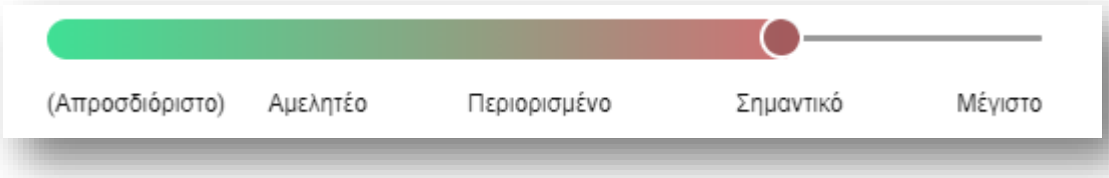
- ✓ Καταστολή κακόβουλου λογισμικού
- ✓ Έλεγχος φυσικής πρόσβασης
- ✓ Ασφάλεια δικτύου – Αποφυγή επιθέσεων μέσω δικτύου
- ✓ Παρακολούθηση δραστηριότητας δικτύου
- ✓ Περιορισμένη πρόσβαση σε αποσπώμενα μέσα αποθήκευσης

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

Οι πληροφορίες που επεξεργάζονται είναι υψηλής σπουδαιότητας. Πιθανή διαρροή για παράδειγμα δεδομένων οφειλών, αυτό μπορεί να επιφέρει ψυχολογικό στρες, αίσθημα εισβολής στην προσωπική ζωή του υποκειμένου, ανάπτυξη φοβίας, θύμα εκβιασμού κλπ. Πιθανή διαρροή ευαίσθητων προσωπικών δεδομένων πχ δεδομένα υγείας, μπορεί να προκαλέσουν στο υποκείμενο κοινωνικό στιγματισμό, κατάθλιψη, αίσθηση εισβολής στην ιδιωτική ζωή, ψυχολογικό εκφοβισμό κλπ.

Πιθανή διαρροή δεδομένων περιουσιακής κατάστασης μπορούν να επιφέρουν στο υποκείμενο αίσθηση εισβολής στην ιδιωτικότητά του, πιθανή παρενόχληση κλπ.

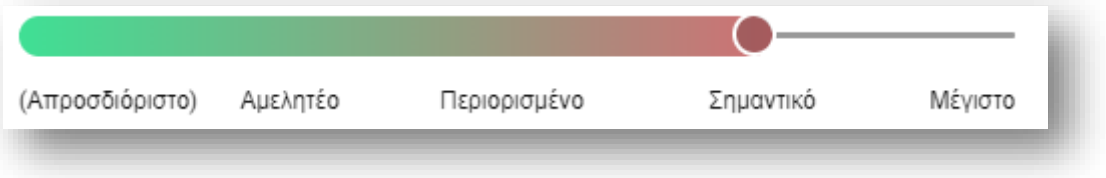
Πιθανή διαρροή προσωπικών δεδομένων (τηλέφωνο, διεύθυνση, email, ΑΦΜ, αριθ. ταυτότητας) μπορεί να προκαλέσει παρενόχληση στον κυβερνοχώρο, φυσική παρενόχληση, αίσθηση εισβολής στο προσωπικό χώρο του υποκειμένου, αλλά και πιο σοβαρές καταστάσεις όπως πιθανότητα πλαστοπροσωπίας κλπ.



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

Η πιθανότητα του κινδύνου λαμβάνοντας υπόψη τα προγραμματισμένα μέτρα, είναι σημαντική. Ο έλεγχος της φυσικής πρόσβασης στα δεδομένα και τα ληφθέντα μέτρα ως

προς την ασφάλεια του δικτύου μετριάζουν την πιθανότητα του κινδύνου, αλλά ο ανθρώπινος δόλος είναι ένας παράγοντας που δε μπορεί να εξαλειφθεί, οπότε και η πιθανότητα του κινδύνου παραμένει.



4.1.5 Κίνδυνοι – Ανεπιθύμητη τροποποίηση των δεδομένων

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

- ✓ Οικονομικά προβλήματα
- ✓ Ψυχολογικό στρες
- ✓ Μείωση της εμπιστοσύνης ως προς τις διαδικασίες που ακολουθεί ο Δήμος

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

- ✓ Ανθρώπινο λάθος
- ✓ Ανθρώπινος δόλος
- ✓ Κακόβουλο λογισμικό
- ✓ Σκόπιμη ή ακούσια διακοπή τροφοδοσίας

Ποιες είναι οι πηγές κινδύνου;

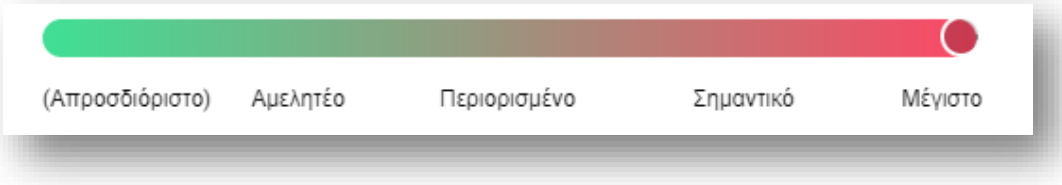
- ✓ Αμελής χρήστης
- ✓ Εξωτερικός εισβολέας στο σύστημα
- ✓ Κακόβουλος χρήστης
- ✓ Φυσική καταστροφή
- ✓ Εξωτερικός παράγοντας (διακοπή ρεύματος)

Ποια από τα προσδιορισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

- ✓ Καταστολή κακόβουλου λογισμικού
- ✓ Ασφάλεια δικτύου - Αποφυγή επιθέσεων μέσω δικτύου
- ✓ Παρακολούθηση δραστηριότητας δικτύου
- ✓ Προστασία από πηγές κινδύνων πλην του ανθρώπου
- ✓ Έλεγχος φυσικής πρόσβασης
- ✓ Ασφάλεια τεχνολογικού υλικού
- ✓ Συντήρηση Εξοπλισμού

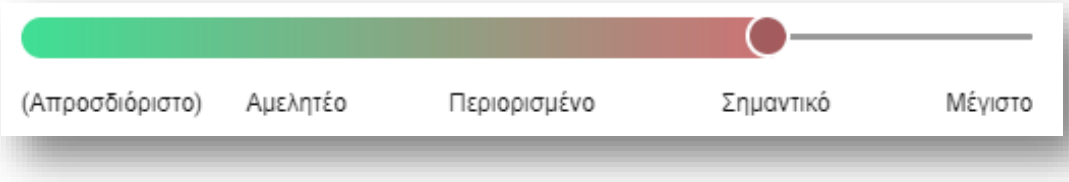
Πώς εκτιμάτε τη σοβαρότητα του κινδύνου, ιδίως ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Ιδιαίτερα σε ότι αφορά την αλλοίωση οικονομικών δεδομένων, ο αντίκτυπος στο υποκείμενο μπορεί να επιφέρει έντονη ψυχολογική βλάβη, σημαντικά χρέη, μέχρι και ποινικές κυρώσεις



Πώς εκτιμάτε την πιθανότητα του κινδύνου, ιδίως σε σχέση με τις απειλές, τις πηγές κινδύνου και τα προγραμματισμένα μέτρα;

Τα προγραμματισμένα μέτρα καλύπτουν το μεγαλύτερο μέρος ως προς τον περιορισμό της εμφάνισης των πιθανών κινδύνων, αλλά ο ανθρώπινος δόλος είναι ένας παράγοντας που δε μπορεί να εξαλειφθεί, οπότε και η πιθανότητα του κινδύνου παραμένει



4.1.6 Κίνδυνοι – Εξαφάνιση Δεδομένων

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

- ✓ Οικονομικά προβλήματα

- ✓ Ψυχολογικό στρες
- ✓ Μείωση της εμπιστοσύνης ως προς τις διαδικασίες που ακολουθεί ο Δήμος

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

- ✓ Κακόβουλο λογισμικό
- ✓ Ανθρώπινο λάθος
- ✓ Ανθρώπινος δόλος
- ✓ Σκόπιμη ή ακούσια διακοπή τροφοδοσίας

Ποιες είναι οι πηγές κινδύνου;

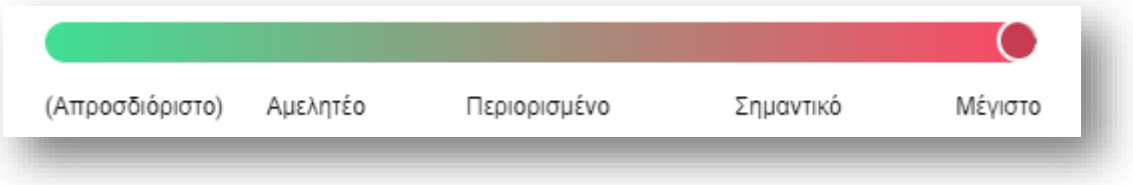
- ✓ Αμελής χρήστης
- ✓ Διακοπή ρεύματος
- ✓ Εξωτερικός εισβολέας στο σύστημα
- ✓ Κακόβουλος χρήστης
- ✓ Φυσική καταστροφή
- ✓ Αστοχία υλικού

