ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΓΑΛΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ GDPR ΣΤΗ ΝΕΑ ΕΠΟΧΗ ΤΟΥ ΨΗΦΙΑΚΟΥ ΔΙΚΑΣΤΗΡΙΟΥ

Διπλωματική Εργασία

του

Αντωνίου Κίζα

Θεσσαλονίκη, Φεβρουάριος 2019

ΜΕΓΑΛΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ GDPR
ΣΤΗ ΝΕΑ ΕΠΟΧΗ ΤΟΥ ΨΗΦΙΑΚΟΥ ΔΙΚΑΣΤΗΡΙΟΥ

Αντώνιος Κίζας

Πτυχίο Πληροφορικής, ΕΑΠ, 2016

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ
ΠΛΗΡΟΦΟΡΙΚΗ

Περίληψη

Αδιαμφισβήτητα, στις μέρες μας, βιώνουμε στον απόλυτο βαθμό τη λεγόμενη τεχνολογική επανάσταση, με την εισαγωγή νέων μεθόδων ψηφιοποιημένης εργασίας, οι οποίες προκαλούν παγκόσμια αναταραχή στον τρόπο με τον οποίο επικοινωνούν και ανταλλάσσουν πληροφορίες οι άνθρωποι. Η επίδραση των νέων τεχνολογιών σε κάθε τομέα της οργανωμένης δραστηριότητας, δημιουργεί προκλήσεις, όσο αφορά τις παραδοσιακές φιλοσοφίες διαχείρισης και πρόσβασης στις πληροφορίες. Η πρώτη και πιο προφανής είναι η επιβεβλημένη χρήση της τεχνολογίας των Big Data, ως νέος τρόπος προσέγγισης των δικαστικών υπηρεσιών καθώς εισάγει διαφορετικά κριτήρια επεξεργασίας των νομικών δεδομένων. Προς αυτή την κατεύθυνση, καταλυτικό ρόλο παίζει και η ραγδαία άνοδος του διαδικτύου, η οποία τροφοδοτεί με εκθετική αύξηση την ανάγκη για αποθήκευση, καθώς και για προστασία και ανάλυση των όγκων πληροφοριών. Η δεύτερη και άκρως ουσιώδης σχετίζεται με τη διασφάλιση των προσωπικών στοιχείων, όπως καθορίζεται στο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation), με τη χρήση βέλτιστων πρακτικών κατά την αποθήκευση και διαχείρισή τους. Ο σχεδιασμός σύγχρονων συστημάτων επεξεργασίας βασισμένος στην τεχνολογία των μεγάλων δεδομένων προτρέπει τους υπεύθυνους χάραξης της ψηφιακής δικαιοσύνης, να αγκαλιάσουν τις ευκαιρίες που παρουσιάζονται σε μια δικτυωμένη κοινωνία και να υιοθετήσουν την αυξανόμενη επικράτηση των δικαστικών πληροφοριών σε ψηφιακή μορφή, αντιμετωπίζοντας παράλληλα τους αναδυόμενους κινδύνους και προκλήσεις.

Λέξεις Κλειδιά: Μεγάλα Δεδομένα, Ψηφιακό Δικαστήριο, GDPR, Προστασία Δεδομένων

Abstract

Undoubtedly, we now experience the so-called technological revolution, with the introduction of new methods of digitized work, which cause a global disruption to the way people communicate and exchange information. The impact of new technologies on every area of organized activity poses challenges as far as traditional management philosophies and access to information is concerned. The first and most obvious is the forced use of Big Data technology as a new way of approaching the judicial services as it introduces different criteria for processing legal data. In this direction, the rapid rise of the Internet, which exponentially increases the need for storage as well as for the protection and analysis of information volumes, plays a catalytic role. The second and most essential relates to the safeguarding of personal data, as defined in the General Data Protection Regulation (GDPR), using best practices when storing and managing them. Designing advanced processing systems based on Big Data technology encourages digital justice designers to embrace the opportunities in a networked society and to adopt the increasing prevalence of judicial information in digital form while addressing emerging dangers and challenges.

Keywords: Big Data, Digital Courtroom, GDPR, Data Protection

Πρόλογος – Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του Μεταπτυχιακού Προγράμματος Σπουδών, του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας και αποτελεί μία πρότυπη μελέτη της εφαρμογής και αξιοποίησης της τεχνολογίας των μεγάλων δεδομένων στο χώρο της Δικαιοσύνης, υπό το πρίσμα της πλήρους εναρμόνισης των διαδικασιών με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων.

Τονίζεται ιδιαίτερα πως η αναφορά στην υπηρεσία του Πρωτοδικείου Θεσσαλονίκης, κατά τη περιγραφή της μελέτης περίπτωσης, η οποία σχετίζεται με την εξέταση του αντίκτυπου των προσωπικών δεδομένων κατά την έκδοση πιστοποιητικών, σε καμία περίπτωση δεν αφορά την άντληση εμπιστευτικών πληροφοριών και προσωπικών δεδομένων, από την οικεία βάση και τα συστήματα διαχείρισης του Πρωτοδικείου.

Στο σημείο αυτό, θα ήθελα να ευχαριστήσω την οικογένειά μου για την συμπαράσταση της και την υπομονή που επέδειξε κατά τη διάρκεια των σπουδών μου.

...αφιερωμένη στη μητέρα μου

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες

- ΕΑΠΔ: Εκτίμηση Αντίκτυπου Προσωπικών Δεδομένων
- DPD: Data Protection Directive
- DPO: Data Protection Officer
- GDPR: General Data Protection Regulation
- PIA: Privacy Impact Assesment

Εισαγωγή

Στην εποχή μας, έχουν ωριμάσει οι συνθήκες για ρηξικέλευθες αλλαγές στον τομέα της δικαιοσύνης, με απώτερο σκοπό την αναβάθμιση της ποιότητας των παρεχόμενων υπηρεσιών προς όλους τους εμπλεκόμενους φορείς. Επί δεκαετίες, είχαν εντοπιστεί λειτουργικές καθυστερήσεις, οι οποίες, εν δυνάμει, επηρέαζαν, έστω και ακούσια, την εκτέλεση των απαιτούμενων διαδικασιών σε εύλογο χρονικό διάστημα. Σ' αυτό ακριβώς το σημείο, έγκειται η δύναμη της εποχής των Big Data, στην πλήρη αξιοποίηση του συνολικού όγκου των πληροφοριών, διατηρώντας στον απόλυτο βαθμό την ακεραιότητα και την ανεξαρτησία της δικανικής κρίσης.

Με τη θέσπιση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR), κωδικοποιήθηκε, για πρώτη φορά, σε κείμενο δεσμευτικής ισχύος, ένα υψηλότερο επίπεδο προστασίας του απορρήτου των προσωπικών πληροφοριών, αποσαφηνίζοντας ένα μακρύ κατάλογο υποχρεώσεων που καλούνται να τηρήσουν πιστά οι φορείς που εμπλέκονται με την επεξεργασία και αποθήκευση των δεδομένων.

Εύλογα, λοιπόν, έχουν ανακύψει καίρια ερωτήματα, με κοινό σημείο την πολιτική "ορθής" χρήσης των Big Data σε συνδυασμό με το GDPR. Εκείνο που διερευνάται είναι η έκταση της χρήσης τους στο δικαστήριο του μέλλοντος. Θα θεραπεύσει τα υπάρχοντα προβλήματα της δικαιοσύνης; Αποτελεί πρόκληση η μετάβαση στην ψηφιακή δικαιοσύνη; Η εναρμόνιση με το GDPR θα είναι ομαλή ή θα σταθεί εμπόδιο στα μεγάλα δεδομένα; Υπάρχει συμβατότητα μεταξύ GDPR και Big Data; Ενδοιασμοί που αναζητούν απαντήσεις, συνθέτουν γνώμες και απόψεις αλλά και συμβάλλουν στην πρόβλεψη πιθανών κατευθύνσεων του ψηφιακού δικαστηρίου και των τρόπων ανάπτυξής του.

Το δίκαιο και η επιστήμη των υπολογιστών οδηγούν σταδιακά στη γέννηση ενός νέου πεδίου, ικανού να συντελέσει στην ψηφιακή επανάσταση της δικαιοσύνης. Η μέγιστη αξιοποίηση των βασικών χαρακτηριστικών των Big Data σε συνδυασμό με την εναρμόνιση των τεχνικών συμμόρφωσης με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων, αποτελεί τον ακρογωνιαίο λίθο της δικαστικής μεταρρύθμισης, η οποία οδηγεί στην εδραίωση ενός "ευφυούς" δικαστικού συστήματος, εξοπλισμένου με τα πιο σύγχρονα τεχνολογικά μέσα, ικανού να θεραπεύσει προβλήματα όπως η γραφειοκρατία, η ασφάλεια των δεδομένων, το αυξημένο λειτουργικό κόστος, η επιβράδυνση στην απονομή της δικαιοσύνης, καθώς και η αδυναμία άμεσης πρόσβασης των εμπλεκομένων μερών μιας δίκης σε όλα τα δεδομένα της. Η χρήση των Big Data

απευθύνεται τόσο σε νομοθέτες όσο και σε φορείς της δικαστικής εξουσίας και αποσκοπεί στην αναδιοργάνωση των δικαστικών διαδικασιών μέσω της μετάβασής τους στο διαδίκτυο.

Μολονότι η υλοποίηση του έργου αυτού φαντάζει ιδανική, δε θα επιτευχθεί χωρίς προβλήματα. Μέσα από τα άρθρα τους, οι περισσότεροι μελετητές εστιάζουν στο αίτημα για εκσυγχρονισμό της δικαιοσύνης, υποδηλώνοντας με τον πλέον εμφατικό τρόπο τα ανωτέρω διαχρονικά προβλήματα αυτής καθώς και τη δυναμική επίλυσή τους, μέσω των Big Data. Προς την ίδια κατεύθυνση αλλά με πιο στοχευμένες παρατηρήσεις, διακρίνονται ερευνητές οι οποίοι υπεραμύνονται για τη διατήρηση του φυσικού ρόλου των συντελεστών μιας δίκης, υποβοηθούμενου σε καθαρά τεχνικό επίπεδο από την ορθή χρήση αυτών. Μέσα στην παρούσα εργασία συστηματοποιούνται οι τρόποι υλοποίησης του εγχειρήματος με κύριο προσανατολισμό τη διασφάλιση των προσωπικών δεδομένων, σε όλα τα στάδια της επεξεργασίας τους.

Κεφάλαιο 1: Big Data

Εισαγωγή

Η αξιοποίηση των "μεγάλων δεδομένων" είναι ένα από τα πιο αναδυόμενα και κρίσιμα ζητήματα που καλείται να εφαρμόσει ο χώρος της δικαιοσύνης στην σύγχρονη ψηφιακή εποχή. Η περιγραφή των βασικών χαρακτηριστικών των μεγάλων δεδομένων (Volume, Variety, Velocity), σε συνδυασμό με τη μεγάλη τυπολογία τους, δίνουν τις ευκαιρίες, για την καλύτερη αξιοποίηση των πόρων των τεχνολογιών της πληροφορίας και της επικοινωνίας αλλά και βελτιστοποιούν την εξατομίκευση των υπηρεσιών ηλεκτρονικής διακυβέρνησης στον δημόσιο τομέα. Οι μεγάλες προκλήσεις διαχείρισης των δεδομένων συμβάλλουν στην οικοδόμηση της κατάλληλης κυβερνητικής διάρθρωσης, στην ενσωμάτωση διαφορετικών πηγών δεδομένων, στη διαχείριση της ψηφιακής ιδιωτικότητας, στην αποτροπή των απειλών που σχετίζονται με την ασφάλεια και στην απόκτηση μεγάλων δεξιοτήτων και εργαλείων δεδομένων, κατά την συμμόρφωσή τους με τον Κανονισμό (GDPR). Η εκπόνηση μιας αποτελεσματικής στρατηγικής διαχείρισης δεδομένων σε συνδυασμό με τη μόχλευση και την ιεράρχηση των μεγάλων δεδομένων, θα συμβάλλει καθοριστικά στην ανάπτυξη των δομών, κατάλληλα προσανατολισμένων στην νέα εποχή της ψηφιακής δικαιοσύνης.

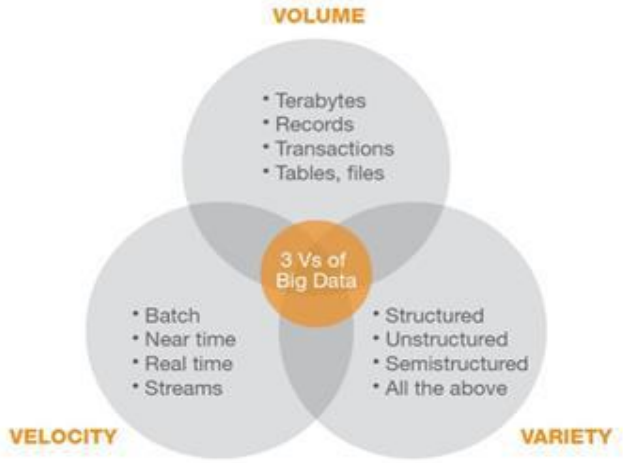
1.1 Ορισμός

Αν και η ακριβής φύση και η οριοθέτηση των Big Data εξακολουθεί να είναι ασαφής ,τα Big Data ή αλλιώς "Μεγάλα Δεδομένα", είναι ένας όρος που περιγράφει τον τεράστιο όγκο δεδομένων, δομημένων και μη δομημένων, τα οποία είναι σχεδόν αδύνατον να επεξεργαστούν και αναλυθούν με τις παραδοσιακές μεθόδους. Συχνά, ο όρος αναφέρεται στην εκθετική ανάπτυξη, τόσο της διαθεσιμότητας των δεδομένων, όσο και της αυτοματοποιημένης χρήση πληροφοριών από αυτά. Οι ανάγκες της σύγχρονης ψηφιακής εποχής, με την κατακόρυφη πτώση του κόστους αποθήκευσης, την τεράστια αύξηση της επεξεργαστικής ισχύος και την ταχεία εμφάνιση και αξιοποίηση νέων τεχνολογιών μέσω διαδικτύου, δημιουργούν μια ταχύτατη έκρηξη παραγωγής, επεξεργασίας και χρήσης των δεδομένων.

1.2 Χαρακτηριστικά

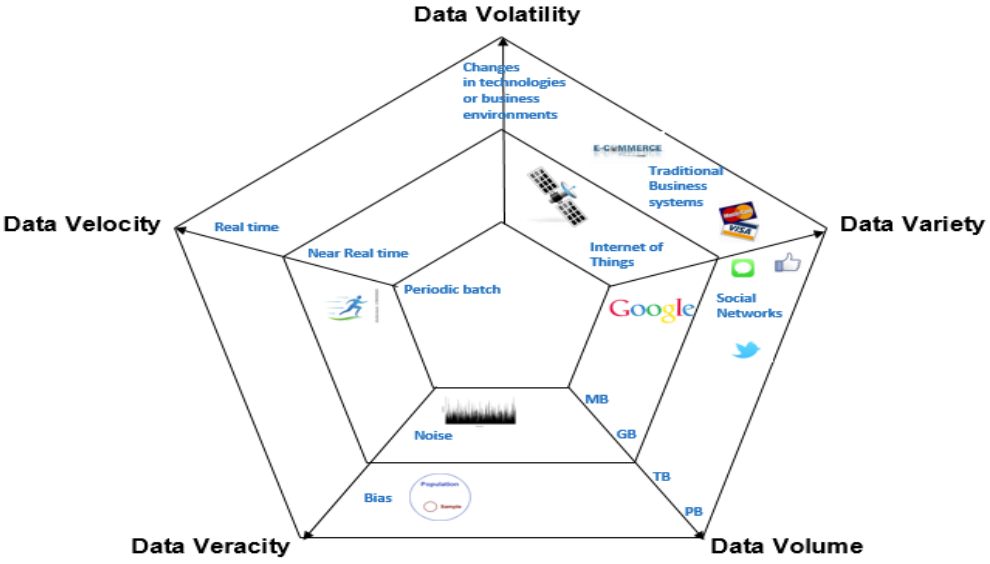
Τα τρία βασικά χαρακτηριστικά [3],[9],[15] των μεγάλων δεδομένων είναι ο όγκος (Volume), η ταχύτητα (Velocity) και η ποικιλία (Variety). Αναλυτικότερα ο όγκος αναφέρεται στο μέγεθος των δεδομένων και σχετίζεται με τη λήψη, την αποθήκευση και την ανταλλαγή πληροφοριών, επεκτείνοντας έτσι σημαντικά την ικανότητα των τυπικών εργαλείων λογισμικού για βάσεις δεδομένων αλλά και τη διαχείριση – ανάλυση των δεδομένων. Η ταχύτητα ως ένα άλλο χαρακτηριστικό των μεγάλων δεδομένων, αναφέρεται πάντα σε πραγματικό ή σχεδόν πραγματικό χρόνο, κατά τον οποίο τα δεδομένα συναλλάσονται, ιδίως μέσα από το χώρο του διαδικτύου και συγκεκριμένα των on line εφαρμογών. Η ποικιλία ορίζει τη φύση των δεδομένων που υπάρχουν στα μεγάλα δεδομένα και περιλαμβάνει τις διαφορετικές μορφές δεδομένων, τη σημασιολογία τους καθώς και τις δομές τους. Προσανατολίζεται στην παροχή διαφορετικών τεχνικών για την επίλυση και τη διαχείριση της ποικιλίας των δεδομένων, όπως τεχνικές ευρετηρίασης για τη σύνδεση δεδομένων με διαφορετικούς και ασύμβατους τύπους, προφίλ δεδομένων για την εύρεση αλληλεξαρτήσεων και ανωμαλιών μεταξύ πηγών δεδομένων, την εισαγωγή δεδομένων σε καθολικά αποδεκτές και χρησιμοποιήσιμες μορφές, όπως η Extensible Markup Language (XML) και τη διαχείριση μεταδεδομένων με σκοπό την επίτευξη συνεκτικότητας των δεδομένων.

Αξιοσημείωτο χαρακτηριστικό, εξάλλου, αποτελεί η ασφάλεια και προστασία των προσωπικών δεδομένων, καθώς νέες προκλήσεις και πρότυπα αναπτύχθηκαν και δημιουργήθηκαν αναφορικά με τα δεδομένα ασφάλειας, μέσω της ανάπτυξης και χρήσης της τεχνολογίας των μεγάλων δεδομένων, κάτι που δημιουργεί μια αυξανόμενη ανάγκη για περαιτέρω έρευνα, σχετικά με τεχνολογίες ασφάλειας, ικανών να χειριστούν τις τεράστιες ποσότητες δεδομένων, διασφαλίζοντας την αποτελεσματικότητά τους. Ωστόσο, τα χαρακτηριστικά των μεγάλων δεδομένων έχουν αυξηθεί με την πάροδο του χρόνου, δίνοντας έμφαση στις ευκαιρίες αλλά και στις προκλήσεις που οι φορείς καλούνται να αντιμετωπίσουν, κατά την ενσωμάτωση τους, στις υπάρχουσες δραστηριότητες τους (Εικόνα 1-1).



Εικόνα 1-1 : The 3 V's of big data
Πηγή: Gustav Stigestadh Felix Moberg, sping semester 2018, "Big data, for better or worse: GDPR support for the individual"

Η φιλαλήθεια (Veracity) αναφέρεται στο θόρυβο, τις προκαταλήψεις και τις ανωμαλίες, που ενδεχομένως να προκαλέσει η αποθήκευση και η εξαγωγή των δεδομένων, γεγονός που συνδέεται με την αξία και το κύρος των μεγάλων δεδομένων. Ο καθορισμός στρατηγικής με σκοπό τη διατήρηση "καθαρών δεδομένων", αποτελεί πρόκληση για την παγίωση της αξιοπιστίας κάθε φορέα. Η μεταβλητότητα (Volatility), αναφέρεται στο χρονικό διάστημα αποθήκευσης των δεδομένων, ώστε αυτά να αποτελούν χρήσιμες πηγές δεδομένων για τον χρήστη και να μην οδηγούν σε διαχειριστικές ευπάθειες, όπως μη έγκυρες αναλύσεις και αποτελέσματα.



Εικόνα 1-2 : 5V's of Big Data
Πηγή:Cornelia L. Hammer, Diane C. Kostroch, Gabriel Quirós, and STA Internal Group ,2017, "Big Data: Potential, Challenges, and Statistical Implications"

Τα μεγάλα δεδομένα περιλαμβάνουν συνεχώς όλο και περισσότερα σύνολα δεδομένων με μεγάλο όγκο, πέρα από την ικανότητα των εργαλείων λογισμικού, που χρησιμοποιούνται για τη λήψη, την επεξεργασία, τη διαχείριση και την επεξεργασία των δεδομένων σε αποδεκτά χρονικά διαστήματα. Ένα τεράστιο σύνολο δεδομένων δημιουργείται κάθε δευτερόλεπτο από κάθε μέρος του κόσμου, με αποτέλεσμα, ο όγκος των δεδομένων να μη μπορεί ποτέ να μειωθεί αλλά να αυξάνεται καθημερινά, προσθέτοντας συνεχώς νέα χαρακτηριστικά, ικανά να παρέχουν έναν ευρύ ερευνητικό ορίζοντα, κατάλληλο για κάθε φορέα με αποστολή την αποτελεσματικότερη διαχείριση των μεγάλων δεδομένων. Ο παρακάτω πίνακας συνοψίζει μια πρόσφατη έρευνα που απαριθμεί δεκατέσσερα (14) χαρακτηριστικά των Big Data.

Πίνακας 1-1: 14 V's of Big Data
Πηγή: Arockia Panimalar.S 1, Varnekha Shree.S2, Veneshia Kathrine.A3 , Sep-2017, "The 17 V's Of Big Data"

Big data 14 v' s			
	Big data Χαρακτηριστικά	***Διευκρίνιση***	***Περιγραφή***
1	***Volume***	Μέγεθος των δεδομένων	Ποσότητα των συλλεγόμενων και αποθηκευμένων δεδομένων
2	***Velocity***	Ταχύτητα των δεδομένων	Ο ρυθμός μεταφοράς των δεδομένων μεταξύ πηγής και προορισμού
3	***Value***	Σημαντικότητα των δεδομένων	Η επιχειρησιακή αξία της πληροφορίας που προέρχεται από τα μεγάλα δεδομένα
4	***Variety***	Τυπολογία των δεδομένων	Διαφορετικοί τύποι των δεδομένων ήχος, εικόνα
5	***Veracity***	Ποιότητα των δεδομένων	Ακριβής ανάλυση για την χρησιμότητα των δεδομένων
6	***Validity***	Αυθεντικότητα των δεδομένων	Ακρίβεια των δεδομένων με σκοπό την εξαγωγή ασφαλών αποτελεσμάτων
7	***Volatility***	Διάρκεια χρησιμότητας των δεδομένων	Καθορισμός χρονικού διαστήματος χρησιμότητας των δεδομένων για τον χρήστη
8	***Visualization***	Απεικόνιση των διαδικασιών των δεδομένων	Κατανοητή και οπτικοποιημένη αναπαράσταση των δεδομένων, για την πιο εύκολη συλλογή τους από τον χρήστη
9	***Virality***	Ταχύτητα εξάπλωσης των δεδομένων	Ο ρυθμός με τον οποίο τα δεδομένα μεταδίδονται / διαδίδονται από ένα χρήστη και λαμβάνονται από διάφορους χρήστες
10	***Vagueness***	Ασάφεια δεδομένων	Η έννοια του ότι βρέθηκαν δεδομένα είναι συχνά ασαφής ανεξάρτητα από τη διαθεσιμότητα των δεδομένων.
11	***Variability***	Διαφοροποίηση των δεδομένων	Τα δεδομένα που προέρχονται από διαφορετικές πηγές, διαχωρίζονται σε σημαντικά ή μη.
12	***Venue***	Διαφορετικές πλατφόρμες	Διάφοροι τύποι δεδομένων από διαφορετικές πηγές μέσω διαφορετικών πλατφορμών
13	***Vocabulary***	Ορολογία των δεδομένων	Η ορολογία δεδομένων μοιάζει με μοντέλο δεδομένων και δομές δεδομένων
14	***Complexity***	Συσχέτιση των δεδομένων	Τα δεδομένα προέρχονται από διαφορετικές πηγές και είναι απαραίτητο να καταλάβουμε τις αλλαγές, μικρές ή μεγάλες, συγκριτικά με τα δεδομένα που έχουν φτάσει προηγουμένως, με σκοπό τη γρήγορη εξαγωγή πληροφοριών

1.3 Τυπολογία

Παρά το γεγονός, ότι ο όρος Big Data, είναι πολύ γενικός, η τυπολογία [15],[26] τους περιλαμβάνει πέντε κατηγορίες, ανάλογα με τους σκοπούς που εξυπηρετούν και τα δεδομένα που αναλύονται σε αυτούς. Συγκεκριμένα, έχουμε τα:

Μεγάλα δεδομένα (Big Data), δηλαδή τα κλασικά δεδομένα, που με το τεράστιο πεδίο εφαρμογής τους, αναφέρονται στην ανάλυση και επεξεργασία της πληροφορίας, με στόχο την αποκάλυψη των τάσεων ή την επέκταση των ορίων της επιστημονικής γνώσης, εξάγοντας δεδομένα και θεραπεύοντας προβλήματα.

Νέα δεδομένα (New Data) δηλαδή πληροφορίες που αναζητούμε και μπορούμε να πάρουμε, οι οποίες όμως πιθανόν να μην έχουν εξαχθεί πρόσφατα.

Γρήγορα δεδομένα (Fast Data), δηλαδή μεγάλα σύνολα δεδομένων, τα οποία περιστρέφονται γύρω από το γεγονός ότι μπορούν να δώσουν μια αρκετά γρήγορη αλλά εμπεριστατωμένη απάντηση, σχεδόν σε πραγματικό χρόνο.

Χαμένα δεδομένα (Lost Data) ή λειτουργικά δεδομένα, δηλαδή πληροφορίες που βρίσκονται σε εξοπλισμούς, μηχανήματα και τεχνολογικά αντικείμενα μέσα σε κτίρια ή βιομηχανικές εγκαταστάσεις (πχ αισθητήρες), οι οποίες είναι απομονωμένες σε λειτουργικά συστήματα.

Σκοτεινά δεδομένα (Dark Data)**,** δηλαδή πληροφορίες για τις οποίες δεν έχουμε εύκολη πρόσβαση, όπως ροές βίντεο, φωτογραφίες, χειρόγραφες σημειώσεις.