Ποια από τα προσδιορισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

- ✓ Καταστολή κακόβουλου λογισμικού
- ✓ Ασφάλεια δικτύου - Αποφυγή επιθέσεων μέσω δικτύου
- ✓ Παρακολούθηση δραστηριότητας δικτύου
- ✓ Ασφάλεια τεχνολογικού υλικού
- ✓ Προστασία από πηγές κινδύνων πλην του ανθρώπου
- ✓ Συντήρηση Εξοπλισμού
- ✓ Έλεγχος φυσικής πρόσβασης
- ✓ Αντίγραφα ασφαλείας

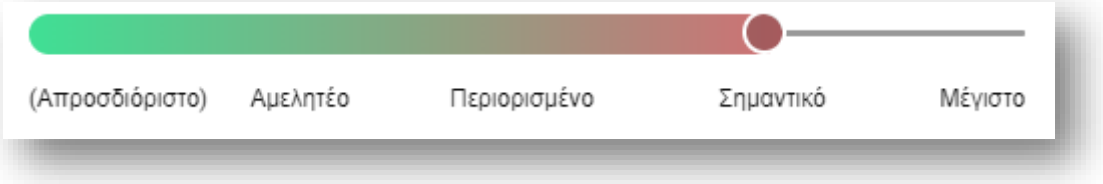
Πώς εκτιμάτε τη σοβαρότητα του κινδύνου, ιδίως ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Τα υποκείμενα ενδέχεται από την απώλεια των δεδομένων να υποστούν μη αναστρέψιμες συνέπειες όπως: σοβαρό χρηματοοικονομικό κίνδυνο, μακροχρόνιες ή μόνιμες ψυχολογικές παθήσεις, ανικανότητα προς εργασία



Πώς εκτιμάτε την πιθανότητα του κινδύνου, ιδίως σε σχέση με τις απειλές, τις πηγές κινδύνου και τα προγραμματισμένα μέτρα;

Τα προγραμματισμένα μέτρα μετριάζουν και σε αυτή την περίπτωση την πιθανότητα εμφάνισης του κινδύνου, παραμένει όμως πάντα ο παράγοντας του ανθρώπινου δόλου, ο οποίος δε μπορεί να εξαλειφθεί, οπότε και η πιθανότητα του κινδύνου παραμένει



4.1.7 Επισκόπηση της Εκτίμησης Αντικτύπου

Η καταγραφή των παραγόντων που επηρεάζουν την πιθανότητα εμφάνισης κινδύνων κατά τη διάρκεια της επεξεργασίας, καθώς και η εκτίμηση για το εύρος των επιπτώσεων που θα έχει η εμφάνιση του κινδύνου στο λογισμικό της CNIL, αποτυπώνει διαγραμματικά τη χαρτογράφηση των κινδύνων (εικόνα 2).

Παρατηρώντας τη χαρτογράφηση των κινδύνων, μπορούμε να συμπεράνουμε, ότι παρά τα εχέγγυα που μπορεί να έχει ένας οργανισμός που εκτελεί την επεξεργασία, η πιθανότητα εμφάνισης κινδύνων παραμένει. Επειδή συγκεκριμένη επεξεργασία αφορά μεγάλης κλίμακας δεδομένα, κρίνεται απαραίτητο ο Υπεύθυνος Επεξεργασίας να προτείνει ένα σχέδιο δράσης, με βελτιωτικά μέτρα, προκειμένου να περιοριστεί όσο το δυνατό περισσότερο, ο αντίκτυπος κατά την εμφάνιση πιθανών απειλών.

Εικόνα 2: Χαρτογράφηση Κινδύνων χωρίς βελτιωτικά μέτρα

4.1.8 Σχέδιο Δράσης

Ο αντίκτυπος των απειλών που εντοπίστηκαν κατά την παραπάνω μελέτη μπορεί να περιοριστεί με κατάλληλα βελτιωτικά μέτρα σε συγκεκριμένους τομείς.

Αμφίδρομη επικοινωνία Δήμου - Αναδόχου

Ένα πολύ σημαντικό θέμα όταν πρόκειται να εκτελεστεί επεξεργασία εκτός φορέα, είναι και ο τρόπος αποστολής των δεδομένων στον Ανάδοχο. Επειδή πρόκειται και για

ευαίσθητα προσωπικά δεδομένα, μια καλή λύση είναι η διακίνηση των δεδομένων να γίνεται μέσω ενός ασφαλούς πρωτοκόλλου μεταφοράς Secure FTP.

Καταστολή κακόβουλου λογισμικού:

Ο υπεύθυνος επεξεργασίας, σε αυτό τον κίνδυνο θα μπορούσε να προτείνει ως βελτιωτικό μέτρο, την προσθήκη στην πολιτική ασφάλειας Antivirus την υιοθέτηση μιας δράσης κατά την οποία οποιαδήποτε συσκευή μολυνθεί από κακόβουλο λογισμικό, θα πρέπει να απομονώνεται από το δίκτυο, μέχρι να ολοκληρωθούν όλες οι κατάλληλες ενέργειες που θα καταστήσουν το υλικό ασφαλές για την επανένταξή του στο δίκτυο.

Ασφάλεια δικτύου - Αποφυγή επιθέσεων μέσω δικτύου:

Ένα πολύ καλό μέτρο για την πρόληψη μιας τέτοιας απειλής, θα μπορούσε να είναι η υιοθέτηση μιας διαδικασίας από τον οργανισμό, κατά την οποία τα συστήματά του θα υποβάλλονται σε Penetration Testing προκειμένου να εντοπιστούν πιθανά τρωτά σημεία.

Παρακολούθηση δραστηριότητας δικτύου:

Εκτός από την εγκατάσταση ενός λογισμικού εποπτείας του δικτύου (monitoring) που έχει ήδη προβλεφθεί από τον οργανισμό, ένα πολύ αποτελεσματικό μέτρο θα ήταν ένα αυτοματοποιημένο σύστημα ειδοποίησης “alarm” προς τους διαχειριστές του δικτύου, σε περίπτωση που εντοπιστεί ύποπτη κίνηση στο δίκτυο. Με τον τρόπο αυτό εξασφαλίζεις ότι η ανταπόκριση ως προς μια πιθανή επίθεση μέσω διαδικτύου θα είναι όσο το δυνατό πιο άμεση.

Ασφάλεια τεχνολογικού υλικού:

Ένα βελτιωτικό μέτρο που μπορεί σχεδόν να εκμηδενίσει την πιθανή αστοχία του υλικού και την απώλεια δεδομένων λόγω ξαφνικής διακύμανσης της τάσης του ρεύματος ή της διακοπής αυτού, θα ήταν η απαίτηση εγκατάστασης UPS στον εξοπλισμό τον οποίο εκτελείται η επεξεργασία. Επίσης, μια πιο συχνή λήψη αντιγράφων ασφαλείας και έλεγχος της ορθότητας αυτών, είναι ένα μέτρο που θα μπορέσει να προστατέψει τα δεδομένα έπειτα από πιθανή αστοχία υλικού.

Φυσική πρόσβαση στους χώρους εκτέλεσης της επεξεργασίας:

Ένας από τους παράγοντες κινδύνου πιο δύσκολα αντιμετωπίσιμους, είναι και ο ανθρώπινος δόλος. Μια βελτιωτική κίνηση ως προς τα άτομα που έχουν πρόσβαση σε συγκεκριμένους χώρους επεξεργασίας, θα ήταν και η υιοθέτηση μια πολιτικής κατά την οποία όταν μιας μεγάλης κλίμακας επεξεργασία λαμβάνει χώρα σε κάποιο συγκεκριμένο χώρο του οργανισμού, η πρόσβαση σε αυτόν το χώρο να επιτρέπεται μόνο μέσω ID Badge και μόνο για τα άτομα που έχουν αναλάβει την επεξεργασία. Οι κινήσεις εισόδου/εξόδου από τους χώρους θα καταγράφονται σε κατάλληλο λογισμικό και θα παραμένουν αποθηκευμένες για εύλογο χρονικό διάστημα προκειμένου να μπορεί να γίνει ιχνηλάτηση πιθανής κακόβουλης ενέργειας (δόλος).

Ένα κλειστό κύκλωμα βιντεοκαταγραφής και παρακολούθησης των ατόμων που εισέρχονται στις εγκαταστάσεις του οργανισμού επίσης θα μπορούσε να χαρακτηριστεί βελτιωτικό μέτρο, με την προϋπόθεση όμως ότι δε θα επηρεάσει τα δικαιώματα και τις ελευθερίες των υπαλλήλων του οργανισμού.

Επιπλέον, μια καλή πολιτική θα ήταν τα άτομα που θα αναλάβουν την εκτέλεση της επεξεργασίας, καθώς και οι ρόλοι αυτών, να αναγράφονται ρητά στη σύμβαση μεταξύ φορέα (Δήμου) και του αναδόχου.

Ανθρώπινος δόλος με σκοπό την υποκλοπή προσωπικών δεδομένων:

Ο ανθρώπινος δόλος, με τα μέτρα που προτάθηκαν προηγουμένως, περιορίζεται μόνο ως προς ένα βαθμό· τη φυσική δηλαδή παρουσία ενός μη εξουσιοδοτημένου ατόμου εντός του χώρου που πραγματοποιείται η επεξεργασία. Ένα δεύτερο επίπεδο ασφάλειας, το οποίο θα μπορούσε να περιορίσει σχεδόν στο απόλυτο την πιθανότητα κοινολόγησης ψηφιακά αποθηκευμένων προσωπικών δεδομένων μετά από υποκλοπή, είναι η ψευδωνυμοποίηση. Για να διασφαλιστεί η εμπιστευτικότητα των δεδομένων καθ' όλη τη διαδικασία της επεξεργασίας, η ψευδωνυμοποίηση θα πρέπει να υλοποιηθεί στο πρώτο βήμα της διαδικασίας, τη στιγμή δηλαδή που η πληροφορία βρίσκεται ακόμα στον Υπεύθυνο επεξεργασίας και δεν έχει αποσταλεί προς επεξεργασία στον ανάδοχο. Με τον τρόπο αυτό τα δεδομένα ψευδωνυμοποιούνται πριν εκτεθούν σε κινδύνους εκτός του Δήμου, ενώ ακόμα και αν υποκλαπούν η πιθανότητα ταυτοποίησης των υποκειμένων σχεδόν εξαλείφεται.

Πρόταση εφαρμογής της ψευδωνυμοποίησης στη συγκεκριμένη επεξεργασία

Αρχικά όλα τα δεδομένα αποστέλλονται ψευδωνυμοποιημένα στον ανάδοχο. Ο αποστολέας των δεδομένων, δηλαδή ο Δήμος, πριν την αποστολή της πληροφορίας στον ανάδοχο, εκτελεί την εξής διαδικασία: Σε ένα μοναδικό χαρακτηριστικό της κάθε εγγραφής προς επεξεργασία πχ στο ΑΦΜ του οφειλέτη, (ή σε συνδυασμό χαρακτηριστικών για μεγαλύτερη ασφάλεια) εφαρμόζει συνάρτηση κατακερματισμού (hash function) με κλειδί (πχ αλγόριθμο HMAC, με υποκείμενη συνάρτηση κατακερματισμού τον SHA-2). Ο ανάδοχος από τη μεριά του, επί ψευδωνυμοποιημένων δεδομένων εκτελεί την επεξεργασία και την ολοκληρώνει έχοντας καταλήξει στα "ψευδώνυμα" των οφειλετών τους οποίους ο Δήμος πρέπει να εφαρμόσει τα μέτρα είσπραξης. Τα "ψευδώνυμα" αυτά στοιχεία αποστέλλονται στη συνέχεια στο Δήμο, προκειμένου να προχωρήσει στις διαδικασίες είσπραξης. Ο Δήμος, έχοντας το μυστικό κλειδί, μπορεί να κάνει την αντιστοίχιση των ψευδωνύμων με την αρχική πληροφορία, και ενημερώνεται για τους οφειλέτες που προέκυψαν από την επεξεργασία.

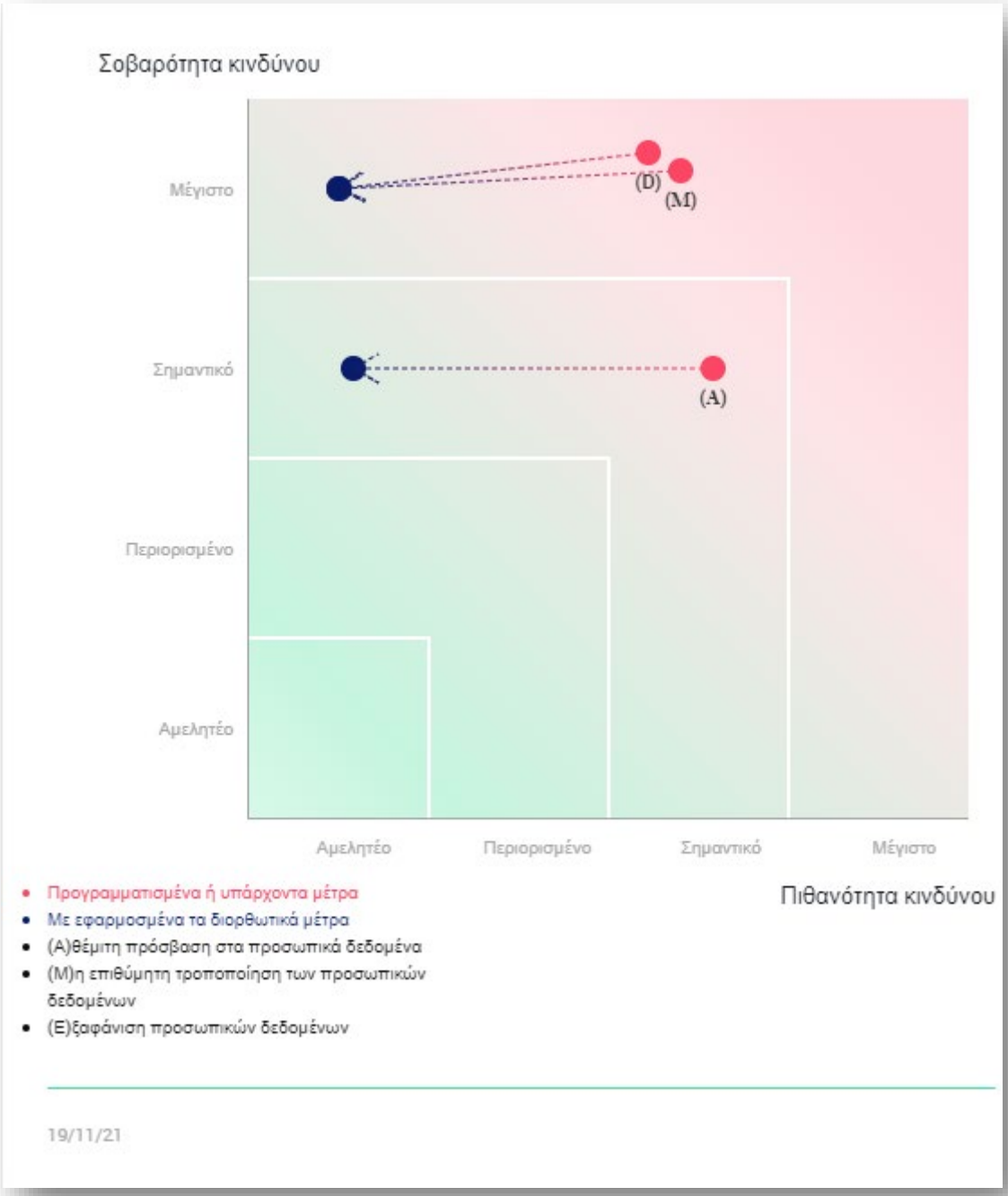
Άλλες τεχνικές κρυπτογράφησης που επιτρέπουν κάποιους υπολογισμούς επί κρυπτογραφημένων δεδομένων, όπως η ομομορφική κρυπτογράφηση, δεν κρίνονται κατάλληλες για τη συγκεκριμένη περίπτωση όπου ο εκτελών χρειάζεται να έχει πρόσβαση στην ακριβή αριθμητική τιμή οφειλής.

Ανεπιθύμητη τροποποίηση των δεδομένων

Ένα αρκετά αποτελεσματικό μέτρο για να αποφευχθεί η ανεπιθύμητη τροποποίηση των δεδομένων, είναι να αποκλειστεί από το διαδίκτυο και τα άλλα δικτυακά συστήματα, ο εξοπλισμός που χρησιμοποιείται στην επεξεργασία, καθώς και να ελαχιστοποιηθούν οι χρήστες που συμμετέχουν στην επεξεργασία στους απολύτως απαραίτητους

4.1.9 Εφαρμογή των βελτιωτικών μέτρων

Έχοντας πλέον ένα σχέδιο δράσης περιορισμού των κινδύνων που εντοπίστηκαν προηγουμένως, μπορούμε να εισάγουμε τα βελτιωτικά αυτά μέτρα στην εφαρμογή PIA, προκειμένου να προκύψει η νέα χαρτογράφηση της πιθανότητας εμφάνισής τους (Εικόνα 3). Από την αποτύπωση φαίνεται ξεκάθαρα, ότι η εφαρμογή των παραπάνω μέτρων μπορεί να ελαχιστοποιήσει την πιθανότητα εμφάνισης των κινδύνων που υπάρχουν.



Εικόνα 3: Χαρτογράφηση Κινδύνων μετά την εφαρμογή των βελτιωτικών μέτρων

Κεφάλαιο 5
Επίλογος

Έχοντας σαν αφετηρία την απαίτηση για προφύλαξη των προσωπικών δεδομένων του ατόμου, η παρούσα μεταπτυχιακή διατριβή εστίασε στη διαχείριση κινδύνων ασφαλείας που ενέχονται σε μια επεξεργασία προσωπικών δεδομένων μεγάλης κλίμακας, καθώς και γενικότερα στην προστασία τους βάσει του υπάρχοντος νομικού πλαισίου.