1.4 Ανάλυση

Ανεξάρτητα από το μέγεθος ή τον τύπο των δεδομένων που συλλέγονται, είναι αρκετά σημαντική και η εμπεριστατωμένη ανάλυσή τους [7], με σκοπό την απόκτηση ουσιωδών αποτελεσμάτων και συμπερασμάτων, εφαρμόσιμων από τους εμπλεκόμενους φορείς. Οι αναλύσεις αυτές απεικονίζουν τα δεδομένα σε μια ποικιλία μοντέλων, τα οποία καθιστούν δυνατή την πρόβλεψη γεγονότων ανάλογα με τον τομέα στον οποίο απευθύνονται και των διαδικασιών, βάσει των οποίων επεξεργάζονται. Μερικοί τύποι ανάλυσης των Big Data είναι:

• Η χρήση αλγορίθμων

Όταν η ανάλυση δεδομένων γίνεται παραδοσιακά, αποφασίζεται μετά το πέρας της, το τι πρέπει να βρεθεί μέσω της ανάλυσης και στη συνέχεια μέσω ερωτημάτων, ανακτώνται οι επιθυμητές πληροφορίες. Η ανάλυση των μεγάλων δεδομένων με χρήση αλγορίθμων, σπάνια ξεκινά με ένα προκαθορισμένο ερώτημα, το οποίο περιλαμβάνει ένα

μεγάλο αριθμό αλγορίθμων που τρέχουν μαζί σε μια μεγάλη ποσότητα δεδομένων . Αυτό πραγματοποιείται προκειμένου να βρεθεί μια σειρά από ομοιότητες, συνδέσεις και σχέδια.

• Η αδιαφάνεια της επεξεργασίας

Οι πιο προηγμένοι τύποι μηχανικής μάθησης ονομάζονται τύποι βαθιάς εκμάθησης, που σημαίνει ότι τεράστια ποσά δεδομένα περνούν μέσα από ένα μη γραμμικό νευρωνικό δίκτυο, το οποίο ταξινομεί τα δεδομένα για κάθε στρώμα, από το οποίο αποτελείται. Η μεγάλη πολυπλοκότητα αυτού του τύπου επεξεργασίας, του δίνει τη δυνατότητα να αποτελεί ένα είδος "μαύρου κουτιού", κάτι που σημαίνει ότι μπορεί να είναι δύσκολο να κατανοήσουμε, το γιατί λαμβάνονται οι διάφορες αποφάσεις μέσα από τα αποτελέσματα της επεξεργασίας των δεδομένων με τον τρόπο αυτό. Ορισμένα συστήματα μπορούν συχνά να πάρουν περίεργες αποφάσεις, οι οποίες είναι δυσνόητες πολλές φορές για τον άνθρωπο, γεγονός που επεκτείνει την ανάλυση των μεγάλων δεδομένων πέρα από τον παραδοσιακό τρόπο.

• Η τάση χρησιμοποίησης όλων των δεδομένων

Η ανάλυση μεγάλων δεδομένων αφορά περισσότερο την ανάλυση και εξαγωγή συμπερασμάτων όλων των διαθέσιμων δεδομένων .Αρκετές όμως είναι οι φορές που κρίνεται επιτακτική η ανάγκη, για εύρεση στατιστικώς αντιπροσωπευτικών δειγμάτων ή τυχαίας επιλογής τους, κατά την ανάλυση στοιχείων στα πλαίσια μιας έρευνας. Αυτό έχει σαν συνέπεια την διευκόλυνση της αποθήκευσης και της ανάλυσης μιας συνεχώς αυξανόμενης ποσότητα δεδομένων.

• Ανακύκλωση δεδομένων

Ένα ακόμα μεγάλο πλεονέκτημα της χρήσης της ανάλυσης των Big Data είναι η επαναχρησιμοποίηση των δεδομένων, η οποία δίνει πολλές ευκαιρίες στο να βρεθούν νέες ιδέες και σχέδια, μέσα από την ενδελεχή ανάλυση τους, μολονότι αρχικά φαίνονταν αρκετά διαφοροποιημένα.

• Ανάλυση κειμένου

Η πραγματοποίηση ανάλυσης κειμένων που παράγονται από ανθρώπους, μέσα από ιστολόγια, φόρουμ, ηλεκτρονικά μηνύματα ή από οργανισμούς, οδηγεί στην

εξαγωγή χρήσιμων συμπερασμάτων και στη λήψη ταχύτερων και ορθότερων αποφάσεων.

• Καταγραφή ήχου (απομαγνητοφώνηση)

Στα πλαίσια της ένταξης των δικαστικών υπηρεσιών στη σύγχρονη ψηφιακή εποχή, η λειτουργία της ηχητικής καταγραφής και μετέπειτα απομαγνητοφώνησης, μιας ακροαματικής διαδικασίας, συμβάλλει καθοριστικά, στην συλλογή και μετατροπή σε κείμενο των φωνητικών δεδομένων, ώστε αυτά να αποτελέσουν ένα αυθεντικό αποδεικτικό των πεπραγμένων μέσα στην αίθουσα του δικαστηρίου, με σκοπό την εξαγωγή τεκμηριωμένων συμπερασμάτων, που θα περιέχονται στην απόφαση.

• Ανάλυση βίντεο

Η ανάλυση των βίντεο υπήρξε πολύ πριν την ανάλυση των Big Data, παρέμενε όμως δύσκολη λόγω του τεράστιου όγκου δεδομένων που παράγονται από τα βίντεο, καθώς ένα δευτερόλεπτο βίντεο υψηλής ανάλυσης αντιπροσωπεύει περίπου πάνω από 2000 σελίδες γραπτού κειμένου. Στα μελλοντικά σχέδια του ψηφιακού δικαστηρίου, είναι και η χρήση έξυπνων αλγόριθμων, οι οποίοι θα εκτελούν αναλύσεις εικόνας βίντεο κατά την ακροαματική διαδικασία και θα μπορούν να μετατρέπουν σε κείμενο, το οποίο θα αποθηκεύεται στη βάση δεδομένων, τις εξ' αποστάσεως καταθέσεις μαρτύρων και κατηγορουμένων.

Δεδομένου ότι η ηλεκτρονική διακυβέρνηση εστιάζει στην παροχή υπηρεσιών με επίκεντρο τον πολίτη και την πληροφόρηση του, τα μεγάλα δεδομένα πρέπει να αξιοποιούνται σε βάθος από τους δημόσιους φορείς, με στόχο την ασφαλή αποθήκευση και διαχείριση διαφόρων ειδών δεδομένων ακόμα και σε πραγματικό χρόνο.

1.5 Ευκαιρίες

Η ορθή ενσωμάτωση των μεγάλων δεδομένων [15], δίνει σε κάθε πολίτη μια σημαντική ευκαιρία συμμετοχής στις παρεχόμενες ηλεκτρονικές υπηρεσίες, με την αύξηση της χρήσης τους και την έκταση των πληροφοριακών συστημάτων που λειτουργούν για την εξυπηρέτησή του. Η μεγάλη ποσότητα των δεδομένων που συλλέγονται από τα πληροφοριακά συστήματα , προσφέρουν μια εξατομικευμένη προβολή όλων των υπηρεσιών, πλήρως οργανωμένων βάσει ημερομηνίας και τύπου υπηρεσίας. Επιπλέον, τα μεγάλα δεδομένα μπορούν επίσης να αυξήσουν την ταχύτητα ροής πληροφοριών και αναλύσεων, αυξάνοντας σημαντικά με δυναμικές προσαρμογές,

την λειτουργικότητα της ψηφιακής διακυβέρνησης, όπως η δυνατότητα αξιοποίησης στο έπακρο, online υπηρεσιών. Ιδιαίτερα χρήσιμη είναι και η ταχύτητα των μεγάλων δεδομένων ιδίως σε καταστάσεις έκτακτης ανάγκης. Μια άλλη ευκαιρία για μεγάλα δεδομένα είναι η αύξηση της αποτελεσματικότητας των κυβερνητικών εργασιών με τη χρήση επιχειρησιακών αναλύσεων, κάτι που θα δώσει τη δυνατότητα για ένα αποτελεσματικότερο σχεδιασμό και για μια πιο στοχευμένη υλοποίηση, των κρατικών ψηφιακών υπηρεσιών, συμβάλλοντας από τη μια στην αύξηση της διαφάνειας, της συμμετοχής και της συνεργασίας και αυξάνοντας από την άλλη το ποσοστό ικανοποίησης των πολιτών. Η απελευθέρωση των μεγάλων δεδομένων δίνει μια μεγάλη ευκαιρία για συνεργασία μεταξύ της κυβέρνησης και των πολιτών, με κύριο σκοπό την ανάπτυξη χρήσιμων, ασφαλών και ελεύθερων εφαρμογών, ικανών να παρέχουν υπηρεσίες ακόμα και σε πραγματικό χρόνο.

1.6 Προκλήσεις

Είναι σαφές πως για μια ψηφιακή κυβέρνηση, η πρώτη και πιο σημαντική πρόκληση, κατά την αξιοποίηση των μεγάλων δεδομένων, είναι η διακυβέρνηση, η οποία περιλαμβάνει προκλήσεις με εσωτερικές και εξωτερικές πτυχές. Η εσωτερική πτυχή αναφέρεται στη λήψη αποφάσεων, βάσει δεδομένων σύμφωνα, όμως με την κύρια αρχή διακυβέρνησης, καθώς η χρήση των μεγάλων δεδομένων, δεν θα δημιουργήσει πρόσθετες δημόσιες αξίες, εάν αυτά δεν χρησιμοποιούνται με στόχο, τη βελτίωση των δημόσιων υπηρεσιών.

Επιπλέον, μια ακόμη εσωτερική πτυχή, αποτελεί η ανάγκη για τον καθορισμό των ρόλων και των ευθυνών κατά τη διαχείριση των μεγάλων δεδομένων. Όσο αφορά τις εξωτερικές πτυχές, το θέμα της διακυβέρνησης εστιάζει στο πλήθος των φορέων που συμμετέχουν και στην ανάγκη για την ενσωμάτωση διάφορων πηγών δεδομένων, με προοπτική τη δημιουργία μεγάλων δεδομένων και την εύκολη πρόσβαση σε αυτά. Ωστόσο, οι πολίτες αντιτάσσονται σε μια τέτοια εύκολη δημόσια ηλεκτρονική πρόσβαση σε πληροφορίες ιδιοκτησίας, επικαλούμενοι τη προστασία της ιδιωτικής ζωής.

Ένα άλλο θέμα που σχετίζεται με εξωτερικές πτυχές της διακυβέρνησης, είναι η ενσωμάτωση των δεδομένων μεταξύ φορέων του δημοσίου, η οποία τυπικά απαιτεί τη σύναψη συμφωνιών αλλά και τη εισαγωγή προτύπων και μηχανισμών ανταλλαγής δεδομένων. Φυσικά η ανάπτυξη αυτών των συμφωνιών για την ενοποίηση των δεδομένων, ως ένα νέο πλαίσιο διακυβέρνησης, κρύβει δυσκολίες λόγω των ποικίλων

προσδοκιών των ενδιαφερομένων μερών και των διαφορετικών προδιαγραφών των δεδομένων.

Μια δεύτερη βασική πρόκληση για την αξιοποίηση της δυναμικής των μεγάλων δεδομένων, αφορά την αναζήτηση καταρτισμένου προσωπικού, την ανάπτυξη της τεχνολογίας και ουσιαστικών πηγών. Η ανάλυση των μεγάλων δεδομένων απαιτεί εξειδικευμένα άτομα, προκειμένου το αποτέλεσμα της ανάλυσης να πάρει την αξία που του αναλογεί, μέσα από μια μεγάλη ποσότητα αδόμητων δεδομένων.

Σχετικά με το θέμα της τεχνολογίας εξετάζονται δύο πλευρές. Η μία είναι ο αναπτυσσόμενος χαρακτήρας των μεγάλων δεδομένων και των τεχνολογιών ανάλυσης. Όπως είδαμε και παραπάνω, ο όγκος, ταχύτητα και η ποικιλία των μεγάλων δεδομένων καθιστούν ορισμένα παραδοσιακά συστήματα βάσεων δεδομένων αναποτελεσματικά, όπως για παράδειγμα, παραδοσιακές βάσεις δεδομένων δεν έχουν έναν εύκολο τρόπο ανάλυσης των δεδομένων τους. Επειδή τα περισσότερα από τα μεγάλα δεδομένα είναι αδόμητα (blog post) και με κοινωνικό χαρακτήρα (μέσα κοινωνικής δικτύωσης), η χρήση παραδοσιακών τεχνικών ανάλυσης δεδομένων χωρίς στοιχεία ανάλυσης δικτύου είναι λιγότερο αποτελεσματική.

Η άλλη είναι η ποικιλία αρχιτεκτονικών αναφοράς και πλατφορμών κατάλληλων για τα μεγάλα δεδομένα, κάτι που αυξάνει την πολυπλοκότητα των τεχνολογικών λύσεων. Η πρόκληση για τους δημόσιους φορείς είναι η επιλογή της κατάλληλης πλατφόρμας (πχ cloud-based), του κατάλληλου λογισμικού (open source) και των κατάλληλων ατόμων για την ανάπτυξη και διαχείριση της βάσης δεδομένων, βασισμένη στις ανάγκες του εκάστοτε φορέα.

Η τρίτη πρόκληση των μεγάλων δεδομένων, σχετίζεται με την ασφάλεια και πιο συγκεκριμένα με τη διαχείρισή των κινδύνων της ιδιωτικής ζωής, καθώς η προστασία των προσωπικών δεδομένων αποτελεί έναν πονοκέφαλο για τα μεγάλα δεδομένα, δεδομένου ότι τα μεγάλα δεδομένα περιέχουν μια ποικιλία τύπων δεδομένων όπως εικόνες, χρονοδιαγράμματα, πληροφορίες από online δραστηριότητες. Επιπλέον, η νέα φύση των μεγάλων δεδομένων συνεπάγεται επίσης ότι οι ισχύοντες νόμοι και κανονισμοί ήταν σχετικά αδύναμοι να αντιμετωπίσουν τις σύγχρονες απειλές για τα δεδομένα της ιδιωτικής ζωής. Η ανησυχία για τη ψηφιακή ασφάλεια είναι ανάλογη με το μεγάλο μέγεθος και την υψηλή αξία των μεγάλων δεδομένων, ιδίως όταν αυτά γίνονται στόχος από κακόβουλους εισβολείς. Οι πολλαπλές πηγές ροών δεδομένων καθώς και η ένταξη διαφόρων τύπων δεδομένων δημιουργεί επιπρόσθετα πολλαπλά σημεία ευπάθειας. Είναι

σίγουρο πως μια ψηφιακή απειλή μπορεί να εκδηλωθεί μέσω οποιουδήποτε από αυτά τα σημεία που αναφέραμε. Δεδομένου λοιπόν του μεγέθους, της πολυπλοκότητας και της ανάλυσης των μεγάλων δεδομένων, η πρόκληση ανάγεται στην οικοδόμηση ενός συστήματος ανίχνευσης εισβολής και αντιμετώπισης απειλών, ως ένας τρόπος διασφάλισης των δεδομένων. Ο παρακάτω πίνακας αποτελεί μια περίληψη των προκλήσεων ή ζητημάτων που συνδέονται με τα μεγάλα δεδομένα στη δημόσια διοίκηση και περιλαμβάνει τη διαχείριση των μεγάλων δεδομένων, τη ζήτηση για υλοποίηση αυτών και τη διαχείριση των κινδύνων.

Πίνακας 1-2: Οι προκλήσεις των μεγάλων δεδομένων για τη δημόσια διοίκηση
Πηγή: Yu-Che Chen, *Tsui-Chuan Hsieh,*"Big Data for Digital Government: Opportunities, Challenges, and Strategies"

Προκλήσεις	***Διαστάσεις***	***Περιγραφή***
Διαχείριση μεγάλων δεδομένων	Εσωτερική	Η καλλιέργεια και η εδραίωση μιας κουλτούρας για τη λήψη αποφάσεων, με βάση τα μεγάλα δεδομένα
	Εξωτερική	Διαχείριση και ενοποίηση δημοσίων πηγών δεδομένων
Ανάγκη για αξιοποίηση των μεγάλων δεδομένων	Ικανότητα	Έλλειψη επιστημόνων δεδομένων (data scientists)
	Τεχνολογία	Ανυπαρξία πλατφορμών διαχείρισης και ανάλυσης δεδομένων και εφαρμογών
	Πόροι	Περιορισμένη διαθεσιμότητα πόρων για την απόκτηση ικανοτήτων, υιοθέτηση τεχνολογιών και υλοποίηση εφαρμογών
Διαχείριση κινδύνου	Ιδιωτικότητα	Προφίλ ατόμων ως αποτέλεσμα εξατομίκευσης
	Ασφάλεια	Αυξημένη ευπάθεια λόγω του συνδυασμού των διαφόρων πηγών δεδομένων με μεταβλητά πρότυπα, πρακτικές ασφαλείας και την αξία των μεγάλων δεδομένων

1.7 Στρατηγικές

Θεμελιώδες στρατηγικό στοιχείο [15] για μία πετυχημένη διοίκηση των μεγάλων δεδομένων είναι η κατάλληλη δομή διακυβέρνησης. Μια τέτοια δομή θα πρέπει να προσδιορίσει τα ενδιαφερόμενα μέρη και τις αντίστοιχες ευθύνες τους σχετικά με τα μεγάλα δεδομένα. Μια πιο σύνθετη, συνεπάγεται τη δημιουργία επιτροπών επίβλεψης των ομάδων εργασίας και διαχείρισης των Big Data. Η επιτροπή πρέπει να περιλαμβάνει ικανά και καταρτισμένα άτομα σε τομείς όπως η ασφάλεια, η πληροφόρηση, η τεχνολογία, και άλλες περιοχές που καλύπτουν όλο το φάσμα των μεγάλων δεδομένων.

Μια άλλη ουσιαστική παράμετρος, είναι η ανάπτυξη ικανοτήτων στην επιχειρηματική ευφυΐα και τα analytics. Όλοι οι εμπλεκόμενοι φορείς θα πρέπει να εκπαιδευτούν για να κατανοήσουν τη σχέση, το είδος των δεδομένων και των απαιτούμενων εργαλείων, με κατευθυντήρια γραμμή την αντιμετώπιση των προκλήσεων στον τομέα της τεχνολογίας και των διαθέσιμων πόρων που αναφέρθηκαν νωρίτερα.

Μια μεγάλη στρατηγική δεδομένων απαιτεί, επίσης, μία έξυπνη εφαρμογή για να αξιοποιηθούν όλες οι δυνατότητές τους. Παρόλο που επικρατεί η έννοια του όγκου, η καλύτερη στρατηγική είναι να διερευνηθεί πώς η ταχύτητα και η ποικιλία των Big Data λειτουργούν ως προσθετική αξία. Για μια επιτυχή εφαρμογή, θα πρέπει να επιλεχθούν τα σωστά δεδομένα από πολλαπλές πηγές και ο κάθε εμπλεκόμενος, να παράγει ιδέες, σχετικά με την έξυπνη χρήση τους, με γνώμονα τη μεγιστοποίηση του αντίκτυπου των μεγάλων δεδομένων. Προσφάτως, έχει αναδειχθεί και η σημασία της καινοτομίας προς αυτή την κατεύθυνση.

Κεφάλαιο 2: Big Data & GDPR

Εισαγωγή

Τον Απρίλιο του 2016, μετά από πολυετείς διαπραγματεύσεις, η Ευρωπαϊκή Ένωση (ΕΕ) ενέκρινε τελικά τον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων γνωστό ως General Data Protection Regulation (GDPR) [5], με την ουσιαστική εφαρμογή του να ξεκινά το Μάιο του 2018. Από τότε, οι ρυθμιστικές αρχές, οι επιχειρήσεις και οι δημόσιοι φορείς της Ευρώπης, θέτουν ως πρωταρχικό έργο τους την εναρμόνιση και συμμόρφωση με το νέο νομικό καθεστώς, έτσι όπως αυτό ορίζεται από το GDPR. Δεδομένου ότι ο κανονισμός είναι ίσως το πιο ολοκληρωμένο και προοδευτικό νομοσχέδιο για την αντιμετώπιση των προκλήσεων που σχετίζονται με τη προστασία δεδομένων στην ψηφιακή εποχή, είναι σίγουρο ότι ο αντίκτυπος του θα είναι, κατά πάσα πιθανότητα, μεγάλος σε όλους τους τομείς, που έχουν ως αντικείμενό τους, τη διαχείριση, επεξεργασία και αποθήκευση προσωπικών δεδομένων.

Το GDPR τίθεται σε ισχύ σε μια κρίσιμη στιγμή για την παγκόσμια ψηφιακή κοινότητα, η οποία καλείται, από τη μια, να αντιμετωπίσει όλους τους αναδυόμενους κινδύνους που σχετίζονται με τα δικαιώματα και τις ελευθερίες των ατόμων, ενώ, από την άλλη, θέλει να αξιοποιήσει όλες τις ευκαιρίες για τη δημιουργία αξιών, την προώθηση της ευημερίας, το αίσθημα ασφάλειας και την ενίσχυση διαφόρων κοινωνικών στόχων, σε ένα ταχέως μεταβαλλόμενο ψηφιακό περιβάλλον.

Η μεγαλύτερη πρόκληση που καλείται να αντιμετωπίσει ο γενικός κανονισμός προστασίας δεδομένων, είναι ίσως η παρουσία των μεγάλων δεδομένων και αυτό διότι ο όρος αναφέρεται στις πρακτικές δημιουργίας και ανάλυσης τεράστιων συνόλων δεδομένων, οι οποίες ενίοτε περιλαμβάνουν προσωπικές πληροφορίες. Μια διαδικασία ανάλυσης των Big Data μπορεί πιθανόν να αποβεί επιβλαβής για τα άτομα των οποίων τα δεδομένα αναλύονται ή και να επηρεάσει έμμεσα κάποια άλλα μέσα από τις αναλύσεις αυτές, γεγονός που συνθέτει ένα νέο πλαίσιο εφαρμογής εννοιολογικών και πρακτικών αλλαγών, στο ισχύον νομικό καθεστώς.

2.1 Επιρροή του GDPR στα μεγάλα δεδομένα

Η εισαγωγή του γενικού κανονισμού [22] σηματοδοτεί την απαρχή μιας τεκτονικής αλλαγής στον τρόπο συλλογής, ανάλυσης και εφαρμογής των δεδομένων. Ορίζοντας την έννοια των "μεγάλων δεδομένων", αναφερόμαστε στον όγκο των δεδομένων που συλλέγονται, στην ποικιλία των πηγών, στην ταχύτητα με την οποία

μπορεί να γίνει η ανάλυση των δεδομένων αλλά και στην εγκυρότητα αυτών που θα μπορούσε να επιτευχθεί, αναμφισβήτητα, μέσω της αναλυτικής διαδικασίας.

Καθώς, οι αναλύσεις των Big Data οδηγούνται από αυτοματοποιημένες διαδικασίες, εισάγουν μια ευρεία ποικιλία πρακτικών, ενώ το πεδίο εφαρμογής τους περιλαμβάνει δύο ειδικά χαρακτηριστικά:

α) διαδικασίες οι οποίες βασίζονται και παράγουν, αντίστοιχα, δεδομένα και πληροφορίες προσωπικού χαρακτήρα, με τη διαπίστωση της διευρυμένης έννοιας αυτών.

β) περιπτώσεις στις οποίες τα αποτελέσματα και οι αναλύσεις των μεγάλων δεδομένων εφαρμόζονται σε συγκεκριμένα άτομα, με άμεση επιρροή σ' αυτά.

Η χρήση των Big Data συμβάλλει όχι μόνο στην αποδοτικότητα αλλά και στη σταδιακή προσαρμογή όλων των εμπλεκόμενων φορέων, στις νέες συνθήκες που διαμορφώνει η ψηφιακή εποχή. Ωστόσο, καθώς η γοητεία και η προοπτική τους εντάθηκαν, ο σκεπτικισμός για τυχόν αρνητικούς αντίκτυπους, αποτελεί ένα φυσικό επακόλουθο.

Ως εκ τούτου, η ανάλυση των μεγάλων δεδομένων που περιλαμβάνουν προσωπικές πληροφορίες είναι ιδιάζουσας σημασίας και επηρεάζεται από την έκταση της εκάστοτε πολιτικής προστασίας δεδομένων. Από τη μία πλευρά, οι προηγμένες μορφές αναλύσεων, μπορούν να θέσουν σε κίνδυνο την ιδιωτική ζωή των ατόμων και τα δικαιώματά τους. Στον αντίποδα, οι αυστηροί νόμοι περί προστασίας δεδομένων, εμποδίζουν τη ροή τους καθώς και τους τρόπους που θα μπορούσαν να αναλύονται και να χρησιμοποιούνται.

Οι συντάκτες του GDPR κλήθηκαν να εξισορροπήσουν τη ρυθμιστική ικανότητα του κανονισμού να ασχοληθεί με την πλήρη ανάλυση των δεδομένων και την προστασία της ιδιωτικής ζωής, των συμφερόντων και των δικαιωμάτων των πολιτών, προσπαθώντας να διατηρηθεί μια ισορροπία των αδυναμιών. Η έλευση του GDPR ενέτεινε την προαναφερθείσα διένεξη, η οποία έχει προκαλέσει έντονη διχογνωμία, στον κύκλο των θεωρητικών. Το πώς θα επιτευχθεί η απαιτούμενη ισορροπία είναι μείζον ζήτημα, εάν αναλογιστεί κανείς και τις παρακάτω περιπτώσεις ασυμβατότητας.

2.2 Γιατί τα μεγάλα δεδομένα προκαλούν προβλήματα στο πεδίο εφαρμογής του GDPR;

Η χρήση των μεγάλων δεδομένων [22] που συγκρίνονται και αναλύονται προκειμένου να ληφθούν βέλτιστες αποφάσεις, εμπλέκουν και μια πιθανή σκοτεινή πλευρά στα γενικότερα οφέλη τους, την επίδραση στη ιδιωτική ζωή. Τίθεται όμως το ερώτημα: Το GDPR οφελή τα μεγάλα δεδομένα ή θα επιφέρει ένα καίριο πλήγμα στη χρησιμότητα τους στη προσπάθεια προστασίας του απορρήτου;

Αδιαμφισβήτητα, τα μεγάλα δεδομένα περιλαμβάνουν συχνά προσωπικά δεδομένα, τα οποία σε πολλές περιπτώσεις δεν είναι δυνατό να διαχωριστούν από τα μη προσωπικά δεδομένα. Στόχος των Big Data είναι να αποκαλύψουν τις σχέσεις εντός και μεταξύ των πληροφοριών, μέσω της ανάλυσης και της επεξεργασίας, βασιζόμενα στην ακεραιότητα του εξαγόμενου αποτελέσματος. Το σημείο εκκίνησης όμως των μεγάλων δεδομένων αντιβαίνει σε μια θεμελιώδη αρχή του GDPR , ότι η ακεραιότητα των δεδομένων προσωπικού χαρακτήρα ενός συγκεκριμένου προσώπου, πρέπει να διατηρείται και να προστατεύεται.

Μερικοί από τους κινδύνους για την προστασία της ιδιωτικής ζωής ιδιαίτερα έντονοι στο πλαίσιο της δημιουργίας μεγάλων δεδομένων περιλαμβάνουν, συνεπώς, τα εξής:

- Επεξεργασία προσωπικών δεδομένων εκτός του σκοπού για τον οποίο συλλέχθηκαν.
- Χρήση λανθασμένων και ξεπερασμένων πληροφοριών
- Διακρίσεις ή προκαταλήψεις κατά ορισμένων ατόμων ή ομάδων που προκύπτουν από την εφαρμογή ορισμένων αλγορίθμων δημιουργίας προφίλ.
- Επεξεργασία δεδομένων προσωπικού χαρακτήρα πέρα από αυτό που απαιτείται για την επεξεργασία τους.