Το σενάριο που επιλέχθηκε ως μελέτη περίπτωσης, αφορά σε πραγματική ανάγκη που μπορεί να προκύψει σε ένα δημόσιο φορέα και προσπάθησε να καλύψει το μεγαλύτερο εύρος ως προς τις απαιτήσεις για ασφάλεια κατά την επεξεργασία οικονομικών δεδομένων πολιτών. Για το λόγο αυτό η παρούσα μεταπτυχιακή διατριβή, επειδή καλύπτει μια επεξεργασία προσωπικών δεδομένων μεγάλης κλίμακας, θα μπορούσε να αποτελέσει οδηγό για οποιαδήποτε μικρότερης κλίμακας επεξεργασίας παρουσιάζει κοινά χαρακτηριστικά με αυτή. Το γενικό σενάριο που πραγματεύεται και εμπλέκει δημόσιους φορείς που αναζητούν τρόπο να επεξεργαστούν προσωπικά δεδομένα εκτός του φορέα με ασφάλεια είναι καθημερινότητα, επομένως συναφείς περιπτώσεις που μπορούν να καθοδηγηθούν μέσα από αυτή τη διατριβή σίγουρα υφίστανται.

5.1 Συμπεράσματα

Τα συμπεράσματα που προκύπτουν από την εκπόνηση της μεταπτυχιακής αυτής διατριβής προσανατολίζονται σε δύο διαφορετικές κατευθύνσεις.

Η πρώτη αφορά τη σχέση που φαίνεται να έχει η Εκτίμηση Αντικτύπου, με τη μελέτη Εκτίμησης Κινδύνων όταν αφορούν την ίδια επεξεργασία. Μια αρχική μελέτη πάνω στον εντοπισμό πιθανών κινδύνων που μπορεί να προκύψουν από μια επεξεργασία προσωπικών δεδομένων (χρησιμοποιώντας για παράδειγμα μια μεθοδολογία όπως αυτή της ENISA), γίνεται αμέσως οδηγός για την εκπόνηση της Εκτίμησης Αντικτύπου, αν αυτό απαιτείται.

Η δεύτερη αφορά τη αλληλοκάλυψη ως προς τις απαιτήσεις ασφάλειας που φαίνεται να έχει ο ΓΚΠΔ και το πρότυπο ISO27001. Όπως προέκυψε και από τη μελέτη περίπτωσης, ένας οργανισμός που απαιτείται να είναι συμμορφωμένος ως προς την επεξεργασία των προσωπικών δεδομένων σύμφωνα με τον ΓΚΠΔ, βρήκε σε έναν εξωτερικό συνεργάτη που ακολουθεί το πρότυπο ISO27001, τα εχέγγυα που απαιτούσε για την ασφαλή εκτέλεση μιας επεξεργασίας με υψηλές απαιτήσεις.

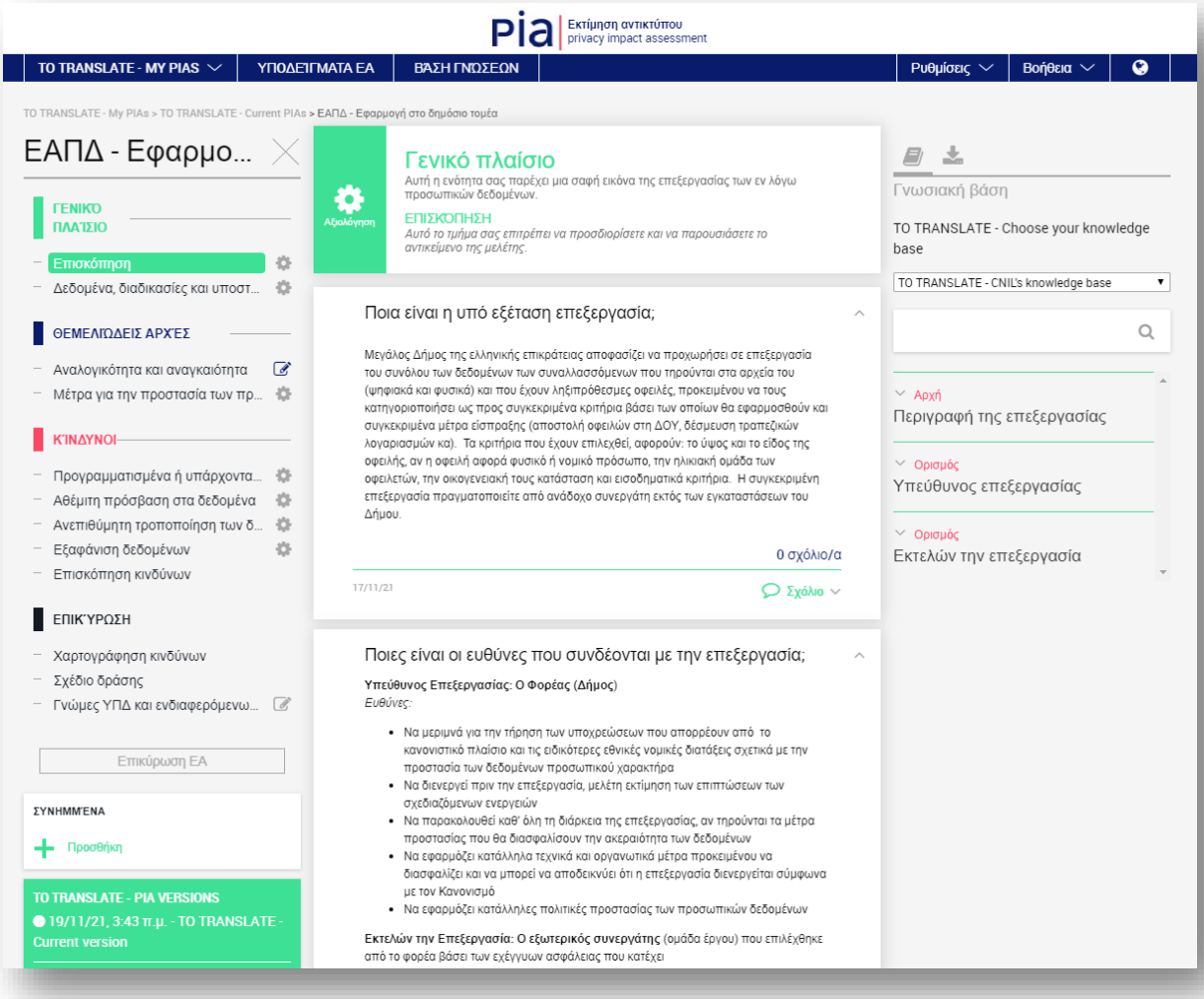
Τρίτο σημαντικό συμπέρασμα είναι ότι μία ορθά εκπονηθείσα εκτίμηση αντικτύπου μπορεί πράγματι να εντοπίσει προβλήματα και, άρα, να υλοποιηθούν έγκαιρα και εξ αρχής οι κατάλληλες λύσεις. Όπως για παράδειγμα, η ανάγκη ψευδωνυμοποίησης που με την εφαρμογή της στο αρχικό στάδιο της επεξεργασίας (κατ' εφαρμογή της αρχής data protection by design), μπορεί να περιορίσει στο ελάχιστο τους κινδύνους που εμφανίζονταν από την απειλή του ανθρώπινου δόλου.

Τέλος, από τη μεθοδολογία που ακολουθήθηκε προκύπτει ότι μία ορθά εκπονηθείσα εκτίμηση αντικτύπου για μία επεξεργασία μπορεί να χρησιμοποιηθεί ως αφετηρία για μία άλλη εκτίμηση αντικτύπου για άλλη επεξεργασία του ίδιου υπευθύνου επεξεργασίας, για άλλο σκοπό, αλλά με κοινά χαρακτηριστικά. Για παράδειγμα, αν ο Δήμος – στον οποίο εστιάσαμε ως μελέτη περίπτωσης- επιθυμεί να αναθέσει στον ίδιο εξωτερικό συνεργάτη επεξεργασία πχ, για τους υπαλλήλους του (πχ διαχείριση μισθοδοσίας κτλ.) τότε, παρόλο που πρόκειται για μία τελείως διαφορετική επεξεργασία με άλλους κινδύνους και άλλα χαρακτηριστικά, εν τούτοις πολλές πτυχές της εκτίμησης αντικτύπου είναι κοινές – όπως τα υλοποιημένα μέτρα ασφάλειας του οργανισμού, βάσει του προτύπου ISO. Ως εκ τούτου, μία εκτίμηση αντικτύπου μπορεί να αποτελέσει οδηγό όχι μόνο για συναφείς επεξεργασίες αλλά και για διαφορετικές επεξεργασίες με κάποια όμως κοινά χαρακτηριστικά.