Συνεπώς, η ισχύς του GDPR αφορά όχι μόνο το σύνολο των δεδομένων που δημιουργήθηκαν πρόσφατα αλλά και αυτά που ήδη υπάρχουν, εφόσον θα αποτελέσουν αντικείμενο επεξεργασίας. Με τον τρόπο αυτό καθίσταται προβληματική η απόκτηση της απαιτούμενης ρητής συγκατάθεσης για συγκεκριμένες χρήσεις ενός συνόλου δεδομένων που υπάρχει ήδη σε χρήση.

2.3 Ενδεικτικές περιπτώσεις ασυμβατότητας

Ο Κανονισμός για την προστασία των δεδομένων, έρχεται σε αντίθεση με πολλές πρακτικές των Big Data [12]. Η διατήρηση των ισορροπιών όχι μόνο δεν έχει υλοποιηθεί στον απαιτούμενο βαθμό αλλά διαπιστώνονται περιπτώσεις που υπονομεύουν την ικανότητα άσκησης ανάλυσης των μεγάλων δεδομένων. Ο ισχυρισμός αυτός αποδεικνύεται, πέρα από κάθε αμφιβολία, με την παραπομπή στις βασικές διατάξεις του περιορισμού του σκοπού, της ελαχιστοποίησης των δεδομένων, των ειδικών κατηγοριών και των αυτοματοποιημένων αποφάσεων.

Μετά από ενδελεχή μελέτη, παρατηρεί κανείς ότι όλες οι ρυθμίσεις ταυτίζονται κατά περιεχόμενο με τις νομικές έννοιες που αναφέρονται στη γενική Οδηγία για την προστασία των δεδομένων (Data Protection Directive, DPD) καθώς και στην ευρωπαϊκή νομοθεσία, χωρίς να διακρίνεται κάποια ουσιώδης διαφοροποίηση. Εκείνο που χρειάζεται να αναφερθεί είναι ότι, κατά τις διαδικασίες επικύρωσης του GDPR, προσμετρήθηκε η σκοπιμότητα και τα οφέλη των αναλύσεων των μεγάλων δεδομένων. Από τα παραπάνω, προκύπτει μια σαφής ένδειξη έγκρισης αυτών των εννοιών, οι οποίες αναδιατυπώνονται στο νόμο, με διαφοροποίηση όμως σε βασικές διαδικαστικές καινοτομίες.

Βελτίωση αυτής συνιστά το GDPR, το οποίο αποβλέπει σε ένα ευρύτερο πεδίο εμπλεκόμενων φορέων που ασχολούνται με την ανάλυση μεγάλων δεδομένων, αναδεικνύοντας την Οδηγία σε νομοθέτημα μείζονος σημασίας. Εκείνο που προέχει είναι η ευαισθητοποίηση των υπευθύνων σχετικά με τους επικείμενους κινδύνους ως προς την προστασία των δεδομένων, η οποία υλοποιείται μέσω της συμμόρφωσης με το GDPR.

Για τη θεμελίωση της ασυμβατότητας, χρήζει η αναφορά των οικείων διατάξεων, με έμφαση στην αιτιολογητική τους βάση, στη σύνδεσή τους με τα Big Data, στα ενδεχόμενα προβλήματα που προκαλεί το GDPR καθώς και στις ελλείψεις που ήδη υπάρχουν στο νόμο.

Ειδικότερα, το άρθρο 5 παρ. 1 στοιχείο β' του γενικού κανονισμού, αναφερόμενο στο περιορισμό του σκοπού της επεξεργασίας των προσωπικών δεδομένων, εισάγει τη θεμελιώδη έννοια ότι αυτά, πρέπει να συλλέγονται για "ειδική, ρητή και νόμιμη" επεξεργασία και πως δεν μπορούν να "τροποποιηθούν" περαιτέρω, με τρόπο "ασυμβίβαστο" ως προς τους πρωτότυπους σκοπούς.

Όμως, η απαιτούμενη συμμόρφωση με τις περιγραφόμενες προδιαγραφές έρχεται σε ευθεία αντίθεση με τη δυναμική προοπτική των Big Data αναλύσεων, στις οποίες

εφαρμόζονται μέθοδοι και πρότυπα που καθιστούν αδύνατη, είτε για το φορέα είτε για το υποκείμενο των δεδομένων, την, οριοθέτηση των μελλοντικών μορφών επεξεργασίας, επιτείνοντας, ακόμη περισσότερο, την ανάγκη για ορισμό του επιτρεπόμενου πεδίου αναλύσεων, πέραν του οποίου τίθεται, η διασφάλιση των προσωπικών δεδομένων.

Στη συνέχεια, το άρθρο 5 παρ. 1 στοιχείο γ' του γενικού κανονισμού, εστιάζει στην αρχή της ελαχιστοποίησης των δεδομένων, διατυπώνοντας το δικαίωμα ότι πρέπει να είναι "περιορισμένα σε ό,τι είναι απαραίτητο, σε σχέση με τους σκοπούς για τους οποίους είναι η επεξεργασία".

Η τήρηση της συγκεκριμένης αρχής επικεντρώνεται στο στάδιο συγκέντρωσης των δεδομένων, το οποίο διασφαλίζεται με τη χρονική διάρκεια κατά την οποία μπορούν να διατηρηθούν και ολοκληρώνεται με την απαίτηση για διαγραφή τους, μετά την προβλεπόμενη χρήση. Στην ουσία, αποτελεί ένα έμμεσο τρόπο αποφυγής φαινομένων παραβίασης του απορρήτου των χρηστών και παράλληλα απειλή κατά της ασφάλειας των δεδομένων.

Όπως γίνεται αντιληπτό, η ελαχιστοποίηση των δεδομένων μπορεί να μειώνει τις προαναφερθείσες ανησυχίες, ωστόσο, εναντιώνεται στις πρακτικές ανάλυσης των μεγάλων δεδομένων, οι οποίες έχουν ως πρωταρχικό μέλημα τη μείωση του υψηλού κόστους συλλογής αλλά και την ενίσχυση της άποψης ότι ο επαυξημένος όγκος αυτών συμβάλλει θετικά στην άντληση γνώσης, με τεράστια οφέλη για τους φορείς και την κοινωνία.

Σ' αυτό ακριβώς το σημείο και για να κατευναστούν οι όποιες αντιρρήσεις, προστέθηκαν ρητές εξαιρέσεις, που επιτρέπουν την ανάλυση μεγάλων δεδομένων, υπό το καθεστώς του "στατιστικού σκοπού", με την προϋπόθεση ότι η ελαχιστοποίηση τελικά λειτουργεί μέσω της διαδικασίας της "ψευδονημίας", δηλαδή της εφαρμογής διασφαλίσεων, οι οποίες δεν επιτρέπουν την αναγνώριση των προσώπων στα οποία αναφέρονται τα δεδομένα.

Το άρθρο 9 του GDPR, απαγορεύει την επεξεργασία παρόμοιων "ειδικών κατηγοριών", προσθέτοντας γενετικά και βιομετρικά δεδομένα, με σκοπό τη μοναδική αναγνώριση ενός φυσικού προσώπου και στοιχεία σχετικά με το σεξουαλικό προσανατολισμό του ατόμου.

Η επεξεργασία τέτοιων πληροφοριών εξακολουθεί να είναι δυνατή, υπό τον όρο της "ρητής συγκατάθεσης" ή εφόσον αφορά "ειδικές" κατηγορίες, οι οποίες δεν εξειδικεύονται, σε περίπτωση που η προαπαιτούμενη συναίνεση χαρακτηρίζεται, ως

δυσχερής και χρονοβόρα διαδικασία. Εκείνο που υπάρχει ως πρόβλεψη είναι η δυνατότητα των κρατών - μελών να θεσπίσουν πρόσθετες παραμέτρους προστασίας για αυτές τις κατηγορίες, προκειμένου να αποφευχθεί ο κίνδυνος διάδοσης ή διαρροής τέτοιου είδους δεδομένων. Απόρροια αυτού, αποτελεί η καθιέρωση νέων πρακτικών για βελτιωμένα αναλυτικά στοιχεία, τα οποία, με τη σειρά τους, κατηγοριοποιούν τα δεδομένα σε "ειδικά" και "τακτικά", παρά το γεγονός ότι κάτι τέτοιο, επιβαρύνει τις διαδικασίες ανάλυσης των Big Data, δημιουργώντας λάθος συσχετισμούς, μεταξύ των δεδομένων και των κατηγοριών, απαιτώντας αφενός την εφαρμογή ενός διαφορετικού συνόλου νομικών κανόνων και υπονομεύοντας δυνητικά αφετέρου τη συνολική διάκρισή τους.

Χαρακτηριστικό παράδειγμα διένεξης GDPR και Big Data είναι η ρύθμιση που περιγράφεται στο άρθρο 22, σύμφωνα με την οποία διατηρείται, με εμφανή τρόπο, ο έντονος σκεπτικισμός αναφορικά με τις αυτοματοποιημένες διαδικασίες, ιδίως όταν αυτές παράγουν ως αποτέλεσμα ανάλυσης την έννοια του "προφίλ" , δηλαδή ενός αλγοριθμικού συμπεράσματος που προέρχεται από δεδομένα σχετικά με ένα άτομο. Η έννοια αυτή χρησιμοποιείται ευρέως στην προσπάθεια αύξησης των ωφέλιμων χρήσεων της ανάλυσης των μεγάλων δεδομένων. Ωστόσο, ορισμένες χρήσεις της, μπορούν να παρουσιάσουν κινδύνους, όπως η έλλειψη διαφάνειας, η πληροφοριακή ανισορροπία, η διάβρωση των αρχών προστασίας δεδομένων, οι ψευδείς συσχετισμοί και τα αδικαιολόγητα αποτελέσματα διακρίσεων.

Για το λόγο αυτό, τίθεται σε εφαρμογή ειδικός κανόνας που διέπει διαδικασίες λήψης αποφάσεων, πλήρως αυτοματοποιημένων, συμπεριλαμβανομένης της μορφοποίησης. Ακόμη και όταν ισχύουν οι προβλεπόμενες εξαιρέσεις, παρέχονται στο υποκείμενο των δεδομένων, σημαντικά δικαιώματα, όπως αυτό της παρέμβασης και της αμφισβήτησης της απόφασης. Και, τούτο, διότι οι αυτοματοποιημένες επεξεργασίες πραγματοποιούνται χωρίς να γνωστοποιούνται επαρκώς σε όσους επηρεάζονται από αυτές, η έλλειψη δε εποπτείας προκαλεί ανησυχία και εγείρει επιφυλάξεις για τα αποτελέσματά τους.

Εύλογη, λοιπόν, διαφαίνεται η απαίτηση για ενεργή συμμετοχή των υποκειμένων, στο στάδιο της έκδοσης αποφάσεων από μηχανές ανάλυσης δεδομένων, υπό την έννοια ότι οι διαδικασίες των Big Data, θα πρέπει να διεξάγονται με τέτοιο τρόπο, ώστε να επιβεβαιώνουν την ικανότητα ερμηνείας τους από αυτό, γεγονός που θέτει σε κίνδυνο την ακρίβεια του συστήματος και εντείνει τη δυναμική της ανθρώπινης

παρέμβασης, η οποία μπορεί να αποτελέσει τροχοπέδη στην εισαγωγή καινοτόμων τεχνολογιών.

2.4 Χρήση των μεγάλων δεδομένων στο πλαίσιο του GDPR

Είναι επιτακτική ανάγκη, οι φορείς να επανεξετάσουν την τρέχουσα χρήση των πρακτικών επεξεργασίας χαρακτηριστικών και των αυτοματοποιημένων διαδικασιών [22], με σκοπό:

- Να προσδιορίσουν που πρέπει να γίνεται χρήση αυτών των προσεγγίσεων επεξεργασίας και εάν υπάρχουν προσωπικά δεδομένα.
- Να κατανοήσουν τις απαιτούμενες εργασίες, σχετικά με τα σύνολα δεδομένων, έτσι ώστε να επιτρέπεται η χρήση τους σύμφωνα με το πρότυπο GDPR, συμπεριλαμβανομένης της ενδεχόμενης χρήσης ψευδωνυμοποίησης των προσωπικών δεδομένων.
- Να κατανοήσουν τα αποτελέσματα της χρήσης της αυτοματοποιημένης επεξεργασίας, ιδίως όταν επηρεάζουν "νόμιμα ή σημαντικά συμφέροντα".
- Να εξασφαλίσουν την εφαρμογή έγκυρης νομικής βάσης στη χρήση προφίλ δηλαδή ρητής και έγκυρης συγκατάθεσης του προσώπου στο οποίο αναφέρονται τα δεδομένα ή που εμπίπτουν στην "εξαίρεση απο τη σύμβαση".
- Να παρέχουν στο υποκείμενο των δεδομένων πληροφορίες σχετικά με την αλγοριθμική λογική που χρησιμοποιείται και τις συνέπειες αυτής.
- Να βεβαιωθούν ότι υπάρχουν διαδικασίες που επιτρέπουν την ανθρώπινη παρέμβαση σε μια απόφαση που λαμβάνεται βάσει αυτοματοποιημένης επεξεργασίας.

2.5 Στατιστικά στοιχεία παραβίασης δεδομένων προσωπικού χαρακτήρα στην Ελλάδα

Σύμφωνα με τη Γ/ΕΞ/10281/20-12-2018, ανακοίνωση της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα [27], ως εποπτική αρχή του Κανονισμού σύμφωνα με το άρθρο 33 αυτού στη χώρα μας, κατά τους πρώτους έξι μήνες εφαρμογής του Κανονισμού (ΕΕ) 2016/679 (Γενικού Κανονισμού Προστασίας Δεδομένων), υποβλήθηκαν 66 γνωστοποιήσεις περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα. Σε 36 από τις περιπτώσεις αυτές οι "υπεύθυνοι επεξεργασίας δεδομένων", με βάση το άρθρο 34 του Κανονισμού και με την καθοδήγηση της Αρχής σε

πολλές περιπτώσεις, προχώρησαν σε ανακοίνωση του περιστατικού στα επηρεαζόμενα φυσικά πρόσωπα.

Ο αριθμός των υποβληθεισών γνωστοποιήσεων ανά μήνα εμφανίζεται στον παρακάτω πίνακα.

Πίνακας 2-1: Υποβληθείσες γνωστοποιήσεις
Πηγή: https://www.taxheaven.gr/news/news/view/id/43234#

Μήνας	Αριθμός Γνωστοποιήσεων
Μάιος 2018	1
Ιούνιος 2018	9
Ιούλιος 2018	7
Αύγουστος 2018	9
Σεπτέμβριος 2018	6
Οκτώβριος 2018	22
Νοέμβριος 2018	12

Μέχρι σήμερα η Αρχή έχει εκδώσει τρεις αποφάσεις τις υπ'αριθμ. 67, 68 και 69/2018, οι οποίες σχετίζονται με τα ανωτέρω περιστατικά, ενώ τουλάχιστον άλλα 9 εξετάζονται περαιτέρω. Παράλληλα, για 6 από τα περιστατικά συνεργάζεται με τις συναρμόδιες αρχές της Ευρωπαικής Ένωσης.

2.6 Συμβουλές της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Η Αρχή εφιστά την προσοχή σε "υπευθύνους επεξεργασίας" και "εκτελούντες την επεξεργασία δεδομένων" για τα εξής:

- ✓ Ο ανθρώπινος παράγοντας αποτελεί βασική πηγή κινδύνων, η οποία εκδηλώνεται με:

α) την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν δεδομένα προσωπικού χαρακτήρα σε λανθασμένο σύνολο αποδεκτών, και

β) την εξαπάτηση χειριστών ηλεκτρονικών υπολογιστών από κακόβουλα μηνύματα που μπορεί να οδηγήσουν σε εγκατάσταση κακόβουλου λογισμικού τύπου ransomware ή malware.

Η Αρχή συστήνει την υλοποίηση δράσεων ευαισθητοποίησης των χρηστών για την κατανόηση και αντιμετώπιση των εν λόγω κινδύνων.

- ✓ Σημαντικός αριθμός περιστατικών παραβίασης οφείλεται στο χρησιμοποιούμενο λογισμικό. Οι "υπεύθυνοι" και "εκτελούντες την επεξεργασία δεδομένων προσωπικού χαρακτήρα" οφείλουν να:

α) φροντίζουν να ελέγχουν πλήρως κάθε νέα έκδοση λογισμικού πριν τη χρήση του και να διαθέτουν διαδικασία για την άμεση αντιμετώπιση προβλημάτων που θα ανακύψουν κατά την παραγωγική του λειτουργία,

β) ελέγχουν τις ρυθμίσεις των διακομιστών διαδικτύου που χρησιμοποιούν ώστε να μην καθίστανται προσβάσιμες μη δημόσιες πληροφορίες, και

γ) παρακολουθούν και επικαιροποιούν άμεσα το λογισμικό με κάθε νέα έκδοση ασφάλειας, όταν αυτή καταστεί διαθέσιμη.

- ✓ Εμφανίστηκαν, επίσης, περιστατικά κλοπής ή απώλειας ηλεκτρονικών υπολογιστών και αποθηκευτικών μέσων.

  Η Αρχή συστήνει τη χρήση λογισμικού κρυπτογράφησης.

Συμπέρασμα

Πρέπει να καταστεί σαφής η σημασία του GDPR για τα μεγάλα δεδομένα. Η ανάγκη για συμμόρφωση με το γενικό κανονισμό, δε θα σημάνει την υποβάθμιση των μεγάλων δεδομένων, αλλά αντίθετα θα θέσει τις βάσεις προκειμένου οι νέοι κανονισμοί, να βασιστούν στη χρήση των μεγάλων δεδομένων. Οι μελλοντικές εφαρμογές των Big Data θα πρέπει να είναι δεοντολογικές και να υπόκεινται σε λεπτομερέστερο έλεγχο προκειμένου να διασφαλιστεί η συμμόρφωση τους με το νόμο, κάτι που για όσους ασχολούνται με την επεξεργασία των δεδομένων, απαιτεί μια λεπτομερή ενημέρωση των πεπραγμένων, κατά την ανάλυση αυτών.

Σημαντικό κομμάτι της συμμόρφωσης θα είναι η ανωνυμοποίηση των δεδομένων, κάτι που μεταφράζεται σε απόρριψη των αναγνωρίσιμων πληροφοριών προτού καν ξεκινήσει μια διαδικασία επεξεργασίας. Η διαφάνεια θα είναι, επίσης, σημαντική για τη διασφάλιση της συμμόρφωσης, τονίζοντας την εμφάνιση του τόπου και του τρόπου συλλογής των δεδομένων.

Η εφαρμογή του GDPR δεν θα θέσει τέλος στα μεγάλα δεδομένα, ούτε πρόκειται να τα επηρεάσει αρνητικά. Μπορεί να επιβραδύνει τη ταχύτητα επεξεργασίας και να αποτρέψει τις ασυνείδητες πρακτικές, αλλά θα καταστήσει τους εμπλεκόμενους με τη

διαδικασία επεξεργασίας δεδομένων, πιο υπεύθυνους για τα δεδομένα που συλλέγουν και επεξεργάζονται, ενισχύοντας έτσι τα συμπεράσματα που θα προκύψουν και τις μελλοντικές προβλέψεις. Η ανωνυμοποίηση των δεδομένων, θα μειώσει το αντίκτυπο μιας μεγάλης παραβίασης ασφάλειας, ενθαρρύνοντας όλους τους φορείς στο να δημιουργήσουν συστήματα που συμμορφώνονται με τον κανονισμό, αλλάζοντας ριζικά τον τρόπο συλλογής, διατήρησης και πρόσβασης στα δεδομένα.

Σαφώς και υπάρχουν συγκεκριμένες προκλήσεις όσον αφορά τον συνδυασμό των αρχών προστασίας δεδομένων που ορίζονται στο GDPR, με τα χαρακτηριστικά των μεγάλων δεδομένων. Δεν είναι, όμως, ανυπέρβλητες, ούτε ασυμβίβαστες με τους στόχους του GDPR. Θα πρέπει, ωστόσο, να γίνει κατανοητή η σημαντικότητα των μεγάλων δεδομένων, ως το κλειδί για τη ραγδαία αύξηση της ανταλλαγής δεδομένων και της δομημένης πληροφόρησης, υπό το πρίσμα της συμμόρφωσης με την προστασία της ιδιωτικής ζωής, σηματοδοτώντας την απαρχή της νέας ψηφιακής εποχής στη δημόσια διοίκηση και ειδικότερα στο χώρο της δικαιοσύνης.

Κεφάλαιο 3: Λογισμικά συμμόρφωσης με GDPR

Εισαγωγή

Η διαρκής ψηφιακή επανάσταση σηματοδοτεί μια νέα εποχή στη διαχείριση των δεδομένων. Η χρήση των Big Data και των συναφών τεχνολογιών έχει φέρει ριζική ανατροπή στην καθημερινότητά μας καθώς, πλέον, περισσότερο από ποτέ, όλοι είναι σε θέση να αντιληφθούν το βαθύτερο νόημά τους, με αναγωγή στα τεράστια ποσά δεδομένων που διατίθενται σε διάφορους φορείς, υπό τις κατάλληλες μορφές. Εκείνο που χρήζει ιδιαίτερους χειρισμούς και επηρεάζει την αποτελεσματικότητα της χρήσης των μεγάλων δεδομένων, είναι η συλλογή, επεξεργασία και αποθήκευση, σύμφωνα με τη φύση τους.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), από το Μάιο του 2018, έρχεται, να επιβάλλει σε όλους τους φορείς που διαχειρίζονται, προσωπικά δεδομένα, κανόνες συμμόρφωσης, ώστε να τηρούνται και να διαφυλάσσονται θεμελιώδη δικαιώματα των πολιτών, όπως τα ευαίσθητα προσωπικά δεδομένα τους και η ιδιωτικότητα της ζωής τους. Στο παρόν κεφάλαιο, επιχειρείται μια πρότυπη προσέγγιση της εφαρμογής του κανονισμού της Ευρωπαϊκής Ένωσης, στη νέα εποχή της ψηφιακής δικαιοσύνης.

Η επιλεγείσα μελέτη περίπτωσης εισάγει τη χρήση λογισμικού, πλήρως συμμορφωμένου με την οδηγία, στη διαδικασία έκδοσης πιστοποιητικών του Πρωτοδικείου Θεσσαλονίκης, ώστε να εκτιμηθεί και να καθοριστεί με σαφήνεια, η θέσπιση του κατάλληλου κώδικα δεοντολογίας, η τρέχουσα κατάσταση του συστήματος διαχείρισης δεδομένων, οι κίνδυνοι που ελλοχεύουν, ο σχεδιασμός μέτρων πρόληψης και ανάσχεσης των απειλών κατά της έκθεσης των δεδομένων, η ανάθεση ρόλων σε όλους τους εμπλεκόμενους και το αντίκτυπο των επιπτώσεων της προστασίας των προσωπικών δεδομένων, με απώτερο σκοπό την εναρμόνιση του φορέα με τη κοινοτική οδηγία, αλλά και την εξασφάλιση της ακεραιότητας και εμπιστευτικότητας των δεδομένων των πολιτών.

3.1 Λογισμικά συμμόρφωσης με GDPR

Η επιλογή του κατάλληλου λογισμικού ως προς, τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), αποτελεί ένα από τα πιο σημαντικά στάδια κατά την εκκίνηση ένταξης, του εκάστοτε φορέα, στο ευρύτερο πλαίσιο για την

προστασία και διαχείριση των προσωπικών δεδομένων, βάσει των οδηγιών της Ευρωπαϊκής Κοινότητας.

Μετά από ενδελεχή έρευνα, η παρούσα εργασία [17] παραθέτει με μορφή πινάκων τα δημοφιλέστερα και πλήρως εναρμονισμένα με το GDPR, προγράμματα επεξεργασίας προσωπικών δεδομένων δύο τύπων, των οποίων τα κυριότερα χαρακτηριστικά έχουν ως εξής:

Πίνακας 3-1: Closed Source Software
Πηγή: https://www.capterra.com/gdpr-compliance-software

ΛΟΓΙΣΜΙΚΟ	ΠΕΡΙΓΡΑΦΗ	ΤΙΜΗ	ΔΟΚΙΜΑΣΤΙΚΗ ΕΚΔΟΣΗ	ΕΓΚΑΤΑΣΤΑΣΗ / ΥΠΗΡΕΣΙΕΣ	Χαρακτηριστικά συμμόρφωσης GDPR
iGrafx	Λειτουργίες μοντελοποίησης, εντοπισμός και μετριασμός των κινδύνων, επίτευξη συμμόρφωσης και αυτοματοποίηση επιχειρηματικών διαδικασιών, σύμφωνα με τους κανόνες του GDPR.	Δεν παρέχεται	ΝΑΙ	Cloud SaaS Web Windows	√ Έλεγχος πρόσβασης √ Χαρτογράφηση δεδομένων √ PIA / DPIA √ Διαχείριση πολιτικής √Διαχείριση κινδύνου
ECOMPLY	Λογισμικό συμμόρφωσης GDPR για μικρές και μεσαίες επιχειρήσεις το οποίο περιλαμβάνει 1) Εγγραφές των δραστηριοτήτων επεξεργασίας 2) Διαχείριση προμηθευτών 3) Εποπτεία DPO 4) DPIA 5) Διαχείριση Συναίνεσης	49 €/μήνα (1 χρήστης) 99 €/μήνα (5 χρήστες)	ΝΑΙ	Cloud SaaS Web	√ Διαχείριση Συναίνεσης √ Χαρτογράφηση δεδομένων √ Διαχείριση περιστατικών √ PIA / DPIA √ Διαχείριση πολιτικής √ Διαχείριση κινδύνου

GDPR365	Λογισμικό που βασίζεται σε σύννεφο, το οποίο αξιολογεί την κατάσταση της συμμόρφωσης με το GDPR, δημιουργεί ένα χάρτη πορείας για να συμμορφώνεται με τους κανονισμούς και να τεκμηριώνει τις προσπάθειες.	56,00 $/μήνα ή 48,94 €/μήνα	ΝΑΙ	Cloud SaaS Web	√ Διαχείριση Συναίνεσης √ Χαρτογράφηση δεδομένων √ Διαχείριση περιστατικών √ PIA / DPIA √ Διαχείριση πολιτικής √ Διαχείριση κινδύνου
OneTrust	Πλατφόρμα διαχείρισης απορρήτου δεδομένων για τη συμμόρφωση με τους κανονισμούς περί απορρήτου δεδομένων, συμπεριλαμβανομένων του GDPR.	550,00 $ /μήνα ή 480,83€/μήνα	ΟΧΙ	Cloud SaaS Web	√ Έλεγχος πρόσβασης √ Διαχείριση Συναίνεσης √ Χαρτογράφηση δεδομένων √ Διαχείριση περιστατικών √ PIA / DPIA √ Διαχείριση κινδύνου
TrustArc the new TRUSTe	Ευέλικτο και κλιμακωτό λογισμικό για τη συμμόρφωση με το GDPR και τη διαχείριση των κινδύνων, με ολοκληρωμένη τεχνολογία, συμβουλευτικές υπηρεσίες και επικύρωση GDPR TRUSTe, τα οποία καλύπτουν όλες τις φάσεις διαχείρισης δεδομένων, βάσει του κανονισμού GDPR.	Δεν παρέχεται	ΟΧΙ	Cloud SaaS Web	√ Έλεγχος πρόσβασης √ Διαχείριση Συναίνεσης √ Χαρτογράφηση δεδομένων √ Διαχείριση περιστατικών √ PIA / DPIA √ Διαχείριση πολιτικής √ Διαχείριση κινδύνου √ Ευαίσθητα δεδομένα

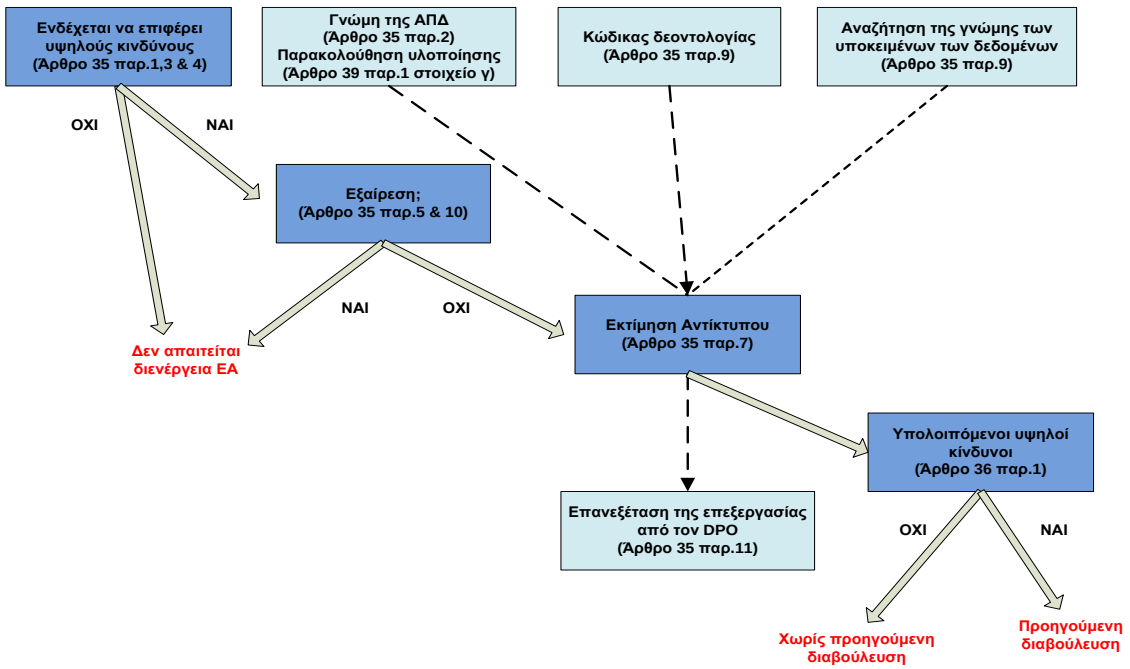
Πίνακας 3-2: Open Source Software
Πηγή: https://www.capterra.com/gdpr-compliance-software

ΛΟΓΙΣΜΙΚΟ	ΠΕΡΙΓΡΑΦΗ	ΤΙΜΗ	ΔΟΚΙΜΑΣΤΙΚΗ ΕΚΔΟΣΗ	ΕΓΚΑΤΑΣΤΑΣΗ / ΥΠΗΡΕΣΙΕΣ	Χαρακτηριστικά συμμόρφωσης GDPR
BLACKDUCK by synopsys	Παρέχει λύσεις διαχείρισης και ελέγχου ασφαλείας των προσωπικών δεδομένων, καθώς και διαχείριση του συνολικού κινδύνου ασφάλειας των εφαρμογών επεξεργασίας προσωπικών δεδομένων, διατηρώντας τη συμμόρφωση με το GDPR.	ΔΩΡΕΑΝ	ΟΧΙ	SaaS	√ Αυτοματοποιημένη διαχείριση ευπάθειας κατά την ανάπτυξη εφαρμογών επεξεργασίας προσωπικών δεδομένων. √ Συνεχής παρακολούθηση για νέες ευπάθειες που επηρεάζουν τις εφαρμογές επεξεργασίας προσωπικών δεδομένων. √ Έλεγχος των κανόνων ασφαλείας ως προς τη συμμόρφωση τους με το GDPR, για την προστασία της ιδιωτικότητας των δεδομένων.
OpenProject	Λογισμικό για την ασφάλεια των προσωπικών δεδομένων και των διαδικασιών επεξεργασίας τους, βάσει των νομικών απαιτήσεων και της σημασίας για τη προστασία της ιδιωτικότητας των δεδομένων που ορίζει το GDPR.	ΔΩΡΕΑΝ Community Version	ΟΧΙ	MySQL with Apache server Docker Engine Linux	√ Πολιτικές ασφαλείας και προστασίας απορρήτου. √ Φυσική ασφάλεια. √ Επιχειρησιακές διαδικασίες ασφαλείας √ Αξιοπιστία της αρχιτεκτονικής του συστήματος √ Ανάπτυξη και συντήρηση συστημάτων √ Τακτικοί έλεγχοι ασφάλειας και προστασίας της ιδιωτικότητας των δεδομένων
PONTUS VISION	Πλατφόρμα πλήρους ανοικτού κώδικα για, την αποτελεσματική διαχείριση, των προσωπικών δεδομένων με ασφάλεια, τηρώντας τον κανονισμό συμμόρφωσης του GDPR.	ΔΩΡΕΑΝ	ΝΑΙ	Cloud Linux servers	√ Βαθμολογίες συμμόρφωσης GDPR για κάθε ένα από τα 12 βήματα της διαδικασίας συμμόρφωσης. √ Παροχή δυνατότητας αυτόματης ή μη αυτόματης εκτέλεσης αιτήσεων πρόσβασης των προσώπων στα δεδομένα που τους αφορούν. √ Ανάλυση παραβίασης δεδομένων. √ Καταγραφή των επιπτώσεων των προσωπικών δεδομένων έπειτα από παραβιάσεις ασφαλείας.
snyk	Λογισμικό που περιέχει εργαλεία πλήρως επικεντρωμένα στους προγραμματιστές - διαχειριστές, των βάσεων προσωπικών δεδομένων, διατηρώντας σε υψηλό επίπεδο τις διαδικασίες ενημέρωσης και ασφάλειας τους, σύμφωνα με το GDPR.	ΔΩΡΕΑΝ Free plan version	ΝΑΙ	PaaS Serverless	√ Παρακολούθηση γνωστών τρωτών σημείων στις βάσεις διαχείρισης και αποθήκευσης προσωπικών δεδομένων. √ Εύκολος εντοπισμός τρωτών σημείων, επιδιόρθωση και παρεμπόδιση εισαγωγής νέων. √ Ενσωματωμένες ροές εργασίας και εργαλεία προγραμματιστή. √ Ανάπτυξη μεθόδων ασφάλειας των προσωπικών δεδομένων σε υψηλή κλίμακα.

3.2 Η σημασία της Εκτίμησης Αντίκτυπου Προσωπικών Δεδομένων

Ένα από τα πλέον ουσιώδη χαρακτηριστικά συμμόρφωσης με τον Γενικό Κανονισμό, είναι η Εκτίμηση Αντίκτυπου. Στοιχεία αυτής εντοπίζονται σε όλο το Κανονισμό, γεγονός που αποδεικνύει ότι συνιστά μια δυναμική διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία των προσωπικών δεδομένων, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται αυτή (άρθρο 35 παρ. 1, το οποίο επεξηγείται από την παρ. 3 και συμπληρώνεται από την παρ. 4), αξιολογώντας και καθορίζοντας παράλληλα, τα μέτρα για την αντιμετώπισή τους (άρθρο 35 παρ. 7 και αιτιολογικές σκέψεις 84 και 90). Αποτελεί ένα σημαντικό εργαλείο καθώς συνδράμει στο έργο των υπεύθυνων επεξεργασίας, στο μέτρο της συμμόρφωσης με τις προδιαγραφές του ΓΚΠΔ, αλλά και της απόδειξης ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για τη διασφάλιση της εναρμόνισης προς τον Κανονισμό (άρθρο 24).

Η διενέργεια της Εκτίμησης Αντίκτυπου αποτελείται από βασικές αρχές, οι οποίες περιγράφονται στα άρθρα 35 και 36 και απεικονίζονται στην παρακάτω εικόνα.



Εικόνα 3-1 : Βασικές Αρχές που διέπουν την ΕΑ
Πηγή:http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/GDPR/FILES%20GDPR/WP253_EL.PDF

Μέσα από μια σύντομη επισκόπηση του ΓΚΠΔ, διαπιστώνεται ότι η υποχρεωτικότητα της ΕΑ συνδέεται με την έλευση "υψηλού" κινδύνου, ιδίως σε περίπτωση που εισάγεται μια νέα τεχνολογία επεξεργασίας δεδομένων (αιτιολογικές σκέψεις 89 και 91). Παράμετροι που προσμετρούνται είναι η ιδιαίτερη πιθανότητα και σοβαρότητα του κινδύνου, λαμβάνοντας υπόψη τη φύση, την έκταση, το πλαίσιο, τους σκοπούς της επεξεργασίας καθώς και τις πηγές του κινδύνου.

Για τη διενέργεια ΕΑ, λαμβάνονται υπόψη, μεταξύ άλλων, και τα κάτωθι κριτήρια [23]:

α) η αξιολόγηση και βαθμολόγηση των υπό επεξεργασία δεδομένων, περιλαμβανομένης της κατάρτισης προφίλ και προβλέψεων (αιτιολογικές σκέψεις 71 και 91)

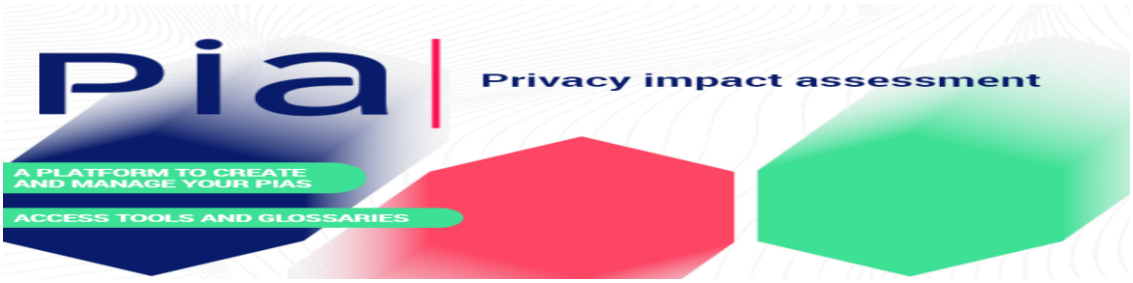
β) η λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα

γ) τα ευαίσθητα δεδομένα

δ) τα δεδομένα μεγάλης κλίμακας επεξεργασίας τα οποία αναφέρονται είτε στον αριθμό των εμπλεκόμενων υποκειμένων είτε στον όγκο των δεδομένων είτε στον απαιτούμενο χρόνο της επεξεργασίας (αιτιολογική σκέψη 91)

Η διενέργεια της Εκτίμησης Αντίκτυπου συμβάλλει καίρια στο έργο του υπεύθυνου επεξεργασίας, στο μέτρο που είναι επιφορτισμένο με τη λήψη όλων των προβλεπόμενων μέτρων και μηχανισμών που μετριάζουν τους κινδύνους, διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα και αποδεικνύουν τη συμμόρφωση προς τον Κανονισμό. Προς αυτή την κατεύθυνση, θεσπίστηκε η δυνατότητα προσφυγής σε διαβούλευση με την εποπτική αρχή, πριν την κύρωση ενός κανονιστικού μέτρου, σε περίπτωση που η διαθέσιμη τεχνολογία και το κόστος εφαρμογής δεν επαρκούν για την αντιμετώπιση των κινδύνων (αιτιολογικές σκέψεις 94, 95 και 96).

3.2.1 Παρουσίαση λογισμικού εκτίμησης αντίκτυπου δεδομένων



Στα πλαίσια της παρούσας μελέτης, επιλέχθηκε η παρουσίαση του Ανοιχτού Λογισμικού Εκτίμησης Αντίκτυπου Προσωπικών Δεδομένων Protection Impact Assesment (PIA), της Γαλλικής Εθνικής Επιτροπής για την Πληροφορική και τις Ελευθερίες (Commission Nationale de l'Informatique et des Libertés – CNIL), ως μία πρότυπη προσπάθεια υλοποίησης αυτού, στον τομέα της ψηφιακής δικαιοσύνης.

Στόχο έχει να βοηθήσει και να διευκολύνει τους Υπεύθυνους Προστασίας Δεδομένων (Data Protection Officers – DPO's), στο να δημιουργήσουν και να αποδείξουν τη συμμόρφωση του φορέα που ανήκουν με το GDPR, εκπονώντας, υπό τις οδηγίες του, αξιολογήσεις αντίκτυπου για την προστασία των δεδομένων [18]. Τα εργαλεία του λογισμικού είναι διαθέσιμα σε όλες τις γλώσσες της Ευρωπαϊκής Κοινότητας, ενώ οι εκδόσεις του ανταποκρίνονται, τόσο σε τοπική εγκατάσταση σε Η/Υ με οποιοδήποτε λειτουργικό σύστημα (Windows, Mac OS, Linux), όσο και σε εγκατάσταση σε περιβάλλον Ubuntu 17.10 server, με δυνατότητες παραμετροποίησης και προσαρμογής του κώδικα και εφαρμογές front και back end (βλ. Παράρτημα Β).

Σύμφωνα με τη CNIL, από την αρχή της εφαρμογής του Γενικού Κανονισμού, το ανοιχτό λογισμικό PIA, έχει βοηθήσει, μεταξύ άλλων, 24.500 φορείς, Αρχές Προστασίας Δεδομένων στην Ευρώπη, να ορίσουν υπεύθυνους προστασίας δεδομένων, με την Γαλλική Αρχή να έχει δεχτεί πάνω από 600 ειδοποιήσεις παραβίασης δεδομένων που αφορούν περίπου 15 εκατομμύρια άτομα, ενώ 3 εκατομμύρια επισκέψεις καταγράφηκαν στο site της, με 150.000 downloads της εφαρμογής. Για το λόγο αυτό η CNIL έχει βραβευτεί στο 40ο International Conference of Data Protection & Privacy Commissioners (ICDPPC), το 2018 στις Βρυξέλλες, με δύο βραβεία, καινοτομίας και ανάληψης ευθύνης αντίστοιχα.

3.2.2 Σε ποιούς απευθύνεται

Κυρίως σε Υπεύθυνους Προστασίας Δεδομένων Data Protection Officer (DPO), οι οποίοι είναι εξουσιοδοτημένοι για την εκτέλεση της διαδικασίας PIA, από την εκάστοτε αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων.

3.2.3 Γενική επισκόπηση λογισμικού

Το ανοικτό λογισμικό PIA της CNIL, εφαρμόζει συνεχώς βελτιώσεις σε αντικείμενα που σχετίζονται με τη δυνατότητα επιπρόσθετης μετάφρασης γλώσσας από τον DPO χρήστη, τη παρουσία εγχειρίδιου χρήσης ως πρόσθετο εργαλείο, τη παρουσία ιστορικού συνημμένων, κατά την επικύρωση της PIA, τη δυνατότητα διαφόρων προσαρμογών της τελικής προς εκτύπωση έκθεσης PIA, τη ροή εργασίας και τη βελτιστοποίηση της διεπαφής για τον DPO χρήστη. Επιπλέον, περιλαμβάνει τρεις επιμέρους κατηγορίες οδηγιών, οι οποίες μπορούν να συνδυαστούν με μια συγκεκριμένη έκδοση, σχετική με το πεδίο των διασυνδεδεμένων αντικειμένων. Οι οδηγίες αυτές αφορούν:

Κατηγορία 1η.

1. Γνωσιακή Βάση (Knowledge Base)

Πρόκειται για μια βάση νομικών [21] και τεχνικών γνώσεων, η οποία αποτελεί ένα χρήσιμο εργαλείο, καθώς περιλαμβάνει τα νομικά σημεία που εξασφαλίζουν, τη νομιμότητα της επεξεργασίας και τα δικαιώματα των υποκειμένων των δεδομένων, τα οποία είναι διαθέσιμα σε όλα τα βήματα της PIA, προσαρμόζοντας τα ανάλογα με το περιεχόμενό τους. Αναλυτικότερα περιλαμβάνει:

1.1 Βάσεις γνώσης για τη μελέτη

1.1.1 Τυπολογία των προσωπικών δεδομένων

Τα προσωπικά δεδομένα κατηγοριοποιούνται ως εξής:

- ✓ **Τύποι:**
  - Συνηθισμένα
  - Προσωπικά
  - Ευαίσθητα
- ✓ **Κατηγορίες:**

- Αστική κατάσταση, ταυτότητα, στοιχεία ταυτότητας
- Προσωπική ζωή (συνήθειες διαβίωσης, οικογενειακή κατάσταση - χωρίς ευαίσθητα ή επικίνδυνα δεδομένα)
- Επαγγελματική ζωή (βιογραφικό σημείωμα, εκπαίδευση και επαγγελματική κατάρτιση)
- Οικονομικές και χρηματοοικονομικές πληροφορίες (εισόδημα, οικονομική κατάσταση, φορολογική κατάσταση)
- Δεδομένα σύνδεσης (διευθύνσεις IP, αρχεία καταγραφής συμβάντων)
- Δεδομένα τοποθεσίας (ταξίδια, δεδομένα GPS, δεδομένα GSM)
- Αριθμός κοινωνικής ασφάλισης
- Βιομετρικά δεδομένα
- Δεδομένα τραπεζών
- Φιλοσοφικές, πολιτικές, θρησκευτικές και συνδικαλιστικές απόψεις, σεξουαλική ζωή, δεδομένα για την υγεία, φυλετική ή εθνοτική καταγωγή.
- Αδικήματα, καταδίκες, ποινικό μητρώο

1.1.2 Τυπολογία των προσωπικών δεδομένων που υποστηρίζουν τα περιουσιακά στοιχεία

- Πληροφοριακά συστήματα
  - Εξοπλισμός υλικού και ηλεκτρονικών μέσων δηλαδή υπολογιστές, δίκτυο, μονάδες USB, σκληροί δίσκοι
  - Λογισμικό όπως λειτουργικά συστήματα, βάσεις δεδομένων, επιχειρηματικές εφαρμογές
  - Υπολογιστικές δομές όπως καλώδια, WiFi, οπτικές ίνες

- Οργανισμοί
  - Ανθρώπινο δυναμικό όπως χρήστες, διαχειριστές συστήματος, υπεύθυνοι χάραξης πολιτικής
  - Τρόποι επικοινωνίας όπως e-mail, fax, ροή εργασίας

1.1.3 Τυπολογία των πηγών κινδύνου

Παρακάτω παρουσιάζονται παραδείγματα πηγών κινδύνου.

➢ **Τύποι:**

- **Εσωτερικές ανθρώπινες πηγές:** εργαζόμενοι, διαχειριστές πληροφορικής, εκπαιδευόμενοι, διευθυντές.
- **Εξωτερικές ανθρώπινες πηγές:** οι παραλήπτες προσωπικών δεδομένων, εξουσιοδοτημένα τρίτα μέρη, πάροχοι υπηρεσιών, χάκερ, επισκέπτες, πρώην εργαζόμενοι, προσωπικό συντήρησης.
- **Μη ανθρώπινες πηγές:** κακόβουλα λογισμικά άγνωστης προέλευσης (virus, worms, malware), φυσικές καταστροφές.

1.1.4 Τυπολογία των αποτελεσμάτων των επικίνδυνων ενεργειών

Ένα επικίνδυνο συμβάν διαφοροποιείται ως προς τις συνέπειες, εάν προκύψει:

✓ Αθέμιτη πρόσβαση σε προσωπικά δεδομένα.

➢ **Τύποι:**

- **Κανένα αποτέλεσμα:** Τα δεδομένα φαίνονται από άτομα που δε χρειάζεται να τα γνωρίζουν, αν και δεν τα χρησιμοποιούν.
- **Αποθήκευση:** Τα δεδομένα αντιγράφονται και αποθηκεύονται σε άλλη τοποθεσία, χωρίς περαιτέρω χρήση.
- **Ανακατανομή:** Τα δεδομένα διαδίδονται περισσότερο από ό,τι είναι απαραίτητο και πέρα από τον έλεγχο των υποκειμένων των δεδομένων (π.χ. ανεπιθύμητη διάδοση στοιχείων στο διαδίκτυο, απώλεια ελέγχου των πληροφοριών που δημοσιεύονται σε ένα κοινωνικό δίκτυο κ.λ.π.).
- **Χρήση:** Τα δεδομένα χρησιμοποιούνται για σκοπούς διάφορους από εκείνους που σχεδιάζονται ή με άδικο τρόπο (π.χ. κλοπές ταυτότητας, χρήση κατά των δεδομένων κ.λ.π.) ή σε σχέση με άλλες πληροφορίες που αφορούν τα πρόσωπα στα οποία αναφέρονται τα δεδομένα (π.χ. δεδομένα γεωγραφικού εντοπισμού σε πραγματικό χρόνο κ.λ.π.).

✓ Ανεπιθύμητη τροποποίηση των προσωπικών δεδομένων

➢ **Τύποι:**

- **Δυσλειτουργία:** Τα δεδομένα τροποποιούνται σε έγκυρα ή μη, τα οποία δε θα χρησιμοποιηθούν σωστά, η επεξεργασία ενδέχεται να προκαλέσει

σφάλματα, δυσλειτουργίες ή να μην παρέχει πλέον την αναμενόμενη υπηρεσία (π.χ. να βλάψει την κατάλληλη πρόοδο σημαντικών βημάτων).

- **Χρήση:** Τα δεδομένα τροποποιούνται σε άλλα έγκυρα, με αποτέλεσμα να καταστραφούν οι πράξεις επεξεργασίας ή θα μπορούσαν να χρησιμοποιηθούν (π.χ. για να κλέψουν ταυτότητες, αλλάζοντας τη σχέση μεταξύ της ταυτότητας των ατόμων και των βιομετρικών δεδομένων άλλων ατόμων).

✓ Εξαφάνιση των προσωπικών δεδομένων

➢ **Τύποι:**

- **Δυσλειτουργία:** Τα δεδομένα λείπουν για επεξεργασίες, τα οποία δημιουργούν σφάλματα, δυσλειτουργίες ή παρέχουν διαφορετική υπηρεσία από αυτήν που αναμένεται (π.χ. ορισμένες αλλεργίες δεν αναφέρονται πλέον σε ιατρικό μητρώο, ορισμένες πληροφορίες που περιέχονται στις φορολογικές δηλώσεις έχουν εξαφανιστεί, γεγονός που εμποδίζει τον υπολογισμό του ποσού του φόρου κ.λ.π.).
- **Εμπλοκή:** Τα δεδομένα λείπουν.

1.1.5 Κλίμακα και κανόνες για την εκτίμηση της σοβαρότητας

Η σοβαρότητα αντιπροσωπεύει το μέγεθος ενός κινδύνου. Εκτιμάται, κατ' αρχάς, όσο αφορά την έκταση των δυνητικών επιπτώσεων στα πρόσωπα στα οποία αναφέρονται τα δεδομένα, λαμβάνοντας υπόψη υπάρχοντες, προγραμματισμένους ή συμπληρωματικούς ελέγχους. Ο παρακάτω πίνακας, παρουσιάζει τη κλίμακα που μπορεί να χρησιμοποιηθεί, για την εκτίμηση της σοβαρότητας .