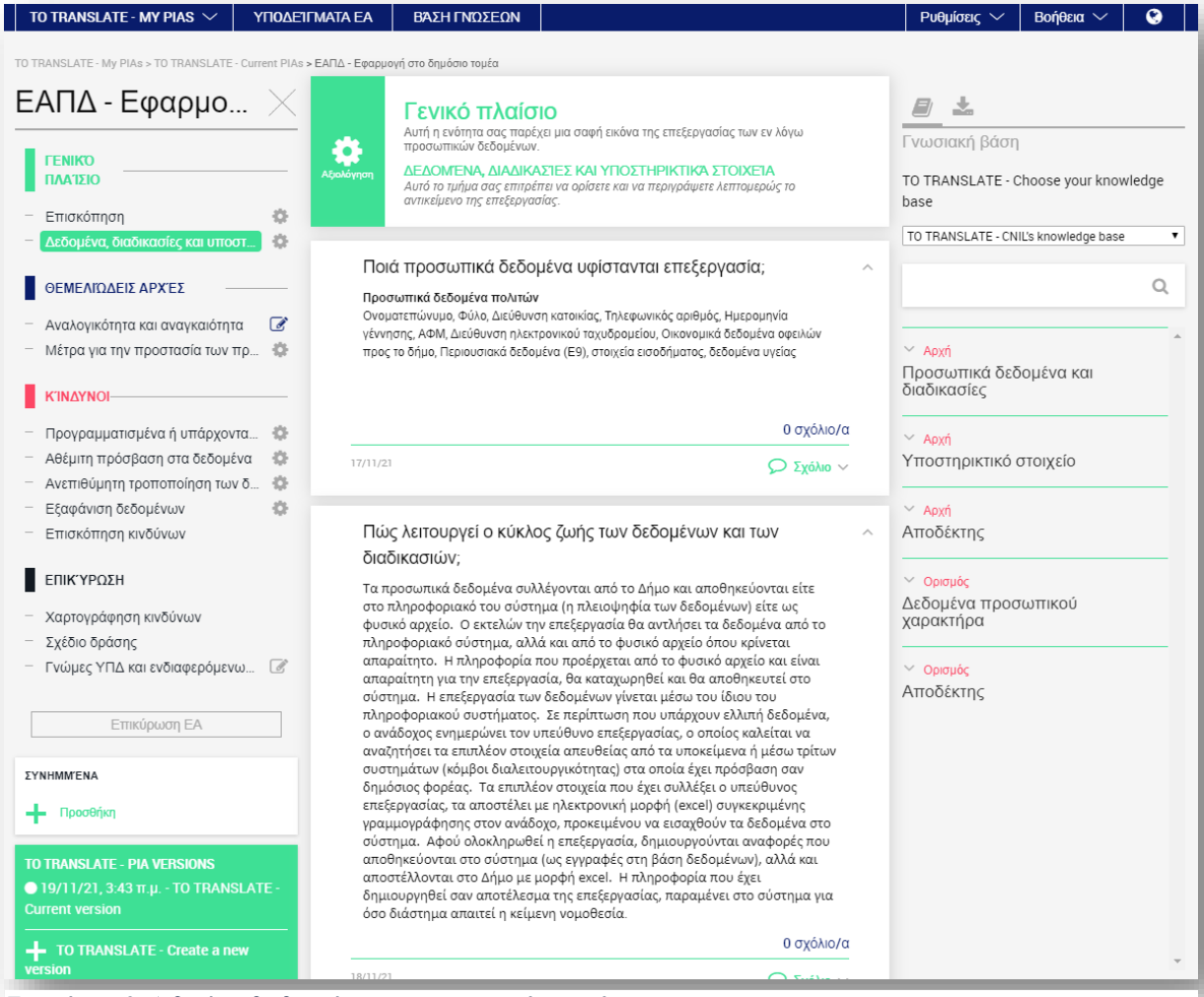
Δεδομένης της σημασίας της εκτίμησης αντικτύπου, εκτιμάται ότι θα ήταν πολύ χρήσιμο, ως μελλοντική έρευνα, να γίνουν προσπάθειες στο να υπάρχουν εξειδικευμένα πρότυπα (templates) ανά σενάρια περίπτωσης, έτσι ώστε ένας υπεύθυνος επεξεργασίας να μην ξεκινά την εκπόνησή της από ένα γενικό πρότυπο αλλά από κάποιο εστιασμένο κατ' αρχάς στις ιδιαιτερότητες της εκάστοτε επεξεργασίας.

Παράρτημα Α

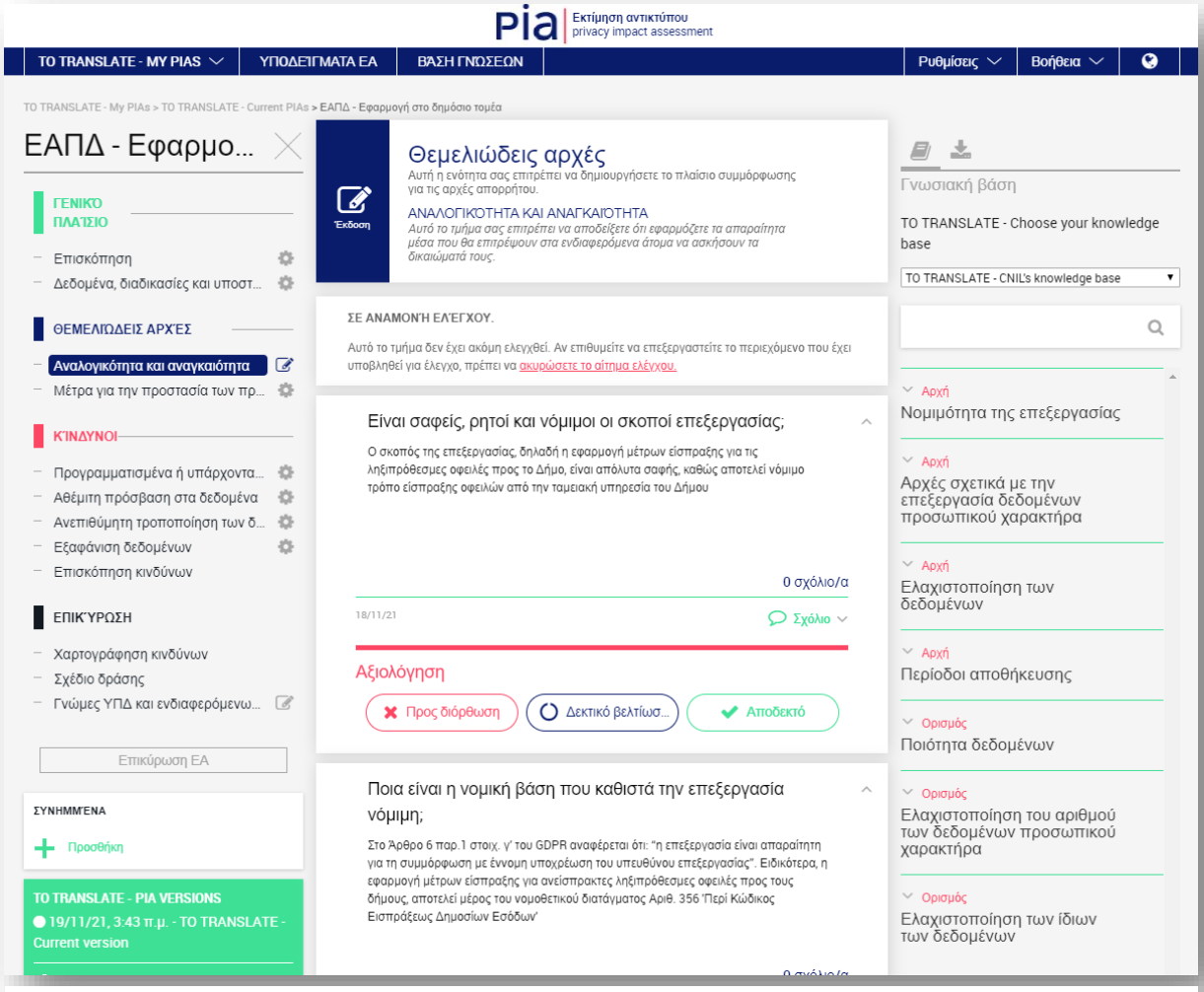
ΕΑΠΔ μέσω του λογισμικού PIA



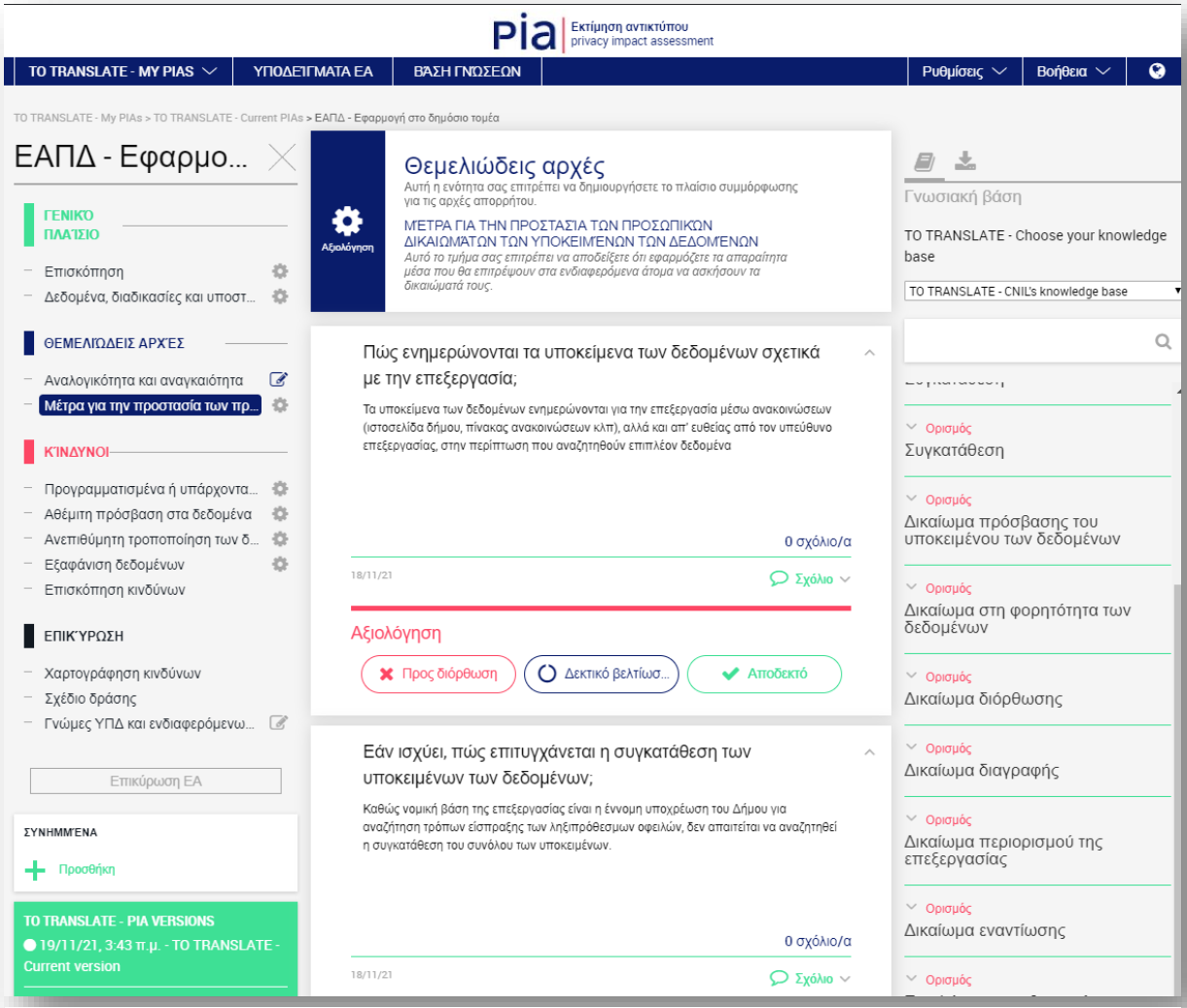
Στιγμιότυπο 1: Γενικό πλαίσιο PIA



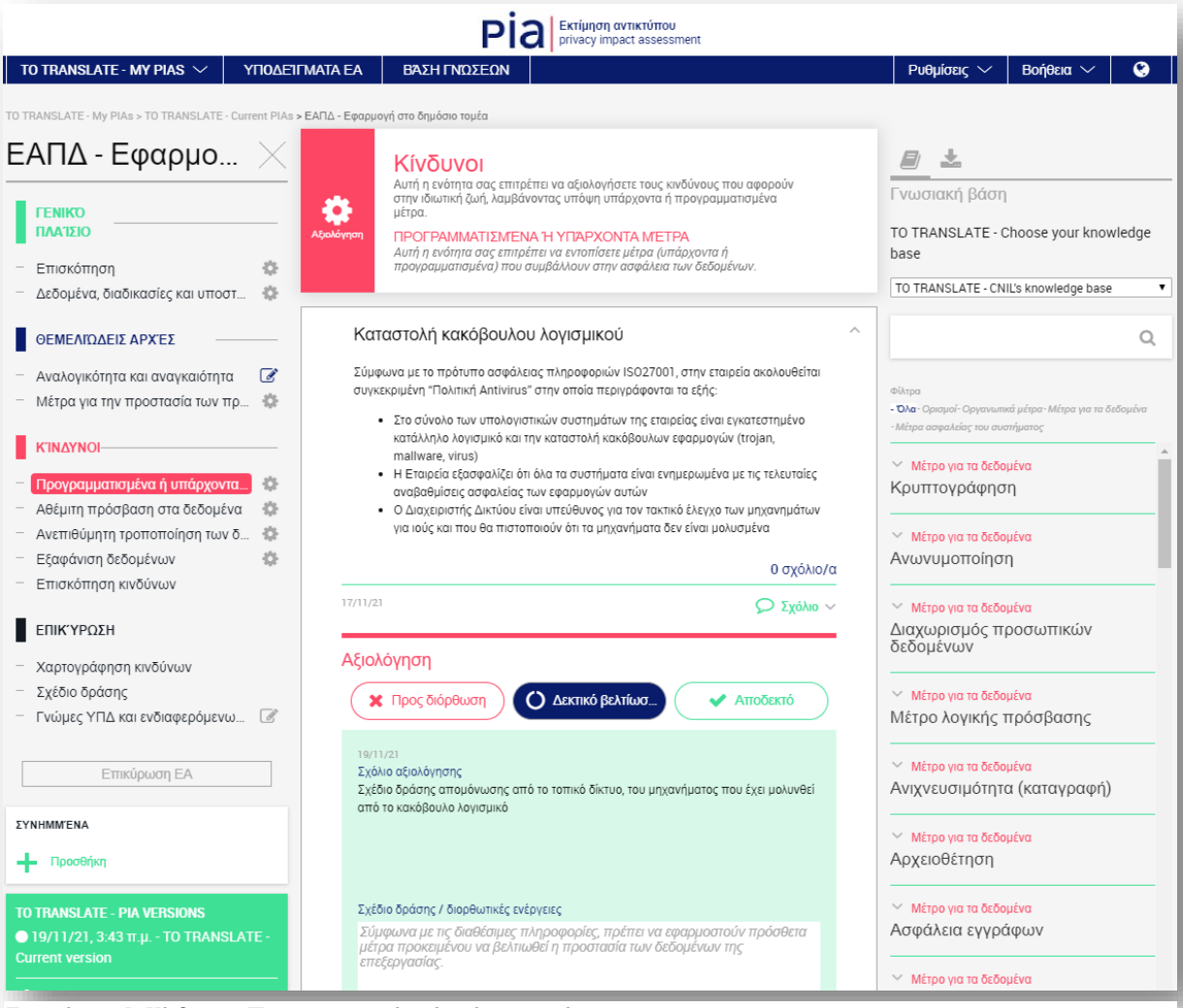
Στιγμιότυπο 2. Δεδομένα, διαδικασίες και υποστηρικτικά στοιχεία