Πίνακας 3-3: Κλίμακα εκτίμησης σοβαρότητας
Πηγή: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

ΕΠΙΠΕΔΑ	Γενική περιγραφή των επιπτώσεων (άμεση και έμμεση)	Παραδείγματα φυσικών επιπτώσεων (3)	Παραδείγματα υλικών επιπτώσεων (4)	Παραδείγματα ηθικών επιπτώσεων (5)
1. Αμελητέο	Τα υποκείμενα δεδομένων είτε δεν θα επηρεαστούν είτε ενδέχεται να αντιμετωπίσουν μερικές δυσκολίες, τις οποίες θα ξεπεράσουν χωρίς κανένα πρόβλημα	Έλλειψη επαρκούς μέριμνας για ένα εξαρτώμενο άτομο (ανήλικος, πρόσωπο υπό κηδεμονία)	1. Απώλεια χρόνου κατά την επανάληψη των διατυπώσεων ή την αναμονή της εκπλήρωσης 2. Παραλαβή ανεπιθύμητης αλληλογραφίας (π.χ. spam) 3.Επαναχρησιμοποίηση δεδομένων που δημοσιεύονται σε ιστότοπους για σκοπούς στοχοθετημένης διαφήμισης (πληροφορίες σε κοινωνικά δίκτυα, επαναχρησιμοποίηση για αλληλογραφία σε χαρτί) 4.Στοχοθετημένη διαφήμιση για κοινά καταναλωτικά προϊόντα	1.Απλή ενόχληση που προκαλείται από τις πληροφορίες που ελήφθησαν ή ζητήθηκαν 2.Φόβος να χάσει τον έλεγχο των δεδομένων κάποιου 3.Αίσθημα εισβολής στην ιδιωτική ζωή χωρίς πραγματική ή αντικειμενική βλάβη (π.χ. εμπορική εισβολή) 4.Απώλεια χρόνου κατά τη διαμόρφωση των δεδομένων κάποιου έλλειψη σεβασμού για την ελευθερία της διαδικτυακής κίνησης λόγω της άρνησης πρόσβασης σε εμπορική περιοχή
2. Περιορισμένο	Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές δυσκολίες, τις οποίες θα μπορέσουν να ξεπεράσουν παρά ορισμένες δυσκολίες	1.Μικρά σωματικά νοσήματα (π.χ., ασήμαντη ασθένεια λόγω παραβίασης των αντενδείξεων) 2.Έλλειψη φροντίδας που οδηγεί σε δευτερεύουσα αλλά πραγματική βλάβη (π.χ. αναπηρία) 3.Η δυσφήμιση που έχει ως αποτέλεσμα φυσικές ή ψυχολογικές ανιπτοίνων	1.Απρόβλεπτες πληρωμές (π.χ. πρόστιμα που έχουν επιβληθεί εσφαλμένα), πρόσθετα έξοδα (π.χ. τραπεζικά έξοδα, νομικά έξοδα), αδυναμίες πληρωμής 2.Άρνηση πρόσβασης σε διοικητικές υπηρεσίες ή εμπορικές υπηρεσίες 3.απώλεια ευκαιριών άνεσης (δηλαδή ακύρωση αναψυχής, αγορές, διακοπές, τερματισμός ενός λογαριασμού στο διαδίκτυο) 4.Έλλειψη προαγωγής σταδιοδρομίας 5.Αποκλεισμός λογαριασμού ηλεκτρονικών υπηρεσιών (π.χ. παιχνίδια, διαχείριση) 6.Παραλαβή ανεπιθύμητων στοχευμένων αποστολών που ενδέχεται να βλάψουν τη φήμη των υποκειμένων των δεδομένων 7.Αύξηση του κόστους (π.χ. αυξημένες ασφαλιστικές τιμές) 8.Μη ενημερωμένα δεδομένα (π.χ. θέση που κρατήθηκε προηγουμένως) 9.Επεξεργασία εσφαλμένων δεδομένων που δημιουργούν για παράδειγμα δυσλειτουργίες λογαριασμών (τράπεζα, πελάτες, με κοινωνικές οργανώσεις κ.λπ.) 10.Στοχοθετημένη διαδικτυακή	1.Άρνηση συνέχισης της χρήσης συστημάτων πληροφοριών (whistleblowing, κοινωνικά δίκτυα) 2.Μικρές αλλά αντικειμενικές ψυχολογικές ασθένειες (δυσφήμιση, φήμη) 3.Προβλήματα σχέσεων με προσωπικούς ή επαγγελματικούς γνωστούς (π.χ. εικόνα, αμαυρωμένη φήμη, απώλεια αναγνώρισης) 4.Αίσθημα εισβολής στην ιδιωτική ζωή χωρίς ανεπανόρθωτη ζημιά 5.Εκφοβισμός στα κοινωνικά δίκτυα

3. Σημαντικό	Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές συνέπειες, τις οποίες θα πρέπει να μπορέσουν να ξεπεράσουν, αν και με πραγματικές και σοβαρές δυσκολίες	1.Σοβαρές σωματικές ασθένειες που προκαλούν μακροχρόνια βλάβη 2.Μεταβολή της σωματικής ακεραιότητας	1.Παραποίηση χρημάτων χωρίς αποζημίωση 2.Μη προσωρινές οικονομικές δυσκολίες 3.Στοχοθετημένες, μοναδικές και μη επαναλαμβανόμενες, χαμένες ευκαιρίες 4.Απαγόρευση της κατοχής τραπεζικών λογαριασμών 5.Ζημία ιδιοκτησίας 6.Απώλεια στέγης 7.Απώλεια της απασχόλησης 8.Διαχωρισμός ή διαζύγιο 9.Οικονομική ζημία ως αποτέλεσμα απάτης 10.Αποκλεισμένοι στο εξωτερικό 11.Απώλεια δεδομένων πελατών	1.Σοβαρές ψυχολογικές ασθένειες 2.Αίσθημα εισβολής στην ιδιωτική ζωή με μη αναστρέψιμες ζημιές 3.Αίσθημα τρωτότητας μετά από κλήτευση στο δικαστήριο 4.Αίσθημα παραβίασης των θεμελιωδών δικαιωμάτων 5.Θύμα εκβιασμού 6.Ηλεκτρονική παρενόχληση/cyberbullying
4. Μέγιστο	Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές ή ακόμη και μη αναστρέψιμες συνέπειες, τις οποίες δεν μπορούν να υπερνικήσουν	1.Μακροχρόνιες ή μόνιμες σωματικές παθήσεις 2.Θάνατος 3.Μόνιμη εξασθένιση της φυσικής ακεραιότητας	1.Οικονομικός κίνδυνος 2.Σημαντικά χρέη 3.Αδυναμία εργασίας 4.Αδυναμία μετεγκατάστασης 5.Απώλεια αποδεικτικών στοιχείων στο πλαίσιο διαφορών 6.Απώλεια πρόσβασης σε ζωτικής σημασίας υποδομές	1.Μακροχρόνιες ή μόνιμες ψυχολογικές ασθένειες 2.Ποινική κύρωση 3.Απαγωγή 4.Απώλεια οικογενειακών δεσμών 5.Αδυναμία να ασκήσει αγωγή 6.Αλλαγή διοικητικού καθεστώτος ή και απώλεια νομικής αυτονομίας

(3) Απώλεια ευπρέπειας, αλλοίωση ή οικονομική απώλεια που σχετίζεται με τη σωματική ακεραιότητα.
(4) Απώλεια σε σχέση με τα περιουσιακά στοιχεία ενός ατόμου.
(5) Φυσική ή συναισθηματική ταλαιπωρία, αλλοίωση ή απώλεια ευπρέπειας.

Η τιμή του επιπέδου που ταιριάζει καλύτερα με τις πιθανές επιπτώσεις που προσδιορίζονται επιλέγεται έπειτα, μετά από σύγκριση με τις επιπτώσεις που προσδιορίζονται στο εξεταζόμενο πλαίσιο με τις γενικές επιπτώσεις στην κλίμακα.

Το επίπεδο σοβαρότητας που λαμβάνεται με τον τρόπο αυτό, μπορεί να αυξηθεί ή να μειωθεί με τη συμπερίληψη πρόσθετων παραγόντων όπως:

- το επίπεδο ταυτοποίησης των προσωπικών δεδομένων
- τη φύση των πηγών κινδύνου
- τον αριθμό διασυνδέσεων (ειδικά με ξένους δικτυακούς τόπους).
- τον αριθμό των αποδεκτών (που διευκολύνει τη συσχέτιση μεταξύ αρχικά διαχωρισμένων προσωπικών δεδομένων).

1.1.6 Κλίμακα και κανόνες για την εκτίμηση της πιθανότητας

Η πιθανότητα αντιπροσωπεύει τη σκοπιμότητα ενός κινδύνου να συμβεί. Εκτιμάται, κατ' αρχάς, όσο αφορά το επίπεδο των τρωτών σημείων των σχετικών

περιουσιακών στοιχείων και το επίπεδο των ικανοτήτων των πηγών κινδύνου για την εκμετάλλευσή τους, λαμβανομένων υπόψη των υφιστάμενων, προγραμματισμένων ή συμπληρωματικών ελέγχων (που πρέπει να αναφέρονται ως δικαιολογητικά).

Αξιοποιώντας τις ιδιότητες των υποστηρικτικών περιουσιακών στοιχείων, μπορεί να χρησιμοποιηθεί η ακόλουθη κλίμακα για να εκτιμηθεί η πιθανότητα εμφάνισης απειλών:

1. **Αμελητέο:** δε φαίνονται οι επιλεγμένες πηγές κινδύνου να υλοποιούν την απειλή.
2. **Περιορισμένο:** φαίνεται δύσκολο να υλοποιηθεί η απειλή.
3. **Σημαντικό:** φαίνεται ότι μπορεί να υλοποιηθεί η απειλή.
4. **Μέγιστο:** φαίνεται εξαιρετικά εύκολο να υλοποιηθεί η απειλή.

Μ' αυτό τον τρόπο, προσδιορίζεται η αξία του επιπέδου που ταιριάζει καλύτερα με τις ευπάθειες των υποστηρικτικών περιουσιακών στοιχείων και των πηγών κινδύνου, με το επίπεδο πιθανότητας που προκύπτει, να διαφοροποιείται με τη συμπερίληψη πρόσθετων παραγόντων όπως:

- άνοιγμα στο Διαδίκτυο ή σε κλειστό σύστημα.
- ανταλλαγές δεδομένων με ξένες χώρες ή όχι.
- διασυνδέσεις με άλλα συστήματα ή χωρίς διασύνδεση.
- ετερογένεια ή ομοιογένεια του συστήματος.
- μεταβλητότητα ή σταθερότητα του συστήματος.
- την εικόνα της οργάνωσης.

1.1.7 Κλίμακα σχεδίου δράσης

Οι κλίμακες που ακολουθούν μπορούν να χρησιμοποιηθούν για την ανάπτυξη του σχεδίου δράσης και την παρακολούθηση της εφαρμογής του:

Πίνακας 3-4: Κλίμακα σχεδίου δράσης
Πηγή:https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

Κριτήρια	Επίπεδο 1	Επίπεδο 2	Επίπεδο 3
Δυσκολία	Χαμηλό	Μέτριο	Υψηλό
Οικονομικό κόστος	Μηδέν	Μέτριο	Υψηλό
Χρονική Περίοδος	Εξάμηνο	Έτος	3 χρόνια
Πρόοδος	Δεν ξεκίνησε	Σε εξέλιξη	Ολοκληρώθηκε

1.2 Ανωνυμία

Στόχος η κατάργηση των χαρακτηριστικών αναγνώρισης από τα προσωπικά δεδομένα και η εφαρμογή καλών πρακτικών που πρέπει να ακολουθούνται, εάν το μέτρο χρησιμοποιείται για την αντιμετώπιση των κινδύνων. Συγκεκριμένα:

• καθορισμός του τί πρέπει να ανωνυμοποιηθεί με βάση το πλαίσιο, τη μορφή στην οποία αποθηκεύονται τα προσωπικά δεδομένα (συμπεριλαμβανομένων των πεδίων βάσεων δεδομένων ή των αποσπασμάτων κειμένων) και τους προσδιορισμένους κινδύνους.

• ανωνυμοποίηση των μόνιμων δεδομένων με βάση τη μορφή τους (συμπεριλαμβανομένων των βάσεων δεδομένων και των κειμένων) και των κινδύνων που εντοπίστηκαν.

• επιλογή κατάλληλων εργαλείων προστασίας (συμπεριλαμβανομένης της μερικής διαγραφής, κρυπτογράφησης, κατακερματισμού και κλειδώματος των δεδομένων), αν αυτά δεν μπορούν να ανωνυμοποιηθούν μόνιμα.

1.3 Αρχειοθέτηση

Στόχος ο καθορισμός όλων των διαδικασιών διατήρησης και διαχείρισης των ηλεκτρονικών αρχείων που περιέχουν τα προσωπικά δεδομένα που αποσκοπούν στην εξασφάλιση της αξίας τους (συγκεκριμένα, της νομικής τους αξίας), καθ' όλη τη διάρκεια της απαραίτητης περιόδου που περιλαμβάνει τη μεταφορά, την αποθήκευση, την πρόσβαση, την εξάλειψη, την πολιτική αρχειοθέτησης και την εμπιστευτικότητα.

Σημαντικές πρακτικές που πρέπει να υιοθετούνται:

1) Επιβεβαίωση ότι έχουν οριστεί οι διαδικασίες διαχείρισης αρχείων όπως ο διαχωρισμός της μεταφοράς, της αποθήκευσης, της διαχείρισης περιγραφικών δεδομένων, των διαδικασιών διαβούλευσης - επικοινωνίας και της διοίκησης, σε σχέση με τα γραφεία προέλευσης, την τεχνολογική και νομική παρακολούθηση αλλά και την αναβάθμιση μέσων και μορφών.

2) Επιβεβαίωση ότι έχουν αναγνωριστεί οι ρόλοι αρχειοθέτησης, όπως ο διαχωρισμός των πηγών προέλευσης (γραφεία), οι μεταβιβάσιμες υπηρεσίες, οι αρχές αρχειοθέτησης (υπεύθυνες για τη συντήρηση) και οι οργανισμοί επιθεώρησης (ασκώντας τον επιστημονικό και τεχνικό έλεγχο των δημόσιων αρχείων).

3) Επιβεβαίωση ότι τα μέτρα μπορούν να εξασφαλίσουν, εάν είναι αναγκαίο, τον προσδιορισμό και την εξακρίβωση της προέλευσης των αρχείων, την ακεραιότητα, τη

σαφήνεια, την αναγνωσιμότητα, τη διαθεσιμότητα και την προσβασιμότητα των αρχείων, πόσο χρόνο πρέπει να διατηρούνται τα αρχεία και την ιχνηλασιμότητα των εργασιών σχετικά με τα αρχεία (συμπεριλαμβανομένης της μεταφοράς, της διαβούλευσης, της μετανάστευσης, της διαγραφής κ.λ.π.) και να λάβουν πρόσθετα μέτρα, εάν αυτό δεν συμβαίνει. Ειδικότερα, η εφαρμογή ειδικών μεθόδων πρόσβασης για τα αρχειοθετημένα δεδομένα, η κρυπτογράφηση των αρχείων και η προετοιμασία για την, εκ νέου, κρυπτογράφηση των αρχείων, με νέα κλειδιά πριν από την λήξη των προηγούμενων κλειδιών κρυπτογράφησης, η αλλαγή παρωχημένων δεδομένων που υποστηρίζουν τα στοιχεία ενεργητικού και η επιλογή μιας διαδικασίας ικανής να διασφαλίσει την καταστροφή ολόκληρου του αρχείου.

4) Προσδιορισμός των μεθόδων προστασίας της εμπιστευτικότητας των αρχειοθετημένων προσωπικών δεδομένων, βάσει των εντοπισθέντων κινδύνων. Συστηματική κρυπτογράφηση των ευαίσθητων δεδομένων.

5) Επιβεβαίωση ότι οι αρχές αρχειοθέτησης διαθέτουν πολιτική αρχειοθέτησης και, ειδικότερα, εάν το έγγραφο τεκμηριώνει επισήμως τους νομικούς, λειτουργικούς και τεχνικούς περιορισμούς που πρέπει να τηρούν οι διάφοροι ενδιαφερόμενοι ώστε η ηλεκτρονική αρχειοθέτησή του να μπορεί να θεωρηθεί αξιόπιστη και μόνιμη.

6) Επιβεβαίωση ύπαρξης δήλωσης πρακτικών αρχειοθέτησης, εάν δηλαδή το έγγραφο περιγράφει όλες τις διαδικασίες που έχουν τεθεί για την επίτευξη των στόχων που τίθενται στην πολιτική αρχειοθέτησης.

1.4 Κρυπτογράφηση

1.4.1 Γενικά μέτρα

Στόχος να καταστούν τα προσωπικά δεδομένα ακατανόητα σε οποιονδήποτε χωρίς άδεια πρόσβασης, με τη χρήση συμμετρικής ή ασύμμετρης κρυπτογράφησης, χρήση ισχυρών δημόσιων αλγορίθμων και πιστοποιητικών ελέγχου ταυτότητας.

Πρακτικές που πρέπει να ακολουθούνται:

• προσδιορισμός του τί πρέπει να κρυπτογραφηθεί, συμπεριλαμβανομένου ενός ολόκληρου σκληρού δίσκου, partition του δίσκου, μιας βάσης δεδομένων ή ενός καναλιού επικοινωνίας, με βάση τη μορφή στην οποία αποθηκεύονται τα δεδομένα, τους κινδύνους που εντοπίστηκαν.

• επιλογή του τύπου κρυπτογράφησης (συμμετρική ή ασύμμετρη) με βάση το πλαίσιο και τους κινδύνους που εντοπίστηκαν.

• υιοθέτηση λύσεων κρυπτογράφησης με βάση ισχυρούς δημόσιους αλγόριθμους. Συγκεκριμένα χρήση πιστοποιημένων κρυπτογραφικών εργαλείων συμπεριλαμβανομένων των συστημάτων προστασίας ιδιωτικών κλειδιών, μονάδων κρυπτογράφησης ή μονάδων αποκρυπτογράφησης.

• καθιέρωση μέτρων για τη διασφάλιση της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας των πληροφοριών.

1.4.2 Συμμετρική κρυπτογράφηση

Για την επιτυχή εκτέλεση αυτής, απαιτείται:

• η χρήση ενός μόνο κλειδιού για ένα μόνο σκοπό.

• η επιλογή κατάλληλων αλγόριθμων κρυπτογράφησης, όπως ο αλγόριθμος AES, ο οποίος χρησιμοποιεί ένα επεξεργασμένο μέγεθος μπλοκ ίσο με τουλάχιστον 128 bits.

• η τεκμηρίωση του συστήματος διαχείρισης κλειδιών, παράλληλα με το σχεδιασμό μιας κρυπτογραφικής διαδικασίας.

1.4.3 Ασύμμετρη (δημόσιο κλειδί) κρυπτογράφηση

Σε ακολουθία των ανωτέρω και στο μέτρο που ο επιδιωκόμενος σκοπός είναι η αντιμετώπιση των κινδύνων, προβλέπεται:

• η χρήση ενός μόνο κλειδιού για ένα μόνο σκοπό.

• η επιλογή κατάλληλων αλγόριθμων κρυπτογράφησης όπως ο αλγόριθμος RSAES-OAEP (Optimal Asymmetric Encryption Padding), σε συνδυασμό με τον αλγόριθμο RSA.

• η καθιέρωση μηχανισμών για την επαλήθευση των ηλεκτρονικών πιστοποιητικών. Συγκεκριμένα, κατά τη λήψη ενός ηλεκτρονικού πιστοποιητικού, να επιβεβαιώνεται η εγκυρότητά του, ότι δεν έχει ανακληθεί αλλά και ότι διατηρεί μια κατάλληλη αλυσίδα πιστοποίησης σε όλα τα επίπεδα.

• η προστασία της ασφαλούς δημιουργίας κλειδιών και της χρήση τους, όταν αυτά αποθηκεύονται από τους χρήστες, συμπεριλαμβανομένων περιοριστικών κανόνων που διέπουν τα δικαιώματα πρόσβασης, τον κωδικό πρόσβασης καθώς και η εφαρμογή ενισχυμένων μέτρων ασφαλείας.

• η επίσημη τεκμηρίωση του συστήματος διαχείρισης κλειδιών, με σκοπό την ανάπτυξη μιας πολιτικής πιστοποίησης, η οποία θα καθορίζει τις ευθύνες, την αναγνώριση και την πιστοποίηση ταυτότητας, τις λειτουργικές απαιτήσεις του κύκλου

ζωής του πιστοποιητικού, τα τεχνικά και μη μέτρα ασφάλειας, τις διαδικασίες ανάκλησης, τους ελέγχους συμμόρφωσης και άλλες αξιολογήσεις.

1.4.4 Κρυπτογράφηση του εξοπλισμού

Στόχος είναι να καταστούν τα προσωπικά δεδομένα ακατανόητα σε οποιονδήποτε χωρίς εξουσιοδότηση πρόσβασης, προκειμένου να μειωθούν οι κίνδυνοι που σχετίζονται με την ανάκτηση ενός τμήματος του εξοπλισμού (ένας σταθμός εργασίας, ένας server ή αφαιρούμενα μέσα).

Χρήσιμες πρακτικές:

• κρυπτογράφηση δεδομένων σε επίπεδο υλικού όπως η επιφάνεια του σκληρού δίσκου ή σε επίπεδο λειτουργικού συστήματος όπως η κρυπτογράφηση κάποιου partition ή container, με χρήση λογισμικών όπως τα dm-crypt για Linux, VeraCrypt για Windows, FileVault για MacOS.

• επιλογή προηγμένων συστημάτων που δε θα αποθηκεύουν κλειδιά του εξοπλισμού που πρόκειται να κρυπτογραφηθεί, εκτός και αν αυτά υλοποιούν ασφαλείς συσκευές αποθήκευσης όπως τα TPM (Trusted Platform Module) chips στα laptops, δηλαδή ειδικούς μικροελεγκτές που έχουν σχεδιαστεί, για να ασφαλίζουν το υλικό μέσω ολοκληρωμένων κρυπτογραφικών κλειδιών.

1.4.5 Κρυπτογράφηση των βάσεων δεδομένων

Σχετίζεται με την ελαχιστοποίηση των κινδύνων που συνδέονται με την κλοπή του server, την ανεπιθύμητη φυσική πρόσβαση σε έναν σταθμό εργασίας ή τον server και την άμεση πρόσβαση στα δεδομένα της βάσης από τον διαχειριστή.

Ο ανωτέρω σκοπός επιτυγχάνεται ως εξής:

• κρυπτογράφηση της περιοχής αποθήκευσης σε επίπεδα υλικού, λειτουργικού συστήματος ή βάσης δεδομένων, με βάση τους κινδύνους που εντοπίστηκαν, έτσι ώστε να παρέχεται προστασία από φυσική κλοπή μέρους των δεδομένων. Ως απώτερο αποτέλεσμα, θεωρείται η διατήρηση της εγγύησης της εμπιστευτικότητας των δεδομένων, εκ μέρους των διαχειριστών και η πρόσβαση σε αυτά μόνο από τους διαχειριστές των βάσεων δεδομένων.

1.4.6 Κρυπτογράφηση partitions ή containers

Μέσω αυτής, επιδιώκεται ο περιορισμός των κινδύνων που αναφέρονται στην ανάκτηση ενός εξοπλισμού, συμπεριλαμβανομένου ενός σταθμού εργασίας, server ή αφαιρούμενων μέσων, την ανεπιθύμητη πρόσβαση σε έναν σταθμό εργασίας ή server και την άμεση πρόσβαση στα δεδομένα του server από έναν διαχειριστή.

Πώς μπορεί να λειτουργήσει αυτή; Ως κατωτέρω:

• κρυπτογράφηση των δεδομένων σε επίπεδο λειτουργικού συστήματος, ενός partition, καταλόγου ή αρχείου, με τη χρήση εξειδικευμένου λογισμικού κρυπτογράφησης container όπως το VeraCrypt και το Zed!.

1.4.7 Κρυπτογράφηση αυτόνομων αρχείων

Γίνεται χρήση αυτής, προκειμένου να αντιμετωπιστούν οι κίνδυνοι που συνδέονται με την κλοπή ενός σταθμού εργασίας ή server, την ανεπιθύμητη πρόσβαση σε ένα σταθμό εργασίας ή server και την άμεση πρόσβαση στα δεδομένα από έναν διαχειριστή.

Για την υλοποίηση αυτής, απαιτείται:

• κρυπτογράφηση αποθηκευμένων αρχείων ή των συνημμένων του ηλεκτρονικού ταχυδρομείου με τη χρήση λογισμικών όπως το ZoneCentral, το AxCrypt ή το Gnu Privacy Guard (GPG) αλλά και τη χρήση ενός εργαλείου συμπίεσης που επιτρέπει κρυπτογράφηση με κωδικό πρόσβασης, όπως το 7-Zip, το οποίο παρέχει κρυπτογράφηση AES.

1.4.8 Κρυπτογράφηση ηλεκτρονικού ταχυδρομείου

Η διασφάλιση των δεδομένων του ηλεκτρονικού ταχυδρομείου επιτυγχάνεται με τη χρήση λογισμικού όπως το Gnu Privacy Guard (GPG).

1.4.9 Κρυπτογράφηση ενός καναλιού επικοινωνίας

Η απροσπέλαστη ροή των δεδομένων, διασφαλίζεται ως εξής:

• κρυπτογράφηση του καναλιού επικοινωνίας μεταξύ ενός πιστοποιημένου διακομιστή και ενός απομακρυσμένου υπολογιστή - πελάτη, με τη χρήση ενός πιστοποιητικού ελέγχου ταυτότητας υπηρεσίας που συμμορφώνεται με τις πιο πρόσφατες εκδόσεις του πρωτοκόλλου TLS (πρώην SSL), ώστε κάθε φορά να απαιτείται ένας κωδικός πρόσβασης για να χρησιμοποιείται το ιδιωτικό κλειδί αλλά και να

προστατεύεται η πρόσβαση στο κανάλι, μέσω περιορισμένων δικαιωμάτων πρόσβασης ή μέσω της εγκατάστασης κρυπτογραφημένου VPN ή IP (VPN-IPSec) δικτύου.

1.5 Κατανομή δεδομένων (σε σχέση με το υπόλοιπο σύστημα πληροφοριών)

Στόχος είναι να μειωθεί η πιθανότητα συσχέτισης των προσωπικών δεδομένων και μιας γενικής παραβίασης δεδομένων, προσδιορίζοντας τις ομάδες δεδομένων που αφορούν κάθε επιχείρηση και διαχωρίζοντάς τες με λογικό τρόπο.

Προς επίτευξη αυτού, είναι χρήσιμο να ακολουθούνται οι εξής πρακτικές:

• προσδιορισμός των μοναδικών δεδομένων που είναι απαραίτητα για κάθε φορέα και η πρόσβαση των υπαλλήλων μόνο σε αυτά που πραγματικά χρειάζονται.

• διαχωρισμός των δεδομένων που είναι χρήσιμα σε κάθε διαδικασία με λογικό τρόπο και η διαχείρισή τους από τους υπαλλήλους ανάλογα με το τμήμα που ανήκουν (ανάθεση ρόλων χρήστη).

• επιβεβαίωση, σε τακτά χρονικά διαστήματα, ότι τα προσωπικά δεδομένα διαχωρίζονται αποτελεσματικά χωρίς την προσθήκη παραληπτών και διασυνδέσεων.

1.6 Φυσικός έλεγχος πρόσβασης

Αποσκοπεί στον περιορισμό της φυσικής πρόσβασης μη εξουσιοδοτημένων προσώπων σε προσωπικά δεδομένα, μέσω της:

• κατηγοριοποίησης των χώρων των κτιρίων ανάλογα με το πόσο ευάλωτοι είναι, με σκοπό την οριοθέτηση περιοχών προσιτών στο κοινό.

• επιλογής μεθόδων πιστοποίησης των υπαλλήλων.

• καθιέρωσης ελέγχου ταυτότητας επισκεπτών.

• ορισμού ενεργειών που πρέπει να ακολουθούνται σε περίπτωση που αποτύχει ο έλεγχος ταυτότητας (η ταυτότητα δεν μπορεί να επιβεβαιωθεί ή έλλειψη εξουσιοδότησης για την είσοδο σε μια περιοχή ασφαλείας), κάτι που συνεπάγεται την άρνηση εισόδου στον επισκέπτη και την ειδοποίηση του υπεύθυνου ασφαλείας.

• τήρησης αρχείου πρόσβασης με καταγραφή της ταυτότητας των επισκεπτών, ημερομηνία και ώρα άφιξης και αναχώρησης.

• εγκατάστασης συστήματος προειδοποίησης, σε ιδιαίτερα ευαίσθητες περιοχές, όπου διατηρούνται ή επεξεργάζονται δεδομένα (computer room, αρχείο).

1.7 Παρακολούθηση ακεραιότητας

1.7.1 Γενικά μέτρα

Στόχος είναι η προειδοποίηση σε περίπτωση ανεπιθύμητης τροποποίησης ή εξαφάνισης προσωπικών δεδομένων. Προς τούτο, μπορεί να χρησιμοποιηθούν οι εξής πρακτικές:

• προσδιορισμός των δεδομένων που χρήζουν παρακολούθηση για τη διαφύλαξη της ακεραιότητας τους.

• επιλογή μεθόδων κρυπτογράφησης (hash functions, επαλήθευση MAC), με βάση το πλαίσιο που ακολουθείται και τους εκτιθέμενους κινδύνους.

• προσδιορισμός του πότε πρέπει να εφαρμοστεί η μέθοδος και πότε πρέπει να γίνει η παρακολούθηση βάσει του εσωτερικού κανονισμού λειτουργίας του φορέα.

• δημιουργία μέτρων για την αποφυγή επιθέσεων scripting ή SQL injection, σε περίπτωση που τα δεδομένα αποστέλλονται σε μια βάση δεδομένων, τα οποία θα περιλαμβάνουν τρόπους αποτροπής εισαγωγής οποιωνδήποτε δεδομένων, όπως το φιλτράρισμα ή η κρυπτογράφηση των δεδομένων πριν αποθηκευτούν και τον περιορισμό του όγκου των δεδομένων που μπορούν να εισαχθούν.

1.7.2 Ηλεκτρονική υπογραφή

Η ορθή χρήση αυτής, εξασφαλίζεται μέσω της:

• χρησιμοποίησης ενός μόνο κλειδιού για ένα μόνο σκοπό.

• υιοθέτησης λύσεων υπογραφής βασισμένων σε ισχυρούς δημόσιους αλγόριθμους, με χρήση εργαλείων όπως πιστοποιημένες συσκευές δημιουργίας υπογραφής και επαλήθευσης υπογραφών.

• καθιέρωσης μηχανισμών για την επαλήθευση των ηλεκτρονικών πιστοποιητικών. Ειδικότερα, κατά τη λήψη ηλεκτρονικού πιστοποιητικού, να επαληθεύεται, τουλάχιστον, ότι είναι έγκυρο, δεν έχει ανακληθεί και ότι διαθέτει την κατάλληλη πιστοποίηση.

• προστασίας της δημιουργίας κλειδιών και της χρήση τους σύμφωνα με το επίπεδό τους στην ιεραρχία κλειδιών.

• τεκμηρίωσης του συστήματος διαχείρισης κλειδιών, με ανάπτυξη μιας "πολιτικής πιστοποίησης" που καθορίζει τις αρμοδιότητες, τον προσδιορισμό ταυτότητας και την πιστοποίηση ταυτότητας, τις λειτουργικές απαιτήσεις του κύκλου ζωής του πιστοποιητικού, τα τεχνικά και μη μέτρα ασφάλειας.

1.8 Έλεγχος πρόσβασης

Στόχος είναι να περιοριστούν οι κίνδυνοι από την ηλεκτρονική πρόσβαση μη εξουσιοδοτημένων ατόμων σε προσωπικά δεδομένα όπως διαχείριση προφίλ χρηστών, μηχανισμός ελέγχου ταυτότητας και πολιτικές κωδικών πρόσβασης.

1.8.1 Διαχείριση δικαιωμάτων προφίλ χρηστών για πρόσβαση σε προσωπικά δεδομένα

Για τη διασφάλιση του προφίλ των χρηστών, είναι δυνατό να προταθούν οι εξής τρόποι:

• διαχωρισμός των καθηκόντων και των τομέων ευθύνης, ώστε να περιορίζεται η πρόσβαση σε προσωπικά δεδομένα, αποκλειστικά και μόνο σε εξουσιοδοτημένους χρήστες.

• παροχή σε κάθε χρήστη νόμιμης πρόσβασης με τη χρήση ενός μοναδικού αναγνωριστικού, με ταυτόχρονη καταγραφή των δραστηριοτήτων του.

• περιορισμός πρόσβασης σε εργαλεία και διεπαφές διαχείρισης, μόνο σε εξουσιοδοτημένα άτομα.

• περιορισμός χρήσης λογαριασμών που παρέχουν αυξημένα προνόμια, σε λειτουργίες που τις απαιτούν.

• περιορισμός χρήσης λογαριασμών με δικαιώματα "διαχειριστή" και μόνο με προσωπικό κωδικό πρόσβασης.

• διεξαγωγή ετήσιας αναθεώρησης των προνομίων με σκοπό τον εντοπισμό και τη διαγραφή των αχρησιμοποίητων λογαριασμών και την αναπροσαρμογή των δικαιωμάτων με τις λειτουργίες κάθε χρήστη.

• απόσυρση των δικαιωμάτων των εργαζομένων - χρηστών, όταν αποχωρήσουν από την εργασία (λύση υπαλληλικής σχέσης) και η δημιουργία
προσωρινών λογαριασμών με καθορισμένη ημερομηνία λήξης για εργαζόμενους - χρήστες με σχέση εργασίας ορισμένου χρόνου ή για όσους τελούν σε καθεστώς πρακτικής άσκησης.

1.8.2 Πιστοποίηση ατόμων

Ως εχέγγυο της προστασίας των προσωπικών δεδομένων, αποτελεί την αναγκαία συνθήκη, η οποία πληρώνεται ως εξής:

• επιλογή μεθόδου ελέγχου ταυτότητας, κατά τις περιόδους σύνδεσης, είτε με χρήση ενός κωδικού πρόσβασης εάν οι κίνδυνοι δεν είναι αυξημένοι, είτε με χρήση κωδικού μίας χρήσης, εάν είναι υψηλότεροι.

• απαγόρευση κωδικών πρόσβασης που χρησιμοποιούνται από την εμφάνιση μη κρυπτογραφημένων προγραμμάτων και αρχείων, κατά την εισαγωγή τους.

• προσδιορισμός ενεργειών που πρέπει να γίνουν σε περίπτωση αποτυχημένου ελέγχου ταυτότητας, όπως αποκλεισμός του λογαριασμού μετά από τρείς αποτυχίες σύνδεσης ή αύξηση του χρόνου αναμονής μεταξύ δύο προσπαθειών σύνδεσης και ταυτόχρονη καταγραφή στα log files των προσπαθειών σύνδεσης.

• πρόβλεψη για διαδικασία δεύτερης επαλήθευσης ταυτότητας για απόκτηση πρόσβασης σε εφαρμογές που περιέχουν προσωπικά δεδομένα και βρίσκονται σε περιβάλλοντα με ανεπαρκή ασφάλεια, όπως κοινόχρηστοι σταθμοί εργασίας.

1.8.3 Διαχείριση των διαπιστευτηρίων

Η εξασφάλιση της λειτουργίας τους, διέπεται από τις εξής παραμέτρους:

• υιοθέτηση πολιτικής κωδικών πρόσβασης, όπως το ότι πρέπει να αποτελούνται από οκτώ τουλάχιστον χαρακτήρες, να ανανεώνονται είτε περιοδικά (κάθε έξι μήνες ή μία φορά το χρόνο) είτε εάν υπάρχει κάποια ένδειξη ότι έχουν τεθεί σε κίνδυνο, να περιλαμβάνουν τουλάχιστον τρεις από τις τέσσερις μορφές χαρακτήρων (κεφαλαία γράμματα, μικρά γράμματα, αριθμοί και ειδικοί χαρακτήρες). Επίσης, όταν αλλάξει ένας κωδικός πρόσβασης, οι τελευταίοι πέντε κωδικοί πρόσβασης ενδέχεται να μην επαναχρησιμοποιηθούν, ο ίδιος κωδικός πρόσβασης δεν θα πρέπει να χρησιμοποιείται για διαφορετικές προσβάσεις και οι κωδικοί πρόσβασης δεν πρέπει να σχετίζονται με προσωπικά στοιχεία όπως όνομα ή ημερομηνία γέννησης.

• θέσπιση συγκεκριμένης πολιτικής κωδικών πρόσβασης για τους διαχειριστές, όπως το ότι ποτέ δεν πρέπει να χρησιμοποιούν τον ίδιο κωδικό πρόσβασης για διαφορετικές προσβάσεις, δεν πρέπει να σχετίζονται με προσωπικά στοιχεία, να μην διατηρούνται ποτέ αποθηκευμένοι σε εφαρμογές και να επιτρέπεται ένας μέγιστος αριθμός προσπαθειών πέραν του οποίου εκδίδεται μια προειδοποίηση και αποκλείεται ο έλεγχος ταυτότητας.

• δημιουργία ενός αρχικού μοναδικού τυχαίου κωδικού πρόσβασης για κάθε λογαριασμό χρήστη, τον οποίο πρέπει να αλλάξει κατά την πρώτη σύνδεση και να ορίσει ένα νέο κωδικό πρόσβασης.

• επιμελής και διαβαθμισμένη αποθήκευση των πληροφοριών ελέγχου ταυτότητας, συμπεριλαμβανομένων των κωδικών πρόσβασης και των ιδιωτικών κλειδιών που συνδέονται με ηλεκτρονικά πιστοποιητικά, ώστε να είναι διασφαλισμένα και προσβάσιμα μόνο σε εξουσιοδοτημένους χρήστες.

1.9 Περιορισμένη διάρκεια αποθήκευσης

Στόχος είναι να μειωθεί η σοβαρότητα των κινδύνων, διασφαλίζοντας ότι τα προσωπικά δεδομένα δε διατηρούνται για περισσότερο από το αναγκαίο χρονικό διάστημα. Συνήθεις πρακτικές:

• ο καθορισμός, για κάθε κατηγορία δεδομένων, της διάρκειας αποθήκευσης που είναι χρονικά περιορισμένη και κατάλληλη για τους σκοπούς της επεξεργασίας και των νομικών απαιτήσεων.

• η δημιουργία αυτόματου μηχανισμού για την εκτέλεση ελέγχου κατά την επεξεργασία των δεδομένων, που επιτρέπει την ανίχνευση του τέλους της διάρκειας αποθήκευσης βάσει της ημερομηνίας δημιουργίας ή τελευταίας χρήσης των δεδομένων.

• ο καθορισμός μιας ενδιάμεσης διάρκειας αποθήκευσης, με την οποία τα δεδομένα καθίστανται διαθέσιμα αρχικά σε όλους για ορισμένο χρονικό διάστημα και έπειτα, σε έναν περιορισμένο αριθμό προσώπων.

• η ανάπτυξη αυτοματοποιημένης διαδικασίας διαγραφής των δεδομένων, συμπεριλαμβανομένης της καταγραφής των ιχνών, μετά τη λήξη της διάρκειας αποθήκευσης, με την επιφύλαξη της ενδιάμεσης αρχειοθέτησης των απαραίτητων δεδομένων.

• η κατανόηση του ότι η μείωση του αριθμού των διαθέσιμων και των επεξεργασμένων δεδομένων, η αρχειοθέτηση και η διαγραφή, συμβάλλουν στον περιορισμό των επιπτώσεων σε περίπτωση κλοπής ή τυχαίας διάδοσης της βάσης δεδομένων.

1.10 Πηγές κινδύνου σε ασφαλή απόσταση

Όσο αφορά τις μη ανθρώπινες πηγές κινδύνους, είναι απαραίτητο να ληφθούν τα εξής μέτρα προφύλαξης:

• αποθήκευση επικίνδυνων υλικών συμπεριλαμβανομένων των εύφλεκτων, διαβρωτικών, εκρηκτικών και υγρών αντικειμένων, σε κατάλληλες περιοχές αποθήκευσης και σε ασφαλή απόσταση από τις περιοχές επεξεργασίας των προσωπικών δεδομένων.

• μη αποθήκευση δεδομένων σε μια ξένη χώρα χωρίς εγγυήσεις που μπορούν να εξασφαλίσουν ένα κατάλληλο επίπεδο προστασίας δεδομένων, όπως την πρωθύστερη υπογραφή τυποποιημένων συμβατικών ρητρών ή δεσμευτικών κανόνων που έχουν εγκριθεί από την Ευρωπαϊκή Επιτροπή. Σε όλες τις περιπτώσεις, ο υπεύθυνος επεξεργασίας διατηρεί το ρόλο του ως προς την ασφάλεια των αποθηκευμένων προσωπικών δεδομένων και πρέπει να εξασφαλίζει το κατά συνθήκη κατάλληλο επίπεδο ασφάλειας αποθήκευσης.

1.11 Σκοποί: καθορισμένοι, σαφείς και νόμιμοι

Απαραίτητη συνθήκη για την ορθή υλοποίηση της προστασίας των προσωπικών δεδομένων, είναι η συμμόρφωση με τα άρθρα 5 & 6 του γενικού κανονισμού (GDPR), προς αποφυγή ασυμβίβαστων χρήσεων και φαινόμενων κατάχρησης. Ειδικότερα, θα πρέπει να προβλεφθεί:

- η λεπτομερής περιγραφή των σκοπών της επεξεργασίας δεδομένων και η αιτιολόγηση της νομιμότητάς τους.
- η ανάλυση των σκοπών της ανταλλαγής με τρίτους καθώς και της επεξεργασίας δεδομένων για τη βελτίωση της λειτουργίας της υπηρεσίας.
- η αποσαφήνιση συγκεκριμένων όρων υπό τους οποίους θα γίνεται η επεξεργασία.

1.12 Νομιμότητα της επεξεργασίας και απαγόρευση της κατάχρησης

Αδιαμφισβήτητα, αποτελεί τον ακρογωνιαίο λίθο του πλαισίου προστασίας των προσωπικών δεδομένων, το οποίο οριοθετείται ως εξής:

• Προσδιορισμός και αιτιολόγηση των κριτηρίων της νομιμότητας που ισχύει για την υπό εξέταση επεξεργασία δεδομένων. Προϋποθέτει ότι το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους και συγκεκριμένους σκοπούς όπως:

- για την εκτέλεση μιας σύμβασης στην οποία συμμετέχει το πρόσωπο στο οποίο αναφέρονται τα δεδομένα ή για να ληφθούν μέτρα κατόπιν αιτήματος του υποκειμένου των δεδομένων πριν από τη σύναψη της σύμβασης.
- για τη συμμόρφωση με μια νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.
- για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.

- για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή στην άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.
- για την εκτέλεση επεξεργασίας που πραγματοποιείται σύμφωνα με νομική υποχρέωση ή όταν είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται για λόγους δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας.

1.13 Διαχείριση των περιστατικών και των παραβιάσεων δεδομένων

Στόχος είναι ο εκάστοτε φορέας να αποκτήσει μια επιχειρησιακή οργάνωση, με την οποία να μπορεί να ανιχνεύει και να αντιμετωπίζει περιστατικά που ενδέχεται να επηρεάσουν τις ελευθερίες και το απόρρητο των προσώπων στα οποία αναφέρονται τα δεδομένα, καθώς είναι δυνατό να υιοθετηθούν οι εξής πρακτικές:

• ο καθορισμός των ρόλων και των ευθυνών των εργαζομένων καθώς και η θέσπιση διαδικασιών για την παροχή ανατροφοδότησης και απαντήσεων σε περίπτωση παραβίασης προσωπικών δεδομένων, μέσω επίσημης τεκμηρίωσης του DPO.

• η δημιουργία καταλόγου με τα άτομα που είναι υπεύθυνα για τη διαχείριση παραβιάσεων προσωπικών δεδομένων.

• η ανάπτυξη σχεδίου δράσης σε περίπτωση παραβίασης προσωπικών δεδομένων για κάθε υψηλό κίνδυνο, το οποίο θα ενημερώνεται και θα δοκιμάζεται περιοδικά, τουλάχιστον μία φορά κάθε δύο χρόνια.

• η κατηγοριοποίηση των παραβιάσεων των προσωπικών δεδομένων με βάση την επίδρασή τους στις ελευθερίες και στην ιδιωτική ζωή των υποκειμένων των δεδομένων.

• η αντιμετώπιση των περιστατικών με βάση την κατηγοριοποίησή τους ως απλό συμβάν, όχι τόσο σοβαρό συμβάν, καταστροφικό συμβάν ή κρίση. Ειδικότερα, εάν η παραβίαση αφορά ένα απλό συμβάν, καταγράφεται και ενημερώνεται ο "υπεύθυνος προστασίας δεδομένων" (DPO), εάν η παραβίαση συνεπάγεται ένα όχι τόσο σοβαρό συμβάν, αυτό επιλύεται και ταυτόχρονα ενημερώνονται τα υποκείμενα των δεδομένων που αφορά η παραβίαση, εάν η παραβίαση συνεπάγεται ένα καταστροφικό συμβάν, ξεκινά μια εις βάθος ανάλυση του περιστατικού και εάν η παραβίαση συνεπάγεται κρίση, ξεκινά η υλοποίηση του προβλεπόμενου σχέδιου διαχείρισης.

• η διατήρηση ενημερωμένων εγγράφων σχετικά με τις παραβιάσεις δεδομένων και συγκεκριμένα η καταγραφή του πλαισίου των παραβιάσεων των δεδομένων, της κατηγορίας των υποκειμένων των δεδομένων και των σχετικών αρχείων, τις επιπτώσεις παραβίασης και τα μέτρα που λαμβάνονται για την αντιμετώπισή τους.

• η λεπτομερής ανάλυση της δυνατότητας βελτίωσης των μέτρων ασφάλειας, σύμφωνα με τις παραβιάσεις προσωπικών δεδομένων που έχουν συμβεί.

1.14 Διαχείριση προσωπικού

Στόχος είναι να μειωθεί η πιθανότητα να επηρεαστούν αρνητικά τα προσωπικά δεδομένα, από μη επαρκείς δεξιότητες, δόλο ή αμέλεια των εργαζομένων, που τα επεξεργάζονται. Προς διασφάλιση αυτού, κρίνεται επιβεβλημένη:

• η πρόσβαση σε προσωπικά δεδομένα και η επεξεργασία αυτών από άτομα ικανά για τη συγκεκριμένη εργασία, με επαρκή κατάρτιση και κατάλληλα προσόντα.

• η εξασφάλιση ικανοποιητικών συνθηκών εργασίας.

• η αύξηση της ευαισθητοποίησης, σχετικά με τους κινδύνους που σχετίζονται με τα τρωτά σημεία των προσωπικών δεδομένων. Ειδικότερα, θα πρέπει να γίνει ιδιαίτερη μνεία στο γεγονός ότι κακόβουλα άτομα μπορούν να επωφεληθούν από εργαζόμενους που μιλούν πάρα πολύ, είναι προβλέψιμοι στις ενέργειές τους, επηρεάζονται ή είναι ευάλωτοι στις πιέσεις που τους ασκούνται.

1.15 Διαχείριση των θέσεων εργασίας

Αναζητείται ο περιορισμός της πιθανότητας χρήσης των χαρακτηριστικών του λογισμικού που επηρεάζουν αρνητικά τα προσωπικά δεδομένα όπως ενημερώσεις λογισμικού, φυσική προστασία και πρόσβαση, έλεγχοι ακεραιότητας. Προς αυτή την κατεύθυνση, κινούνται οι κάτωθι πρακτικές:

• η εξασφάλιση, μέσω του τμήματος πληροφορικής, στους χρήστες, σταθμών εργασίας που διατηρούνται ασφαλείς και λειτουργικοί.

• η ανάκτηση δεδομένων, με εξαίρεση τα δεδομένα που ορίζονται ως ιδιωτικά ή προσωπικά, από τους σταθμούς εργασίας προτού ανατεθούν σε άλλα άτομα.

• η διαγραφή των δεδομένων από τους σταθμούς εργασίας πριν την εκχώρηση τους σε άλλα άτομα, ιδίως αν μοιράζονται ίδιες θέσεις εργασίας.

• η επιθεώρηση του σταθμού εργασίας, για σημάδια διείσδυσης, προκειμένου να διαπιστωθεί εάν έχουν αλλοιωθεί οι πληροφορίες από τον εισβολέα.

• η διατήρηση ενημερωμένων συστημάτων και εφαρμογών με εγκατάσταση εκδόσεων, ενημερώσεων ασφαλείας και αδειών χρήσης που διατηρούνται από τον κατασκευαστή ή άλλη υπηρεσία.

• ο ορισμός δημόσιων ή ιδιωτικών IP διευθύνσεων, εκεί που πραγματικά χρειάζονται με ταυτόχρονη απενεργοποίηση ή και διαγραφή υπηρεσιών που δεν είναι

απολύτως απαραίτητες, περιττών λογαριασμών, του autorun όταν εισάγεται μια αφαιρούμενη συσκευή.

• η ενεργοποίηση μέτρων προστασίας που παρέχονται από το σύστημα και τις εφαρμογές, όπως το τείχος προστασίας, οι αυτόματες ενημερώσεις, η προστασία κακόβουλου λογισμικού.

• η απαγόρευση τοπικής κοινής χρήσης καταλόγων ή δεδομένων σε σταθμούς εργασίας.

• η αποθήκευση δεδομένων σε ένα δικτυακό αποθηκευτικό χώρο και όχι σε σταθμούς εργασίας τοπικά.

• η διασφάλιση της διαμόρφωσης των προγραμμάτων περιήγησης Web η οποία πρέπει να περιλαμβάνει την προστασία των προσωπικών πληροφοριών που αποθηκεύονται από τα προγράμματα περιήγησης όπως φόρμες, κωδικοί πρόσβασης, πιστοποιητικά, τη χρήση ενός κύριου κωδικού πρόσβασης στο Mozilla Firefox, την αδυναμία αποθήκευσης κωδικών πρόσβασης σε περίπτωση υψηλού κινδύνου.

• η απαγόρευση χρήσης εφαρμογών που έχουν ληφθεί και δεν προέρχονται από ασφαλείς πηγές.

• ο έλεγχος της ακεραιότητας του συστήματος, παρακολουθώντας συνεχώς τις αλλαγές που πραγματοποιούνται σε ορισμένα αρχεία ή καταλόγους, στο μητρώο και στις διεργασίες του συστήματος, στην παρουσία rootkits.

• η εξαγωγή των αρχείων καταγραφής, χρησιμοποιώντας λειτουργίες διαχείρισης τομέα ή λειτουργίες διαχείρισης μέσω syslog client.

1.16 Διαχείριση κινδύνου

Στόχος είναι ο έλεγχος των κινδύνων που συνεπάγονται οι διαδικασίες επεξεργασίας που εκτελεί ο εκάστοτε φορέας και που αφορούν τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Λόγω της κρισιμότητας αυτού, απαιτούνται οι εξής συνθήκες:

• η καταγραφή των διαδικασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα, είτε είναι αυτοματοποιημένες είτε όχι, των επεξεργασμένων δεδομένων όπως αρχεία πελατών, συμβόλαια και των υποστηρικτικών στοιχείων στα οποία βασίζονται όπως: το υλικό (server, φορητός υπολογιστής, CD-ROM), λογισμικό (λειτουργικό σύστημα), κανάλια επικοινωνίας (οπτικές ίνες, Wi-Fi, Internet) και έγγραφα (εκτυπωμένα, φωτοαντίγραφα).

• η αξιολόγηση του τρόπου τήρησης των θεμελιωδών αρχών όπως των πληροφοριών, της συγκατάθεσης, του δικαιώματος πρόσβασης.

• η αξιολόγηση των κινδύνων που ελλοχεύει κάθε επεξεργασία αλλά και των πιθανών επιπτώσεων στα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα, όταν εκδηλωθούν κίνδυνοι όπως:

1. Αδικαιολόγητη πρόσβαση σε προσωπικά δεδομένα.
2. Ανεπιθύμητη αλλαγή δεδομένων.
3. Εξαφάνιση δεδομένων.

Εξίσου σημαντικός είναι και ο προσδιορισμός:

▪ των πηγών κινδύνου λαμβάνοντας υπόψη, τις εσωτερικές και εξωτερικές ανθρώπινες πηγές, είτε τυχαίες είτε σκόπιμες αλλά και τις εσωτερικές ή εξωτερικές μη ανθρώπινες πηγές όπως φυσικές καταστροφές, ιοί υπολογιστών.

▪ των απειλών που θα μπορούσαν να υλοποιηθούν λόγω κατάχρησης δικαιωμάτων ή λάθος χειρισμού, παρακολούθησης λογισμικού ή υλικού, λειτουργία στο παρασκήνιο κάποιου keylogger, ακούσιας εγκατάστασης κακόβουλου λογισμικού, κλοπής σταθμού εργασίας ή απώλειας USB flash drive, κακής λειτουργίας λόγω φυσικής φθοράς, επίθεσης άρνησης εξυπηρέτησης (virus).

▪ των υφιστάμενων ή προγραμματισμένων μέτρων τεχνικών και οργανωτικών για την αντιμετώπιση κάθε κινδύνου όπως έλεγχος πρόσβασης, δημιουργία αντιγράφων ασφαλείας, ιχνηλασιμότητα, ασφάλεια εγκαταστάσεων, κρυπτογράφηση και ανωνυμοποίηση.

▪ η εκτίμηση της σοβαρότητας και την πιθανότητας των παραπάνω κινδύνων, υπό το πρίσμα των προηγούμενων πληροφοριών και λαμβάνοντας υπόψη τα υπάρχοντα ή ελεγχόμενα μέτρα.

▪ η εφαρμογή και ο έλεγχος των προγραμματισμένων μέτρων όταν θεωρούνται κατάλληλα για τη διασφάλιση του σωστού επιπέδου ασφάλειας, υπό το πρίσμα των κινδύνων.

▪ η πραγματοποίηση περιοδικών ελέγχων ασφαλείας σε ετήσια βάση όπου είναι δυνατόν.

Συμπερασματικά, οι κίνδυνοι ασφάλειας της πληροφορίας μπορούν να μελετηθούν ταυτόχρονα με τους κινδύνους ιδιωτικής ζωής, δεδομένου ότι οι δύο προσεγγίσεις μελέτης είναι συμβατές και δεν είναι δύσκολο να συνδυαστούν, με σκοπό τον προσδιορισμό των τεχνικών και οργανωτικών μέτρων που χρειάζονται.

1.17 Κακόβουλο λογισμικό (malware)

Στόχος είναι η προστασία της πρόσβασης σε δημόσια και μη ελεγχόμενα δίκτυα, σταθμούς εργασίας και διακομιστές από κακόβουλους κώδικες που θα μπορούσαν να επηρεάσουν την ασφάλεια των προσωπικών δεδομένων όπως antivirus, firewall, proxy, anti-spyware. Προς τούτο, χρήσιμη είναι:

• η εγκατάσταση και η συνεχής ενημέρωση antivirus/ antimalware προγραμμάτων, σε διακομιστές και σταθμούς εργασίας, με ταυτόχρονη εξασφάλιση της ανάλυσης του συστήματος σε πραγματικό χρόνο, σύμφωνα με τους κανόνες που ορίζονται από το τμήμα πληροφορικής του φορέα.

• η εφαρμογή μέτρων φιλτραρίσματος ως προς τις εισροές και εκροές δικτύου, δηλαδή χρήση κάποιου firewall.

• η καταγραφή και μεταφορά των συμβάντων προστασίας από ιούς σε κεντρικό διακομιστή για στατιστική ανάλυση και διαχείριση των προβλημάτων, όπως ο εντοπισμός του μολυσμένου διακομιστή ή του ιού που έχει ανιχνευθεί και δεν εξαλείφεται από το antivirus.

1.18 Συντήρηση

1.18.1 Γενικά μέτρα

Το πεδίο επέλευσης των κινδύνων εντοπίζεται, εν δυνάμει, και στις εργασίες συντήρησης υλικού και λογισμικού όπως η απομακρυσμένη συντήρηση ή η διαγραφή δεδομένων. Προς εξάλειψη αυτών, χρήσιμοι μηχανισμοί θεωρούνται:

• η καθιέρωση σύμβασης προμήθειας για τη διαχείριση εργασιών συντήρησης όταν αυτές εκτελούνται από παρόχους υπηρεσιών.

• η λεπτομερής καταγραφή των εργασιών συντήρησης.

• η διαχείριση λειτουργιών απομακρυσμένης συντήρησης με συστηματική χρήση κρυπτογραφημένων καναλιών επικοινωνίας, ισχυρών κλειδιών ελέγχου ταυτότητας ή κωδικών πρόσβασης.