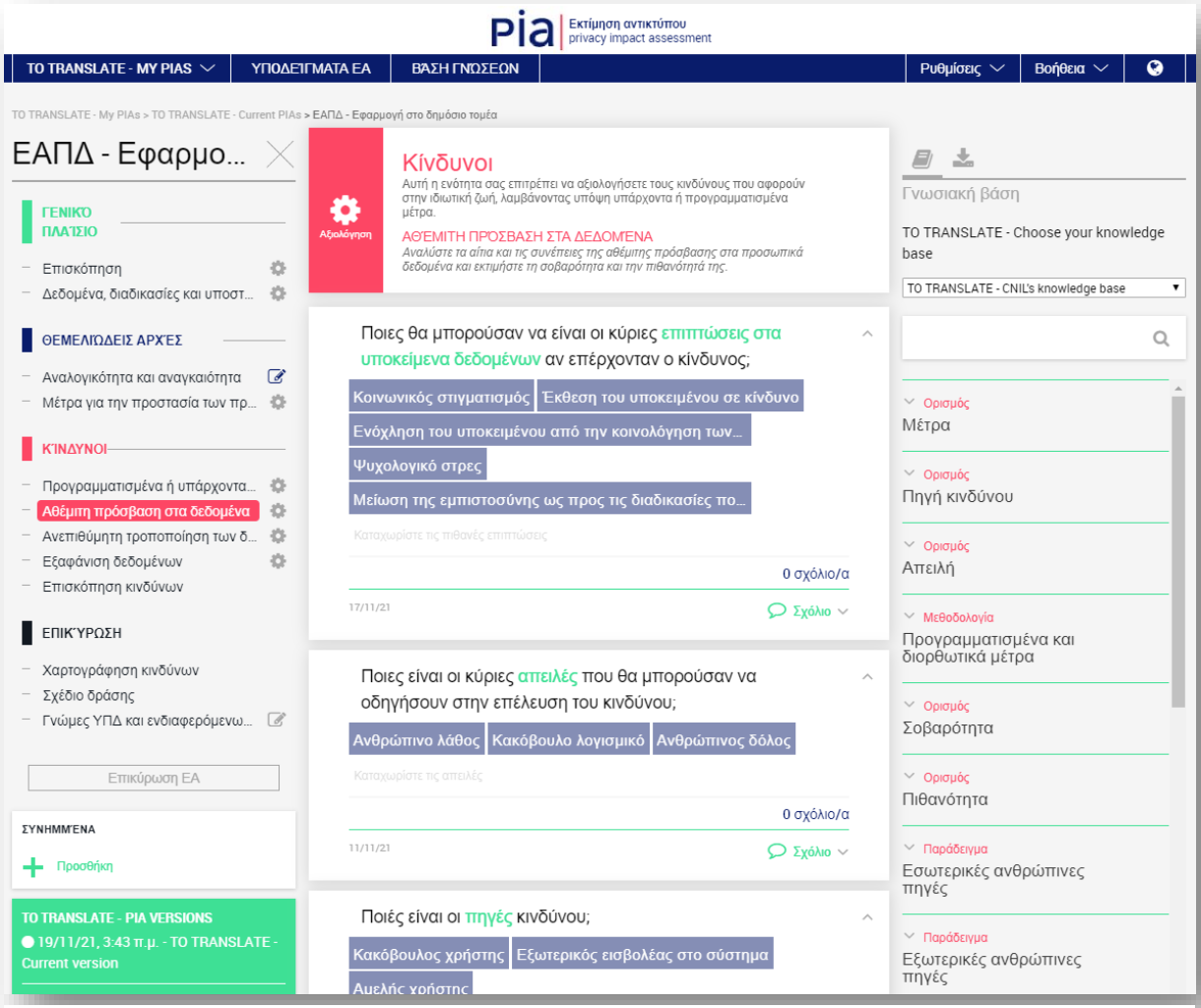
Στιγμιότυπο 3. Θεμελιώδεις Αρχές - Αναλογικότητα και αναγκαιότητα



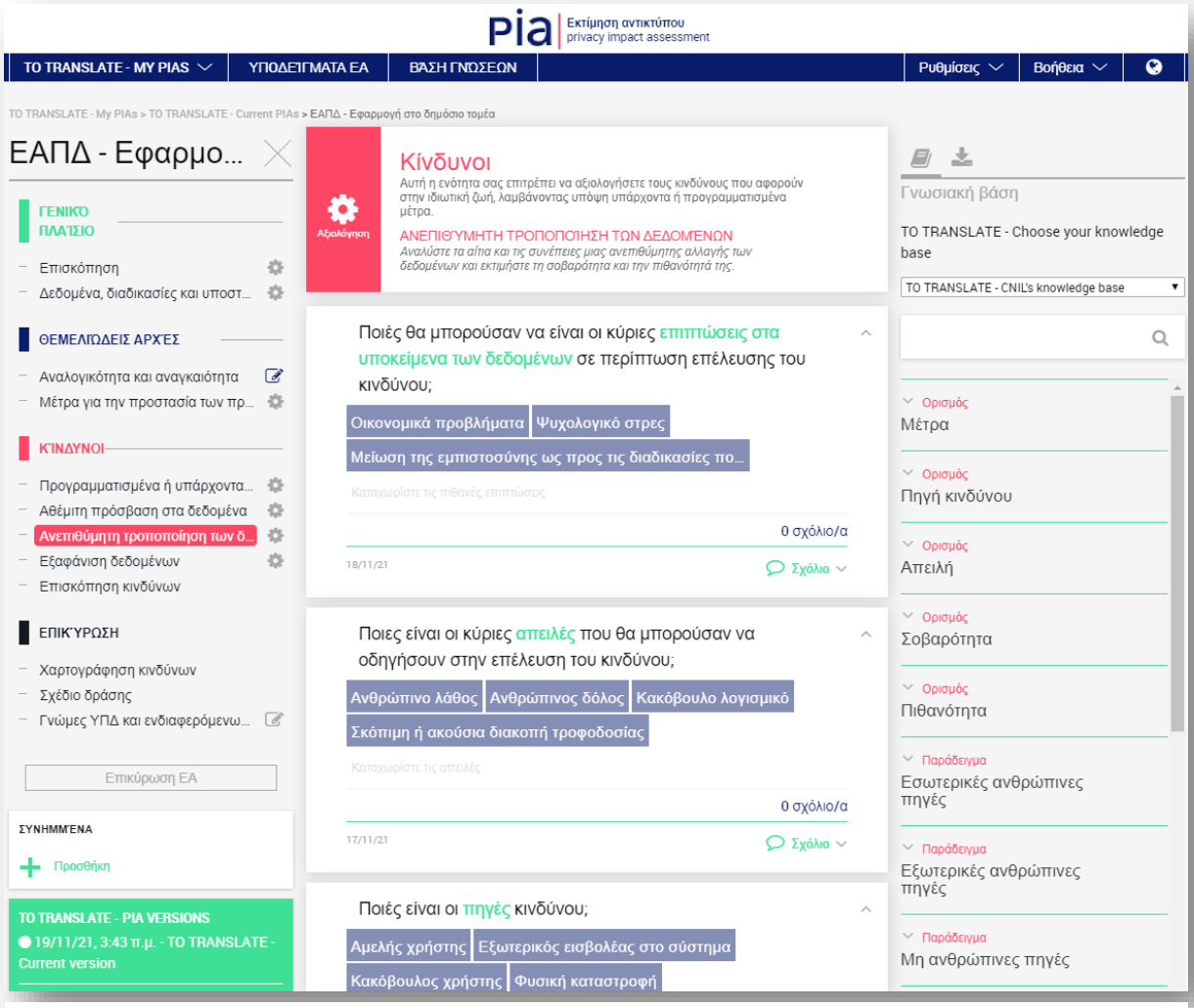
Στιγμιότυπο 4. Θεμελιώδεις Αρχές - Μέτρα για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων



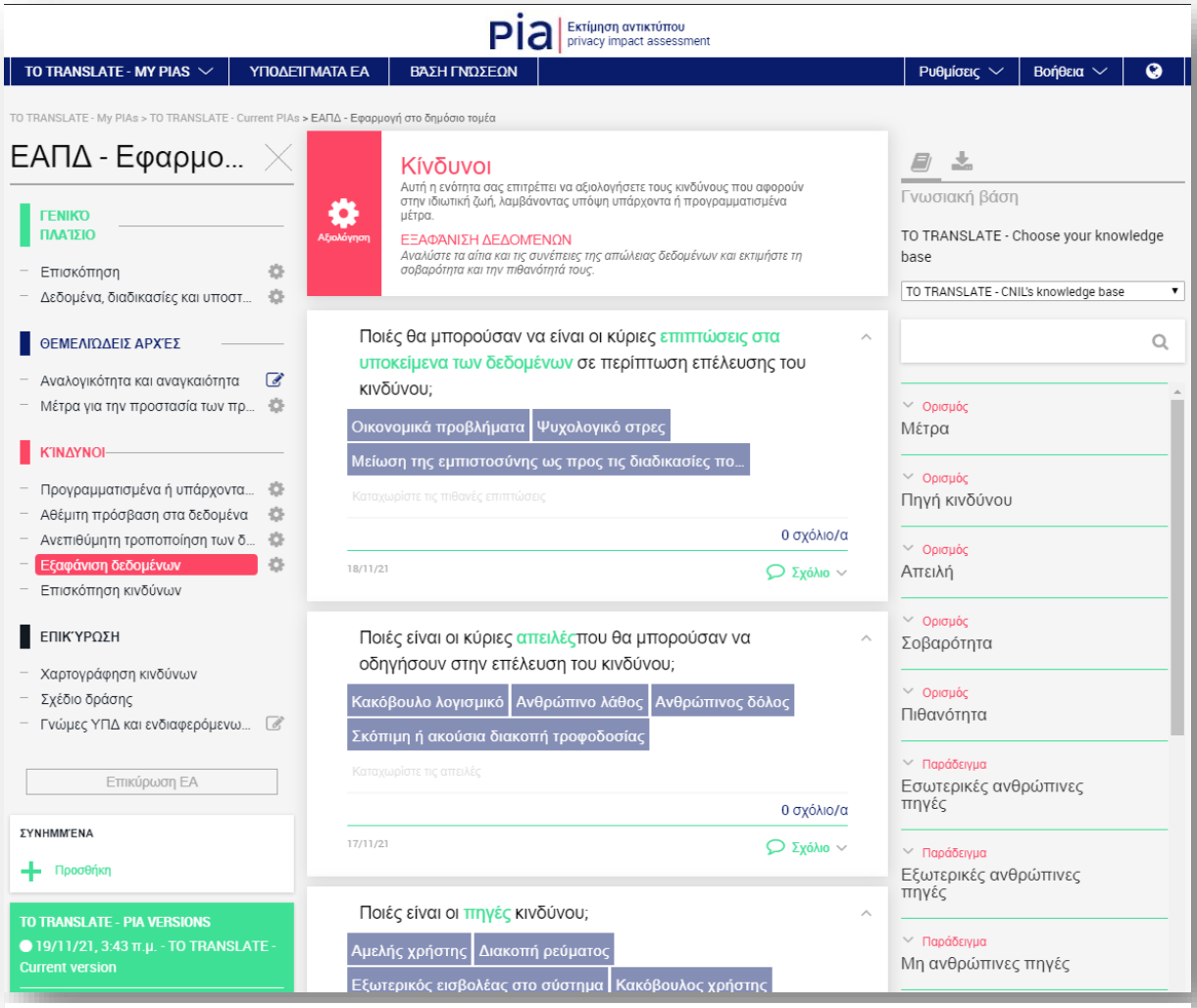
Στιγμιότυπο 5. Κίνδυνοι - Προγραμματισμένα ή υπάρχοντα μέτρα



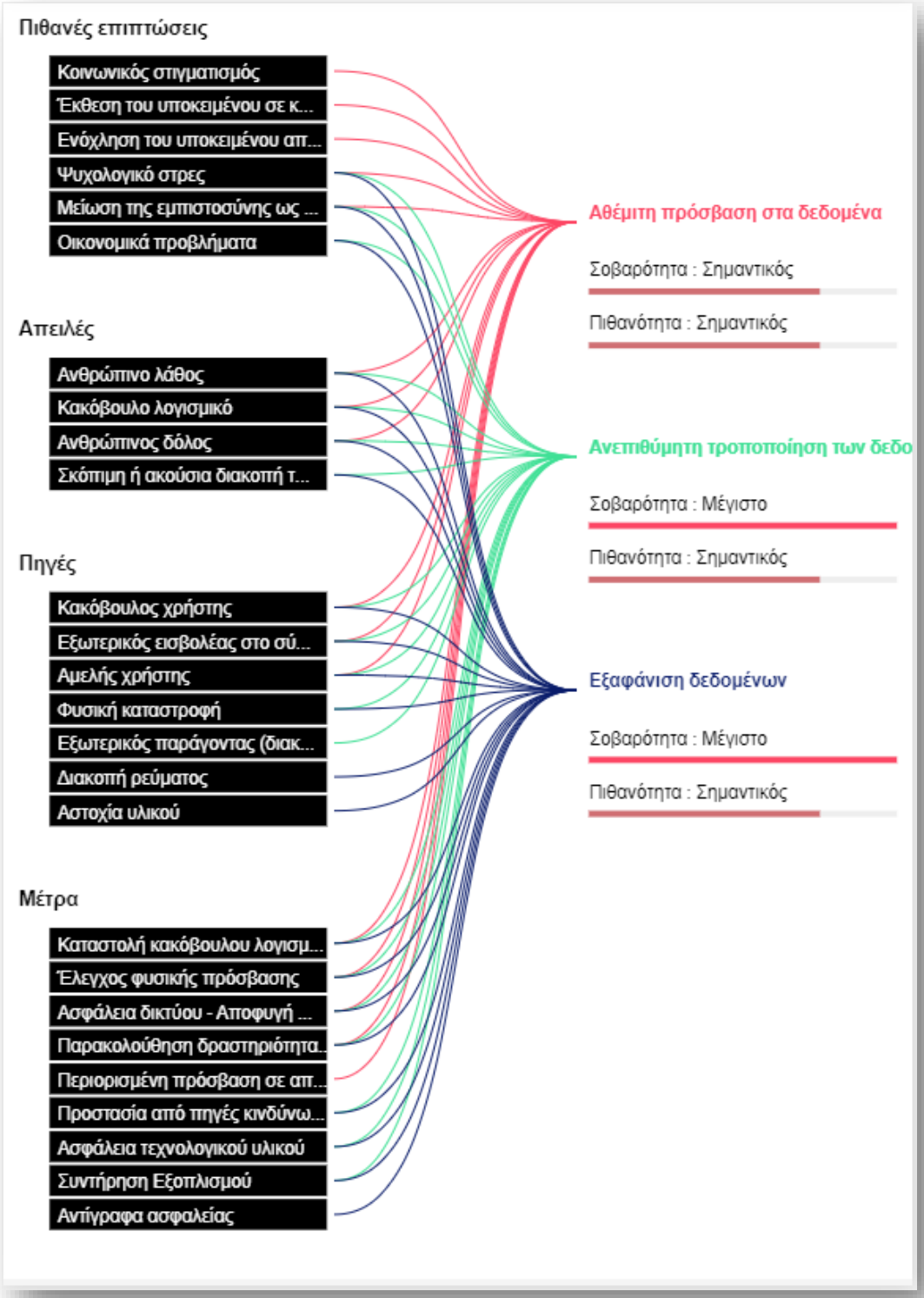
Στιγμιότυπο 6. Κίνδυνοι - Αθέμιτη πρόσβαση στα δεδομένα



Στιγμιότυπο 7. Κίνδυνοι - Ανεπιθύμητη τροποποίηση των δεδομένων



Στιγμιότυπο 8. Κίνδυνοι - Εξαφάνιση δεδομένων



Στιγμιότυπο 9. Επισκόπηση κινδύνων

Βιβλιογραφία

CNIL. *The open source PIA software helps to carry out data protection impact assesment | CNIL.* n.d. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-dataprotection-impact-assesment.

ENISA. «Handbook on Security of Personal Data Processing.» n.d. https://www.enisa.europa.eu/publications/handbook-onsecurity-of-personal-data-processing.

European Data Protection Board. *Κατευθυντήριες γραμμές 2/2019 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 6 παρ.1 στοιχ. β) του ΓΚΠΔ στο πλαίσιο της παροχής επιγραμμικών υπηρεσιών σε υποκείμενα δεδοένων.* 8 Οκτωβρίου 2019.

European Parliament. «(GDPR) Γενικός Κανονισμός για την Προστασία Δεδομένων.» 2016.

—. «Οδηγία για την προστασία δεδομένων προσωπικού χαρακτήρα, ΕΕ 1995 L 281, σ. 31.» *Official Journal of the European Communities*, 23 Νοέμβριος 1995: 50.

European Parliament, και Fundamental Rights/Council of Europe. «Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων.» *European Union Agency for Fundamental Rights.* Μοντάζ: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης. Απρίλιος 2014. https://fra.europa.eu/el/publication/2020/egheiridio-shetika-me-tin-eyropaiki-nomothesia-gia-tin-prostasia-ton-prosopikon (πρόσβαση 11 14, 2021).

Information Commissioner's Office (ICO), . «Data protection impact assessments .» n.d. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/?q=PIA.

Maciejewski, Mariusz. *https://www.europarl.europa.eu/.* 10 2021. https://www.europarl.europa.eu/factsheets/el/sheet/157/ (πρόσβαση 11 13, 2021).

Official Journal of the European Union. «REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.» 27 April 2016.

on line dictionary Merriam-webster. n.d. https://www.merriam-webster.com/dictionary/privacy.

PRIVAZYPLAN gets your data protection on course. n.d. https://www.privacy-regulation.eu/el/9.htm (πρόσβαση 11 19, 2021).

Schneier, B. «A Revised Taxonomy of Social Networking Data - Schneier on Security.» n.d. https://www.schneier.com/blog/archives/2010/08/a_taxonomy_of_s_1.html. (πρόσβαση 11 19, 2021).

William Stallings, PhD. «Privacy Impact Assessment: The Foundation for Managing Privacy Risk.» *Cyber Security and Information Systems Information Analysis Center (https://www.csiac.org)*, 17 March 2021.

Αρχή Προστασίας Δεδομένων. *Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων.* n.d. https://www.dpa.gr/ (πρόσβαση 11 19, 2021).

Γενικός Κανονισμός για την Προστασία Δεδομένων. n.d. https://gdprinfo.eu/el (πρόσβαση 11 19, 2021).

Δρ. Λουκάς, Νικόλαος Η. «Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), Κρυπτογράφηση και Ψευδωνυμοποίηση.» *ΣΥΝήΓΟΡΟΣ*, Σεπτέμβριος - Οκτώβριος 2017.

Κουκιάδης, Δημήτριος Ι. *Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το Γενικό Κανονισμό Προστασίας Δεδομένων.* Αθήνα: Σάκκουλα, 2019.

Κυριαζόγλου, Ιωάννης. *Προστασία Προσωπικών Δεδομένων.* FYLATOS PUBLISHING, 2019.

«Ν.4624/.» 2019.

Ομάδα Εργασίας του Άρθ.29 για την προστασία των Δεδομένων. «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.» Οδηγία, Βρυξέλλες, 2017, 29.

Τασιόπουλος, Σταύρος. *ΙΤΑ - Ινστιτούτο Τοπικής Αυτοδιοίκησης.* 19 Δεκέμβριος 2018. https://www.ita.org.gr/el/index.php/proskliseis-ergon/212-gdpr-kanonismos-gia-ta-prosopika-dedomena-i-efarmogi-stous-dimous (πρόσβαση 11 15, 2021).