• η κρυπτογράφηση ή διαγραφή δεδομένων που περιέχονται στο υλικό επιτραπέζιων, φορητών υπολογιστών ή servers, που αποστέλλονται για εξωτερική συντήρηση.

1.18.2 Εκτυπωτές πολλαπλών λειτουργιών και φωτοαντιγραφικά

• Ορισμός κατάλληλων μέτρων αποκλεισμού της πρόσβασης σε προσωπικά δεδομένα, στη περίπτωση που η συντήρηση εκτελείται από εξωτερικό συνεργάτη.

• Υπογραφή συμφωνίας με την εταιρεία συντήρησης, εμπιστευτικότητας και πραγματοποίησης των επιδιορθώσεων επιτόπου, παρουσία ενός μέλους του τμήματος πληροφορικής, σε περιπτώσεις όπου τα δεδομένα είναι ευαίσθητα και δεν μπορούν να κρυπτογραφηθούν ή να διαγραφούν πλήρως, όπως σε περιπτώσεις βλάβης του σκληρού δίσκου ή δυσλειτουργίας του

• Απαγόρευση αποστολής υλικού που περιέχει ευαίσθητα δεδομένα για συντήρηση.

• Αποκλεισμός της πρόσβασης σε προσωπικά δεδομένα που είναι τυχόν αποθηκευμένα στους "κάδους ανακύκλωσης" πολυλειτουργικών εκτυπωτών ή φωτοαντιγραφικών μηχανημάτων, μετά από επιλογή διαγραφής της εργασίας από τον εκάστοτε χρήστη, χρησιμοποιώντας ένα ασφαλές εργαλείο διαγραφής των δεδομένων από τους σκληρούς δίσκους ή την ενσωματωμένη μνήμη των μηχανημάτων.

1.19 Ελαχιστοποίηση δεδομένων

Στόχος είναι η συμμόρφωση με τα άρθρα 5 παράγραφος 1 στ. γ' και 6 του γενικού κανονισμού για την προστασία των δεδομένων (GDPR), για τη μείωση της βαρύτητας των κινδύνων, περιορίζοντας την ποσότητα των προσωπικών δεδομένων σε αυτά που είναι απολύτως απαραίτητα, ώστε να αποφευχθεί η συλλογή περιττών δεδομένων, να χρησιμοποιούνται δεδομένα που δεν επηρεάζουν τον τελικό σκοπό και δεν έχουν υπερβολικές επιπτώσεις για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα.

Το ανωτέρω αυτονόητο αίτημα υλοποιείται με τους εξής τρόπους:

• αιτιολόγηση συλλογής κάθε στοιχείου.

• σαφής διάκριση ανώνυμων και ψευδώνυμων δεδομένων.

• αποφυγή ενσωμάτωσης "σχολίων" ως πεδία κειμένου ελεύθερης μορφής, λόγω του ότι οι χρήστες καταγράφουν εκεί πληροφορίες που δεν συμμορφώνονται με τις αρχές ελαχιστοποίησης όπως μη δηλωμένα ευαίσθητα δεδομένα. Συνεπώς, πρέπει να προτιμηθούν τα πεδία τύπου λίστας κύλισης.

• επιβεβαίωση ότι τα προσωπικά δεδομένα είναι επαρκή, συναφή και όχι υπερβολικά σε σχέση με τον επιδιωκόμενο σκοπό.

• επιβεβαίωση ότι τα προσωπικά δεδομένα δεν αποκαλύπτουν άμεσα ή έμμεσα, τη φυλετική ή εθνική καταγωγή, τις πολιτικές, φιλοσοφικές ή θρησκευτικές απόψεις, την ένταξη σε συνδικαλιστικές οργανώσεις, πληροφορίες για την υγεία ή πληροφορίες σχετικά με τη σεξουαλική ζωή ενός ατόμου.

• επιβεβαίωση ότι τα προσωπικά δεδομένα δε σχετίζονται με αδικήματα, ποινικές καταδίκες ή μέτρα ασφαλείας.

• αποφυγή συλλογής πρόσθετων προσωπικών δεδομένων.

• ιδιαίτερα περιορισμένη και δικαιολογημένη, λόγω της ευαίσθητης φύσης των δεδομένων, λήψη, σχετικά με ανήλικους, τους γονείς τους ή μέλη της οικογένειάς τους, λαμβάνοντας υπόψη την αρχή της δίκαιης συλλογής όσο αφορά έναν ευάλωτο χρήστη.

1.20 Οργάνωση

Στόχος είναι η απόκτηση ικανοτήτων διαχείρισης και ελέγχου, από τον εκάστοτε φορέα, της προστασίας των προσωπικών δεδομένων που τηρούνται σε αυτόν. Για την εύρυθμη οργάνωση, χρήζει:

• ο διορισμός υπεύθυνου προστασίας δεδομένων (DPO), με σαφή καθήκοντα και περιγραφή της θέσης εργασίας του, προκειμένου να εκτελεί τα καθήκοντά του, χωρίς καμία σύγκρουση συμφερόντων.

• ο καθορισμός ρόλων, ευθυνών και αλληλεπιδράσεων μεταξύ όλων των ενδιαφερομένων μερών που εμπλέκονται στην προστασία δεδομένων.

• η δημιουργία επιτροπής παρακολούθησης, η οποία θα αποτελείται από τον υπεύθυνο επεξεργασίας δεδομένων, έναν υπεύθυνο “βοηθό” του DPO και τα ενδιαφερόμενα μέρη. Η επιτροπή αυτή πρέπει να συνεδριάζει τακτικά για να θέτει στόχους και να αναθεωρεί το σύνολο των εργασιών επεξεργασίας του οργανισμού.

1.21 Κώδικας δεοντολογίας

Ακρογωνιαίος λίθος του όλου εγχειρήματος της πολιτικής προστασίας των δεδομένων, είναι η δημιουργία μιας βασικής τεκμηρίωσης η οποία θα καθορίζει τους στόχους και τους κανόνες προστασίας, το σχέδιο δράσης και τη τακτική επανεξέταση του πλαισίου αυτής.

Μεταξύ των απαιτούμενων δράσεων, μπορούν να καταγραφούν:

• ο καθορισμός σημαντικών πτυχών σχετικά με την προστασία των δεδομένων, μέσα από μια βάση τεκμηρίωσης που αποτελεί την πολιτική προστασίας των δεδομένων και σε μορφή προσαρμοσμένη σε κάθε είδους περιεχόμενο όπως κίνδυνοι, βασικές αρχές

που πρέπει να ακολουθούνται, στόχοι και κανόνες που πρέπει να εφαρμόζονται. Ειδικότερα, η χάραξη πολιτικής θα πρέπει να περιλαμβάνει τεκμηριωμένες απαιτήσεις ως ένα σύνολο προδιαγραφών, τη δέσμευση της διοίκησης του φορέα για προστασία της ιδιωτικής ζωής και των δεδομένων, τις κατευθυντήριες γραμμές για τους χρήστες και τη διαδικασία για την ενσωμάτωση θεμάτων προστασίας δεδομένων σε έργα.

• η διανομή της πολιτικής προστασίας δεδομένων σε εκείνους που είναι υπεύθυνοι για την επιβολή της.

• η καθιέρωση πολυετούς σχεδίου δράσης και παρακολούθηση της εφαρμογής του όπως και η θέσπιση εξαιρέσεων από την πολιτική προστασίας δεδομένων.

• ο τακτικός έλεγχος της τήρησης των κανόνων.

• η δυνατότητα τακτικής αναθεώρησης του πλαισίου προστασίας.

1.22 Ποιότητα δεδομένων

Για την αποφυγή υπολογισμών με βάση λανθασμένα ή παρωχημένα δεδομένα, να εκτελούνται:

- τακτικοί έλεγχοι της ακρίβειας των προσωπικών δεδομένων του χρήστη.
- έλεγχοι από τη μεριά του χρήστη και ενημέρωση των δεδομένων σε τακτά χρονικά διαστήματα.
- έλεγχοι για ανίχνευση οποιασδήποτε αλλαγής δεδομένων.

1.23 Αντίγραφα ασφαλείας

Στόχος είναι η διασφάλιση της διαθεσιμότητας και της ακεραιότητας των προσωπικών δεδομένων, διατηρώντας παράλληλα την εμπιστευτικότητά τους με αντίγραφα ασφαλείας σε τακτά χρονικά διαστήματα, κρυπτογράφηση του καναλιού μετάδοσης δεδομένων, δοκιμή ακεραιότητας.

Ενδεικτική αναφορά των τρόπων:

• δημιουργία αντιγράφων ασφαλείας των προσωπικών δεδομένων σε τακτά χρονικά διαστήματα, είτε σε χαρτί είτε σε ηλεκτρονική μορφή, με βάση τις απαιτήσεις διαθεσιμότητας και ακεραιότητας του εκάστοτε φορέα. Τα αντίγραφα ασφαλείας μπορούν να επαληθευτούν αυτόματα, ακολουθώντας την επαλήθευση που εγγυάται την ακεραιότητα, με τη δημιουργία μιας αναφοράς στο τέλος της δημιουργίας αντιγράφων ασφαλείας.

• εφαρμογή μηχανισμών κρυπτογράφησης του καναλιού μετάδοσης δεδομένων όταν η δημιουργία αντιγράφων ασφαλείας μέσω δικτύου είναι αυτοματοποιημένη.

• προστασία του αντίγραφου ασφαλείας (back up) των προσωπικών δεδομένων με το ίδιο επίπεδο ασφαλείας όπως εκείνο που εφαρμόζεται στις λοιπές λειτουργίες.

• τακτικός έλεγχος των αντιγράφων ασφαλείας, λαμβάνοντας ένα δείγμα δεδομένων προς έλεγχο ανά μήνα και ένα πλήρες σύνολο δεδομένων ανά έτος.

• έλεγχος της ακεραιότητας των δεδομένων ασφαλείας, σύμφωνα με τις απαιτήσεις του εκάστοτε φορέα.

• τυπική τεκμηρίωση του επιπέδου δέσμευσης του τμήματος πληροφορικής για την ανάκτηση κρυπτογραφημένων πληροφοριών σε περίπτωση απώλειας ή μη διαθεσιμότητας των μυστικών κλειδιών που εξασφαλίζουν την κρυπτογράφηση.

• διασφάλιση ότι ο φορέας, το προσωπικό, τα συστήματα και οι εγκαταστάσεις που είναι απαραίτητες για τη διεξαγωγή της επεξεργασίας, ανταποκρίνονται στις ανάγκες.

• απαγόρευση μεταφοράς δεδομένων προσωπικού χαρακτήρα και αντιγράφων ασφαλείας εκτός του κτιρίου.

• θέσπιση μιας διαδικασίας δημιουργίας αντιγράφων ασφαλείας και ενός σχεδίου που επιτρέπουν την εξασφάλιση της ακεραιότητας και της βιωσιμότητας των προσωπικών δεδομένων, χωρίς να τίθεται σε κίνδυνο η εμπιστευτικότητά τους.

• σχεδιασμός εφεδρικού σχεδίου με ταυτόχρονο καθορισμό των επιχειρησιακών και τεχνικών μέσων που πρέπει να ληφθούν για την τήρησή του.

1.24 Πάροχοι υπηρεσιών cloud computing & cloud storage

Πέρα από τις ορθές πρακτικές που υιοθετούνται στην περίπτωση που χρησιμοποιείται μια υπηρεσία cloud computing σχετική με τη λειτουργία του φορέα σε περιβάλλον νέφους, μπορούν να εφαρμοστούν και οι παρακάτω:

• απαίτηση από τον πάροχο της υπηρεσίας νέφους, να εφαρμόσει τουλάχιστον ένα λογικό διαχωρισμό μεταξύ των δεδομένων του φορέα και των δεδομένων των άλλων πελατών του.

• καθορισμός ξεκάθαρων χώρων αποθήκευσης στο νέφος, στους οποίους θα αποθηκευτούν τα δεδομένα και η δέσμευση για απομόνωση και προστασία των συγκεκριμένων χώρων από πιθανές απόπειρες πρόσβασης στα αποθηκευμένα δεδομένα, από τρίτους.

1.25 Εποπτεία

Απώτερος σκοπός είναι η απόκτηση μια ολοκληρωμένης και ενημερωμένης εικόνας για την προστασία των δεδομένων και την εν γένει συμμόρφωση τους με την ευρωπαϊκή νομοθεσία. Μεταξύ των ενδεδειγμένων τρόπων είναι και οι κάτωθι:

• τακτικός έλεγχος των εργασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα και επιβεβαίωση ότι συμμορφώνονται με το νόμο, είναι αποτελεσματικές και κατάλληλες, με διενέργεια δειγματοληπτικών ελέγχων των πιο ευαίσθητων διαδικασιών επεξεργασίας και των πράξεων που αποτελούν αντικείμενο παραβιάσεων προσωπικών δεδομένων.

• καθορισμός στόχων προστασίας δεδομένων αλλά και καθορισμός δεικτών για τον υπολογισμό του κατά πόσον πληρούνται αυτοί.

• τακτική αξιολόγηση (σε ετήσια βάση) του ποσοστού συμμόρφωσης με την πολιτική προστασίας δεδομένων και σύνταξη έκθεσης προόδου σχετικά με τις προγραμματισμένες δράσεις.

1.26 Επιτήρηση

1.26.1 Γενικά μέτρα

Στόχος είναι ο έγκαιρος εντοπισμός περιστατικών που αφορούν δεδομένα προσωπικού χαρακτήρα και η διάθεση πληροφοριών που μπορούν να χρησιμοποιηθούν για την ανάλυσή τους ή για την παροχή αποδείξεων σε σχέση με έρευνες για πολιτικές και αρχιτεκτονικές καταγραφής δεδομένων και συμμόρφωση με τις υποχρεώσεις προστασίας προσωπικών δεδομένων.

Ειδικότερα, χρήζει να προβλεφθεί:

• η εγκατάσταση και ρύθμιση αρχιτεκτονικής καταγραφής που διατηρεί ένα αρχείο συμβάντων ασφαλείας και το χρόνο που συνέβησαν, καταγράφοντας την ημερομηνία και τη χρονική σήμανση των περιστατικών.

• η επιλογή των περιστατικών που θα καταγράφονται, να πραγματοποιείται βάσει καθορισμένου πλαισίου το οποίο θα περιλαμβάνει τους σταθμούς εργασίας, τα μέτρα προστασίας, τον εξοπλισμό δικτύου και διακομιστών δικτύου, τους κινδύνους καθώς και το σε ισχύ νομικό πλαίσιο.

• η διεξαγωγή περιοδικών αναλύσεων των καταγεγραμμένων πληροφοριών και η δημιουργία συστήματος αυτόματης ανίχνευσης αδύναμων σημείων.

• ο ορισμός του χρόνου διατήρησης των αρχείων καταγραφής περιστατικών για έξι μήνες, εκτός εάν νομικοί και κανονιστικοί περιορισμοί απαιτούν συγκεκριμένες διάρκειες αποθήκευσης.

1.26.2 Ειδικά μέτρα για θέση εργασίας

• Λεπτομερής αποτύπωση των συμβάντων που σχετίζονται με την εφαρμογή καταγραφής, την ασφάλεια και το σύστημα η οποία περιλαμβάνει τις συνδέσεις των χρηστών ανά θέση εργασίας στο σύστημα με το αναγνωριστικό τους (Username και Password), την ημερομηνία και την ώρα της προσπάθειας σύνδεσης, εάν η σύνδεση ήταν επιτυχής ή όχι, την ημερομηνία και ώρα της αποσύνδεσής τους καθώς και τυχόν προσπάθειες αλλαγών στην ασφάλεια του συστήματος.

• Εξαγωγή των αρχείων καταγραφής με τη χρήση λειτουργιών διαχείρισης τομέα ή μέσω syslog client.

• Ανάλυση του τύπου πρωτοκόλλου που χρησιμοποιήθηκε για τη σύνδεση και του τύπου χρήστη που το χρησιμοποίησε, της αρχικής IP διεύθυνσης με την οποία συνδέθηκε, τυχόν διαδοχικών βλαβών σύνδεσης και των μη προγραμματισμένων διακοπών σε επίπεδο εφαρμογών ή εργασιών.

1.26.3 Ειδικά μέτρα για τείχος προστασίας

• Καθορισμός πολιτικής φιλτραρίσματος που απαγορεύει οποιαδήποτε άμεση επικοινωνία μεταξύ των εσωτερικών σταθμών εργασίας και του "έξω κόσμου", επιτρέποντας συνδέσεις μόνο μέσω του τείχους προστασίας και μόνο μέσω ρητά εξουσιοδοτημένων και απαραίτητων ροών.

• Καταγραφή όλων των επιτυχημένων εξουσιοδοτημένων συνδέσεων αλλά και όλων των απορριφθέντων προσπαθειών για σύνδεση.

• Εξαγωγή των αρχείων καταγραφής, μέσω ασφαλών καναλιών, σε ειδικό server.

1.26.4 Ειδικά μέτρα για εξοπλισμό δικτύου

• Καταγραφή της δραστηριότητας σε κάθε θύρα ενός switch ή ενός router.

• Εξαγωγή αρχείων καταγραφής σε έναν αποκλειστικό server με χρήση ενσωματωμένου syslog client ή μέσω ενός netflow, δίνοντας τη δυνατότητα συλλογής της κίνησης των IP διευθύνσεων σε ένα δίκτυο, καθώς εισέρχονται σε αυτό ή εξέρχονται από αυτό, δίνοντας μια εικόνα της κυκλοφοριακής ροής και του όγκου των δεδομένων στο δίκτυο.

• Παρακολούθηση του όγκου των δεδομένων βάσει των χρόνων καθώς και η παρακολούθηση της συμμόρφωσης με λίστες ελέγχου πρόσβασης Access Control Lists (ACL) για τα routers.

1.26.5 Ειδικά μέτρα για servers

• Καταγραφή όσο το δυνατόν περισσότερων πληροφοριών σχετικά με τις αιτήσεις των clients στους web servers, προκειμένου να εντοπιστούν ελαττώματα διαμόρφωσης και επιθέσεις SQL injections.

• Λεπτομερής καταγραφή της δραστηριότητας των χρηστών στους διακομιστές μεσολάβησης (proxy servers).

• Καταγραφή όλων των ερωτημάτων που γίνονται στους διακομιστές DNS, είτε "τρέχουν" από χρήστες του Διαδικτύου είτε από εσωτερικούς χρήστες του δικτύου.

• Καταγραφή δεδομένων ταυτοποίησης σύμφωνα με το χρόνο, την ημερομηνία και τη διάρκεια κάθε σύνδεσης στους διακομιστές απομακρυσμένης πρόσβασης (remote access servers).

• Καταγραφή της λήψης και διαχείρισης των μηνυμάτων στους διακομιστές ανταλλαγής μηνυμάτων.

1.27 Ασφάλεια δικτύων

1.27.1 Γενικά μέτρα

Προς αποφυγή της πιθανότητας τα χαρακτηριστικά των δικτύων επικοινωνίας όπως ενσύρματα δίκτυα, Wi-Fi και οπτικές ίνες, να επηρεάσουν αρνητικά τα προσωπικά δεδομένα, χρήζει να ληφθούν τα κάτωθι προληπτικά μέτρα προστασίας:

• καταγραφή και ενημέρωση ενός λεπτομερή χάρτη του δικτύου.

• καταγραφή όλων των θυρών πρόσβασης στο Διαδίκτυο (ports) και πρόσθεσή τους στο παραπάνω χάρτη δικτύου.

• διασφάλιση της διαθεσιμότητας των δικτύων υπολογιστών του φορέα για επικοινωνία έτσι ώστε να είναι σε θέση να χειριστούν τις αναμενόμενες ροές κυκλοφορίας και να έχουν εναλλακτικές λύσεις σε περίπτωση βλάβης.

• κατανομή του δικτύου σε αξιόπιστα λογικά υποδίκτυα, βάσει των υπηρεσιών που πρόκειται να αναπτυχθούν, με διαμοιρασμό ουσιαστικά των δικτύων σε εικονικά δίκτυα (VLAN), προκειμένου να ελέγχεται σε πραγματικό χρόνο η ροή των δεδομένων με βάση τις ενεργές διευθύνσεις δικτύου.

• απαγόρευση κάθε άμεσης επικοινωνίας μεταξύ εσωτερικών σταθμών εργασίας και εξωτερικών δικτύων.

• χρήση μόνο συνδέσεων που επιτρέπονται ρητά από ένα τείχος προστασίας, με ταυτόχρονο περιορισμό των απολύτως απαραίτητων θυρών επικοινωνίας και στην περίπτωση που οι web servers είναι προσβάσιμοι μόνο μέσω του πρωτοκόλλου SSL, να επιτρέπεται μόνο η εισερχόμενη κίνηση μιας IP διεύθυνσης στη θύρα 443 και να αποκλείονται όλες οι άλλες θύρες επικοινωνίας.

• παρακολούθηση της δραστηριότητας δικτύου με τη χρήση συστημάτων ανίχνευσης εισβολών ή συστήματος πρόληψης εισβολής και ανάλυση της κυκλοφορίας του δικτύου σε πραγματικό χρόνο και με ταυτόχρονη ανίχνευση κάθε ύποπτης δραστηριότητας η οποία υποδηλώνει την εκδήλωση επιθέσεων στον κυβερνοχώρο.

• εκπόνηση ενός στρατηγικού σχεδίου αντιμετώπισης της εισβολής με οργανωτικά και τεχνικά μέτρα.

• ασφαλής διαχείριση της κυκλοφορίας και περιορισμός ή απαγόρευση της φυσικής και λογικής πρόσβασης σε απομακρυσμένες θύρες, θέτοντας σε όλες τις εργασίες διαχείρισης στους τοπικούς πόρους, πρωτόκολλα ασφαλούς διαχείρισης.

1.27.2 Ειδικά μέτρα για εργαλεία απομακρυσμένης διαχείρισης

• Περιορισμός της απομακρυσμένης διαχείρισης πόρων του συστήματος μόνο από το προσωπικό του τμήματος πληροφορικής του εκάστοτε φορέα και μόνο εάν εμπίπτει στα όρια των καθηκόντων τους.

• Προσδιορισμός μοναδικών χρηστών - εργαλείων για απομακρυσμένη διαχείριση και η πιστοποίησή τους με τουλάχιστον έναν ισχυρό κωδικό πρόσβασης και όπου είναι δυνατόν, με ένα ψηφιακό πιστοποιητικό.

• Διατήρηση ενός αρχείου καταγραφής της δραστηριότητας των χρηστών - εργαλείων απομακρυσμένης διαχείρισης.

• Ρητή απαγόρευση αλλαγών τόσο στις ρυθμίσεις ασφαλείας του εργαλείου όσο και στην προβολή των κωδικών πρόσβασης ή των μυστικών πληροφοριών που χρησιμοποιήθηκαν.

• Κρυπτογράφηση των ροών κυκλοφορίας της απομακρυσμένης διαχείρισης.

• Ενημέρωση του χρήστη - υπαλλήλου, μέσω μιας ειδικής οπτικής ή ακουστικής σήμανσης, ότι η απομακρυσμένη διαχείριση βρίσκεται σε εξέλιξη στον σταθμό εργασίας του.

1.27.3 Ειδικά μέτρα για περιήγηση στο Web

• Χρήση του πρωτοκόλλου SSL (HTTPS) για την εξασφάλιση του ελέγχου ταυτότητας του διακομιστή και της εμπιστευτικότητας των επικοινωνιών.

1.27 4 Ειδικά μέτρα για μεταφορά αρχείων

• Χρήση του πρωτοκόλλου SFTP (SSH File Transfer Protocol) για ασφαλή μεταφορά αρχείων ή ενδεχομένως του πεπαλαιωμένου αλλά σχεδόν καθολικά υποστηριζόμενου από Unix πλατφόρμες, πρωτοκόλλου SCP (Secure Copy Protocol).

• Κρυπτογράφηση των αρχείων πάντα πριν την αποστολή τους, σε περίπτωση υψηλής επικινδυνότητας.

1.27.5 Ειδικά μέτρα για ηλεκτρονικό ταχυδρομείο

• Κρυπτογράφηση συνημμένων αρχείων που περιέχουν προσωπικά δεδομένα.

• Σαφής ενημέρωση των χρηστών ότι πρέπει να αποφεύγουν να ανοίγουν μηνύματα άγνωστης προέλευσης και ιδίως συνημμένα με επεκτάσεις όπως .pif, .com, .bat, .exe, .vbs και .lnk.

• Ευαισθητοποίηση των χρηστών user awareness για ενδεχόμενες απειλές που περιλαμβάνει την ερμηνεία των προειδοποιήσεων, την αναφορά των διαφόρων απειλών στο αρμόδιο τμήμα πληροφορικής και την ικανότητα να αντιλαμβάνεται αν έχει πέσει θύμα επίθεσης.

1.28 Ασφάλεια υλικού hardware

Μέριμνα της πολιτικής προστασίας δεδομένων προσωπικού χαρακτήρα είναι ο περιορισμός της πιθανότητας επίφοβης χρησιμοποίησης των χαρακτηριστικών του υλικού όπως servers, desktops, laptops, usb memory sticks κ.α. Σ' αυτή την προσπάθεια, κρίνονται ως θετικές οι εξής πρακτικές:

• διατήρηση λίστας σταθμών εργασίας και χρηστών, τοπικά διαχειριζόμενων servers, εξοπλισμού δικτύου και τηλεπικοινωνιών, εκτυπωτών. Η λίστα αυτή πρέπει να καθορίζει πληροφορίες σχετικά με τον εξοπλισμό, τον τύπο του λειτουργικού συστήματος, το δίκτυο όπως διεύθυνση IP και διεύθυνση MAC, τις κύριες εφαρμογές που εκτελεί, τις προηγούμενες εκδόσεις τους και τις εγκατεστημένες ενημερώσεις.

• επιβεβαίωση ότι τα μεγέθη χωρητικότητας, αποθήκευσης και επεξεργασίας των σταθμών εργασίας καθώς και οι συνθήκες χρήσης των δεδομένων σε αυτά, είναι συμβατά με την προβλεπόμενη χρήση του υλικού.

• επιβεβαίωση ότι οι τροφοδοτικές διατάξεις των σταθμών εργασίας και των servers προστατεύονται από τις μεταβολές της τάσης και ότι δημιουργούν, ανεμπόδιστα, αντίγραφα ασφαλείας.

• προστασία του υλικού που είναι ευαίσθητο ή έχει υψηλή εμπορική αξία, από μη εξουσιοδοτημένα άτομα.

• περιορισμός της δυνατότητας παρέμβασης και αλλαγής του υλικού, με σφραγίδες ασφαλείας.

1.29 Ιχνηλασιμότητα (καταγραφή)

Στόχος είναι η εξασφάλιση της καταγραφής των ενεργειών που πραγματοποιούνται από τους χρήστες, κατά την επεξεργασία, ώστε να είναι δυνατή η παροχή στοιχείων, κατά τη διάρκεια ερευνών για τυχόν πειθαρχικά παραπτώματα. Τούτο εξασφαλίζεται ως εξής:

• δημιουργία ενός εφαρμόσιμου συστήματος καταγραφής το οποίο διατηρεί αρχείο των τροποποιήσεων των δεδομένων και της πρόσβασης σε αυτά που πραγματοποιούνται από τους χρήστες αλλά και του χρόνου που έλαβαν χώρα.

• ενημέρωση των χρηστών σχετικά με την δυνατότητα ιχνηλασιμότητας που έχει συσταθεί.

• διεξαγωγή περιοδικών αναλύσεων των καταγεγραμμένων πληροφοριών και παράλληλα η δημιουργία συστήματος που ανιχνεύει αυτόματα μη φυσιολογικές δραστηριότητες.

• διατήρηση αρχείων καταγραφής συμβάντων τουλάχιστον για έξι μήνες εκτός εάν οι νομικοί και κανονιστικοί περιορισμοί απαιτούν συγκεκριμένες διάρκειες αποθήκευσης.

Κατηγορία 2η.

2. Μεθοδολογία (Methodology)

Εξηγεί το πώς μπορεί να υλοποιηθεί η διαδικασία της "Εκτίμησης του Αντίκτυπου" (PIA), σύμφωνα με τα κριτήρια και τα πρότυπα για τη διαχείριση των κινδύνων που καθορίζει η εκάστοτε εποπτική αρχή και ο υπεύθυνος επεξεργασίας δεδομένων (DPO) [19]. Η μέθοδος θα πρέπει να εγγυάται την αιτιολογημένη και αξιόπιστη χρήση των προσωπικών δεδομένων, κατά την διάρκεια της επεξεργασίας τους,

με σκοπό αφενός να οικοδομήσει τη συμμόρφωση του φορέα με την εφαρμογή των αρχών προστασίας της ιδιωτικής ζωής και, αφετέρου, να αποδείξει ότι οι λύσεις που προτείνει δεν παραβιάζουν την ιδιωτική ζωή.

Κρίνεται ως βασικός άξονας, η υποχρέωση του φορέα που εμπλέκεται στη δημιουργία ή τη βελτίωση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα να περιλαμβάνει στον κανονισμό συμμόρφωσης:

• αρχές λήψης αποφάσεων και επικύρωσης κατά την επεξεργασία των προσωπικών δεδομένων

• κριτήρια αξιολόγησης των κινδύνων του συστήματος με ταυτόχρονο καθορισμό στόχων ασφάλειας.

προτάσεις για την αντιμετώπιση των κινδύνων, σύμφωνα με τους στόχους που προσδιορίζονται από τον εκάστοτε φορέα.

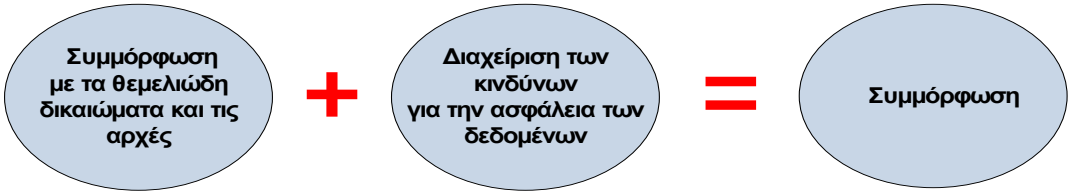
• υπεύθυνους προστασίας δεδομένων (ΥΠΔ) που θα υποστηρίζουν το έργο των αρχών, συνεισφέροντας στη λήψη αποφάσεων στον τομέα της προστασίας των προσωπικών δεδομένων.

• καταρτισμένο προσωπικό πληροφορικής (ΙΤ) επιφορτισμένο με την εφαρμογή, επίβλεψη και υποστήριξη πρωτοκόλλων ασφαλείας πληροφοριών.

Δύο πυλώνες στηρίζουν την προσέγγιση στη συμμόρφωση που εφαρμόζεται, κατά τη διαδικασία της δημιουργίας Εκτίμησης του Αντίκτυπου.

1ος Πυλώνας: θεμελιώδη δικαιώματα και αρχές το οποία είναι «αδιαπραγμάτευτα», θεσπίζονται με νόμο και πρέπει να τηρούνται ανεξάρτητα από τη φύση, τη σοβαρότητα και την πιθανότητα κινδύνων.

2ος Πυλώνας: διαχείριση των κινδύνων ιδιωτικής ζωής των υποκειμένων των δεδομένων, η οποία καθορίζει τους κατάλληλους τεχνικούς και οργανωτικούς ελέγχους για την προστασία των προσωπικών δεδομένων .



Εικόνα 3-2: Προσέγγιση συμμόρφωσης με PIA
Πηγή: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

Συνοψίζοντας, για την ολοκλήρωση της εκτέλεσης μιας PIA είναι απαραίτητο:

1. να καθορίζεται και να περιγράφεται το πλαίσιο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που εξετάζει.

2. να αναλύονται οι έλεγχοι που εγγυώνται τη συμμόρφωση με τις θεμελιώδεις αρχές όπως την αναλογικότητα και την αναγκαιότητα επεξεργασίας καθώς και την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα

3. να αξιολογούνται και να περιγράφονται επακριβώς οι κίνδυνοι που σχετίζονται με την ιδιωτική ζωή και που συνδέονται με την ασφάλεια των δεδομένων και να διασφαλίζεται ότι αυτοί αντιμετωπίζονται κατάλληλα.

4. να τεκμηριώνεται επισήμως η επικύρωση της Εκτίμησης του Αντίκτυπου (PIA), βάσει των προηγούμενων βημάτων ή να αποφασίζεται η αναθεώρησή τους.

Ουσιαστικά πρόκειται για μια διαδικασία συνεχούς βελτίωσης, κατά την οποία, συχνά, απαιτούνται αρκετές επαναλήψεις για να επιτευχθεί ένα αποδεκτό σύστημα προστασίας της ιδιωτικής ζωής. Κρίσιμος παράγοντας είναι και η παρακολούθηση των αλλαγών με την πάροδο του χρόνου σε τομείς όπως περιεχόμενα, ελέγχους, κινδύνους κ.λ.π.

Είναι αυτονόητο ότι κάθε προσέγγιση θα πρέπει να εφαρμόζεται μετά τον σχεδιασμό της νέας επεξεργασίας δεδομένων προσωπικού χαρακτήρα και να βασίζεται στους κανονισμούς της εκάστοτε Αρχής, με σκοπό να καθορίζονται έγκαιρα οι αναγκαίοι και επαρκείς έλεγχοι, με συνέπεια τη βελτιστοποίηση του κόστους. Σε διαφορετική περίπτωση, οι επιλογές που έχουν γίνει και αφορούν την εφαρμογή μπορεί να τεθούν υπό αμφισβήτηση, μετά τη δημιουργία του συστήματος και την εφαρμογή των ελέγχων.

2.1 Μελέτη του πλαισίου

Πραγματοποιείται από τον αρμόδιο φορέα, με τη βοήθεια ενός υπευθύνου σε θέματα "προστασίας των δεδομένων" (DPO, με σκοπό να αποκτήσει μια σαφή εικόνα των πράξεων επεξεργασίας δεδομένων προσωπικού χαρακτήρα που εξετάζονται. Συγκεκριμένα, η μελέτη θα πρέπει να περιλαμβάνει τα εξής στάδια:

Παρουσίαση μιας γενικής εικόνας

Δηλαδή τη παρουσίαση μιας σύντομης περιγραφής των εξεταζόμενων τομέων των προσωπικών δεδομένων, όπως της φύσης, του πεδίου εφαρμογής, του πλαισίου, των σκοπών της επεξεργασίας αλλά και

• τον προσδιορισμό του υπεύθυνου επεξεργασίας δεδομένων καθώς και κάθε μέσου επεξεργασίας αυτών**.**

• τη δημιουργία λίστας αναφορών που εφαρμόζονται κατά την επεξεργασία και είναι αναγκαίες ή πρέπει να τηρούνται, σύμφωνα με τον εγκεκριμένο κώδικα δεοντολογίας και τις πιστοποιήσεις που αφορούν την προστασία των δεδομένων.

Δεδομένα, διαδικασίες και υποστηρικτικά περιουσιακά στοιχεία

Καθορίστε και περιγράψτε λεπτομερώς τα πεδία που σχετίζονται με:

- τα προσωπικά δεδομένα, τους αποδέκτες τους και τη διάρκεια αποθήκευσής τους.

- τη περιγραφή των διαδικασιών και των δεδομένων προσωπικού χαρακτήρα που έχουν ενεργό ρόλο σε ολόκληρο τον κύκλο ζωής των προσωπικών δεδομένων από τη συλλογή έως τη διαγραφή.

2.2 Μελέτη των θεμελιωδών αρχών

Πραγματοποιείται από τον αρμόδιο φορέα και στη συνέχεια αξιολογείται από τον υπεύθυνο σε θέματα "προστασίας των δεδομένων" (DPO), με σκοπό την κατασκευή ενός συστήματος που εξασφαλίζει τη συμμόρφωση με τις αρχές της προστασίας της ιδιωτικής ζωής.

Συγκεκριμένα, η μελέτη των θεμελιωδών αρχών θα πρέπει να περιλαμβάνει τα εξής στάδια:

2.3 Αξιολόγηση των ελέγχων για τη διασφάλιση της αναλογικότητας και της αναγκαιότητας της επεξεργασίας

• Θα πρέπει να εξηγεί και να τεκμηριώνει τις επιλογές που έγιναν για τη συμμόρφωση με απαιτήσεις:

1. σκοποί: καθορισμένοι, σαφείς και νόμιμοι
2. βάση: νομιμότητα της επεξεργασίας και απαγόρευση της κατάχρησης
3. ελαχιστοποίηση των δεδομένων: κατάλληλα, συναφή με δυνατότητα να περιορίζονται
4. ποιότητα των δεδομένων: ακρίβεια των δεδομένων με συνεχή ενημέρωσή τους.
5. περίοδοι αποθήκευσης: οριοθετημένη

Επιπλέον θα πρέπει να διενεργούνται έλεγχοι για το εάν η βελτίωση του τρόπου με τον οποίο κάθε σημείο σχεδιάζεται, διευκρινίζεται και δικαιολογείται, είναι σύμφωνη με το [GDPR], ακόμα και εάν δεν είναι απαραίτητο ή δεν είναι δυνατό, με την προϋπόθεση πάντα πως ανάλογα με την περίπτωση, είναι δυνατή η επανεξέταση της περιγραφή τους ή η πρόταση πρόσθετων ελέγχων.

2.4 Αξιολόγηση των ελέγχων προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων

• Θα πρέπει να προσδιορίζει ή να καθορίζει και να περιγράφει, τους υφιστάμενους ή σχεδιαζόμενους ελέγχους που έχουν επιλεγεί, προς συμμόρφωση με τις ακόλουθες νομικές απαιτήσεις :

1. πληροφορίες για τα υποκείμενα των δεδομένων (δίκαιη και διαφανής επεξεργασία)
2. χορήγηση της συγκατάθεσης, ανάλογα με την περίπτωση
3. την άσκηση του δικαιώματος πρόσβασης και το δικαίωμα στη φορητότητα των δεδομένων
4. την άσκηση του δικαιώματος διόρθωσης και διαγραφής
5. την άσκηση του δικαιώματος περιορισμού της επεξεργασίας και το δικαίωμα αντίρρησης
6. ποιοι θα επεξεργάζονται τα δεδομένα: προσδιορίζονται και διέπονται από σύμβαση
7. μεταφορά δεδομένων: συμμόρφωση με τις υποχρεώσεις που αφορούν τη μεταβίβαση των δεδομένων εκτός της Ευρωπαϊκής Ένωσης.

Επιπλέον θα πρέπει να διενεργούνται έλεγχοι για το αν η βελτίωση κάθε ελέγχου και της περιγραφής του, είναι σύμφωνη με το [GDPR], ακόμα και αν δεν είναι απαραίτητο ή δεν είναι δυνατό, με τη προϋπόθεση πάντα πως ανάλογα με την περίπτωση, είναι δυνατή η επανεξέταση της περιγραφή του ή η πρόταση πρόσθετων ελέγχων.

2.5 Μελέτη των κινδύνων που σχετίζονται με την ασφάλεια των δεδομένων

Ένα υποθετικό σενάριο που περιγράφει το φόβο εκδήλωσης ενός συμβάντος αλλά και όλες τις απειλές που θα επιτρέψουν να συμβεί αυτό, αποτελεί τον ορισμό του κινδύνου της ιδιωτικότητας των δεδομένων. Πιο συγκεκριμένα, η μελέτη των κινδύνων περιλαμβάνει:

• τις πηγές κινδύνου (π.χ. ένας υπάλληλος δωροδοκείται ή είναι αμελής)

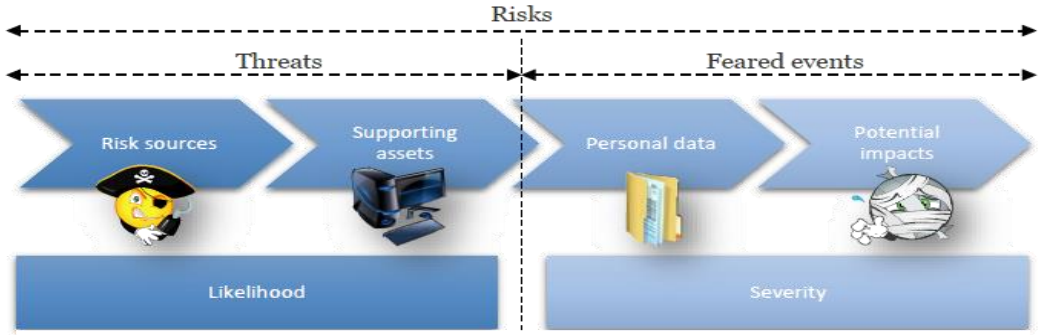
• τους τρόπους που μπορεί να εκμεταλλευτεί κάποιος, εάν εντοπίσει τα τρωτά σημεία του συστήματος διαχείρισης δεδομένων (π.χ.: το σύστημα διαχείρισης αρχείων που επιτρέπει το χειρισμό των δεδομένων)

• το πλαίσιο των απειλών (π.χ. κατάχρηση με την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου) και πως αυτά μπορούν να ευνοήσουν την εκδήλωση απειλών (π.χ. παράνομη πρόσβαση σε προσωπικά δεδομένα)

• το είδος των προσωπικών δεδομένων (π.χ. αρχείο του πελάτη)

• το αντίκτυπο των επιπτώσεων μιας παραβίασης και έκθεσης των προσωπικών δεδομένων στην προστασία της ιδιωτικής ζωής των υποκειμένων των δεδομένων (π.χ. ανεπιθύμητη δημοσιοποίηση στοιχείων, συναισθήματα εισβολής στην ιδιωτική ζωή, προσωπικά ή επαγγελματικά προβλήματα).

Το ακόλουθο διάγραμμα συνοψίζει όλες τις ανωτέρω έννοιες με σαφήνεια:



Εικόνα 3-3: Κίνδυνοι που σχετίζονται με την ασφάλεια των δεδομένων
Πηγή:https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

Το επίπεδο κινδύνου εκτιμάται από την άποψη της σοβαρότητας και της πιθανότητας εκδήλωσής του. Αναλυτικότερα η **δριμύτητα (Severity)** αντιπροσωπεύει το μέγεθος του κινδύνου και εξαρτάται κυρίως από τον προκατειλημμένο χαρακτήρα (επιζημιότητα) των πιθανών επιπτώσεων που θα προκαλέσει, ενώ η **πιθανότητα (Likelihood)** εκφράζει την πιθανότητα να λάβει χώρα ένα επικίνδυνο συμβάν και εξαρτάται κυρίως από το επίπεδο ευπάθειας των υποστηρικτικών μέσων (Hardware), όταν αυτά απειλούνται, αλλά και από το επίπεδο των ικανοτήτων των πηγών κινδύνου.

Συγκεκριμένα η μελέτη των κινδύνων που σχετίζονται με την ασφάλεια των δεδομένων θα πρέπει να περιλαμβάνει τα εξής στάδια:

2.6 Αξιολόγηση των υφιστάμενων ή σχεδιαζόμενων ελέγχων

Πραγματοποιείται από τον αρμόδιο φορέα και στη συνέχεια αξιολογείται από τον υπεύθυνο σε θέματα «προστασίας των δεδομένων» (DPO), με σκοπό να γίνει σαφής η ουσιαστική κατανόηση των ελέγχων που συμβάλλουν στην ασφάλεια των δεδομένων. Συγκεκριμένα η αξιολόγηση θα πρέπει να περιλαμβάνει τα εξής στάδια:

Προσδιορισμός ή καθορισμός των υφιστάμενων ή προγραμματισμένων ελέγχων (που έχουν ήδη αναληφθεί), οι οποίοι διακρίνονται σε:

1. ελέγχους που αφορούν συγκεκριμένα δεδομένα που υποβάλλονται σε επεξεργασία, όπως κρυπτογράφηση, ανωνυμία, διαμέριση, έλεγχο πρόσβασης, ανιχνευσιμότητα.

2. γενικούς ελέγχους ασφαλείας σχετικά με το σύστημα στο οποίο πραγματοποιείται η επεξεργασία: ασφάλεια λειτουργίας, δημιουργία αντιγράφων ασφαλείας, ασφάλεια του υλικού.

3. οργανωτικοί έλεγχοι (διακυβέρνηση): πολιτική, διαχείριση έργου, προσωπικό διαχείρισης, διαχείριση συμβάντων και παραβάσεων, σχέσεις με τρίτους.

Επιπλέον θα πρέπει να πιστοποιείται η βελτίωση κάθε ελέγχου που εφαρμόζεται και της αντίστοιχης περιγραφής του, σύμφωνα με τις βέλτιστες πρακτικές ασφαλείας, ακόμα και αν αυτό δεν είναι απαραίτητο ή δεν είναι δυνατό και ανάλογα με την περίπτωση, να επανεξετάζεται η περιγραφή τους ή να προτείνονται πρόσθετοι έλεγχοι.

2.7 Η αξιολόγηση του κινδύνου: πιθανές παραβιάσεις της ιδιωτικής ζωής

Πραγματοποιείται από τον αρμόδιο φορέα και στη συνέχεια αξιολογείται από τον υπεύθυνο σε θέματα «προστασίας των δεδομένων» (DPO), με σκοπό να αποτυπωθεί μια πλήρης εικόνα των αιτίων και των συνεπειών των κινδύνων.

Συγκεκριμένα για κάθε πιθανή εκδήλωση απειλής (παράνομη πρόσβαση σε προσωπικά δεδομένα, ανεπιθύμητη αλλαγή των προσωπικών δεδομένων και εξαφάνιση των προσωπικών δεδομένων), η αξιολόγηση θα πρέπει να περιλαμβάνει τα εξής στάδια :

1. προσδιορισμός των ενδεχόμενων επιπτώσεων (potential impacts), στην προστασία της ιδιωτικής ζωής των υποκειμένων των δεδομένων, εάν αυτό συμβεί.

2. εκτίμηση της σοβαρότητας (severity), ανάλογα με τον επιζήμιο χαρακτήρα των δυνητικών επιπτώσεων. (ανάλογα με την περίπτωση, οι έλεγχοι θα μπορούσαν να τις τροποποιήσουν)

3. προσδιορισμός των απειλών (threats), σχετικά με προσωπικά δεδομένα που αναφέρονται σε περιουσιακά στοιχεία.

4. εκτίμηση της πιθανότητας (likelihood), ιδιαίτερα όταν αυτή εξαρτάται από το επίπεδο ευπάθειας των δεδομένων προσωπικού χαρακτήρα, τα οποία υποστηρίζουν τα περιουσιακά στοιχεία, το επίπεδο των ικανοτήτων των πηγών κινδύνου για αυτά και τους ελέγχους που ενδέχεται να τροποποιηθούν.

Επιπλέον θα πρέπει να καθοριστεί εάν οι κίνδυνοι που εντοπίζονται με αυτόν τον τρόπο μπορούν να θεωρηθούν αποδεκτοί, σύμφωνα με τους υφιστάμενους ή

σχεδιαζόμενους ελέγχους. Σε διαφορετική περίπτωση θα πρέπει, να προταθούν πρόσθετοι έλεγχοι και εκ νέου αξιολόγηση του επιπέδου του καθενός από τους κινδύνους, έτσι ώστε να προσδιοριστούν οι εναπομείναντες κίνδυνοι.

2.8 Επικύρωση της PIA

Πραγματοποιείται από τον υπεύθυνο σε θέματα «προστασίας των δεδομένων» (DPO) σε συνεργασία με τον αρμόδιο φορέα ο οποίος αποφασίζει εάν πρέπει ή όχι να δεχθεί το πόρισμα της μελέτης εκτίμησης του αντίκτυπου των προσωπικών δεδομένων, σύμφωνα με τον εκάστοτε ισχύοντα κώδικα δεοντολογίας και στη συνέχεια να προβεί στην τελική επικύρωσή του.

Προετοιμασία του υλικού που απαιτείται για την επικύρωση

Συγκεκριμένα αφού συγκεντρωθούν και οριστικοποιηθούν τα ευρήματα της μελέτης θα πρέπει:

1. να προετοιμαστεί μια οπτική παρουσίαση των ελέγχων που επιλέγονται προκειμένου να εξασφαλιστεί η συμμόρφωση με τις θεμελιώδεις αρχές, ανάλογα με τη συμμόρφωσή τους με το GDPR.

2. να προετοιμαστεί μια οπτική παρουσίαση των ελέγχων που επιλέγονται για να συμβάλουν στην ασφάλεια των δεδομένων, ανάλογα με τη συμμόρφωσή τους με τις βέλτιστες πρακτικές ασφαλείας.

3. να παρουσιαστεί μια οπτική χαρτογράφηση των κινδύνων ανάλογα με τη σοβαρότητα και τη πιθανότητα τους.

4. να καταρτιστεί ένα σχέδιο δράσης με βάση τους πρόσθετους ελέγχους που εντοπίστηκαν κατά τα προηγούμενα βήματα. Για κάθε έλεγχο, θα πρέπει να καθοριστεί τουλάχιστον ένα άτομο υπεύθυνο για την υλοποίηση της εφαρμογής, την εκτίμηση του κόστους τόσο σε οικονομικό επίπεδο όσο και σε επίπεδο φόρτου εργασίας, αλλά και την εκτίμηση του προβλεπόμενου χρονικού πλαισίου.

Επιπλέον θα πρέπει να τεκμηριώνει την εξέταση των ενδιαφερομένων, όπως τις συμβουλές του υπευθύνου των πτυχών «Προστασία Δεδομένων» DPO και τις απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους.

2.9 Η επίσημη επικύρωση

Αυτό που απομένει πλέον είναι η λήψη απόφασης σχετικά με το αν οι επιλεγμένοι έλεγχοι, οι υπολειπόμενοι κίνδυνοι και το σχέδιο δράσης είναι τεκμηριωμένα αποδεκτά, υπό το πρίσμα του ισχύοντα κώδικα δεοντολογίας και των

απόψεων των ενδιαφερομένων μερών. Έτσι με τον τρόπο αυτό, η μελέτη εκτίμησης αντίκτυπου προσωπικών δεδομένων (PIA) μπορεί να είναι:

1. Επικυρωμένη
2. Εξαρτώμενη από βελτίωση
3. Απορριπτόμενη (μαζί με την υπό εξέταση επεξεργασία).

Κατηγορία 3η

3. Πρότυπα (Templates)

Βασικός παράγοντας για μια εμπεριστατωμένη και πλήρως εναρμονισμένη Μελέτη Εκτίμησης Αντίκτυπου προσωπικών δεδομένων, είναι η εφαρμογή των ακόλουθων προτεινόμενων προτύπων, τα οποία είναι εφικτό και μάλιστα επιθυμητό να προσαρμόζονται ανάλογα, σε κάθε συγκεκριμένο πλαίσιο, ώστε να συμπληρώνουν τη χρήση της απαιτούμενης μεθοδολογίας [20]. Συγκεκριμένα η δομή των προτύπων περιλαμβάνει τα εξής στάδια:

3.1 Μελέτη του πλαισίου: πρότυπα

3.1.1 Επισκόπηση της επεξεργασίας

Περιγραφή της υπό εξέταση επεξεργασίας η οποία περιλαμβάνει :

- ✓ Προϋποθέσεις Επεξεργασίας
- ✓ Σκοπούς Επεξεργασίας
- ✓ Ελεγκτές – Διαχειριστές
- ✓ Υπεύθυνους Επεξεργασίας Δεδομένων

Ειδικά πρότυπα τομέων που εφαρμόζονται στην επεξεργασία όπως :

- ✓ Ισχύοντα πρότυπα επεξεργασίας
- ✓ Θεώρηση

3.1.2 Δεδομένα, διαδικασίες και υποστηρικτικά στοιχεία

Περιγραφή των δεδομένων, των αποδεκτών και διάρκεια αποθήκευσης η οποία περιλαμβάνει :

- ✓ Τύπους δεδομένων
- ✓ Παραλήπτες

- ✓ Διάρκεια αποθήκευσης

Περιγραφή των διαδικασιών και της υποστήριξης των περιουσιακών στοιχείων η οποία περιλαμβάνει :

- ✓ Διεργασίες
- ✓ Λεπτομερής περιγραφή της διαδικασίας
- ✓ Υποστηρικτικά στοιχεία δεδομένων

3.2 Μελέτη των θεμελιωδών αρχών: τα πρότυπα

3.2.1 Αξιολόγηση των ελέγχων για τη διασφάλιση της αναλογικότητας και της αναγκαιότητας της επεξεργασίας

Εξήγηση και αιτιολόγηση των σκοπών η οποία περιλαμβάνει :

- ✓ Σκοπούς
- ✓ Νομιμότητα

Εξήγηση και αιτιολόγηση της νομιμότητας η οποία περιλαμβάνει:

- ✓ Κριτήρια νομιμότητας όπως:
  - ➢ Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους ειδικούς σκοπούς.
  - ➢ Η επεξεργασία κρίνεται απαραίτητη για την εκτέλεση μιας σύμβασης στην οποία συμμετέχει το πρόσωπο, στο οποίο αναφέρονται τα δεδομένα ή για τη λήψη μέτρων κατόπιν αιτήματος του υποκειμένου των δεδομένων πριν από τη σύναψη μιας σύμβασης
  - ➢ Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με μια νομική υποχρέωση.
  - ➢ Η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου
  - ➢ Η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που εκτελείται προς δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας (DPO).

- Η επεξεργασία είναι αναγκαία για τους σκοπούς των νόμιμων συμφερόντων που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, εκτός εάν τα συμφέροντα ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του προσώπου στο οποίο αναφέρονται τα δεδομένα, απαιτούν προστασία δεδομένων προσωπικού χαρακτήρα, ιδίως όταν τα δεδομένα αφορούν παιδί.

✓ Εφαρμοσιμότητα

✓ Τεκμηρίωση

Εξήγηση και αιτιολόγηση της ελαχιστοποίησης των δεδομένων η οποία περιλαμβάνει:

✓ Λεπτομέρειες σχετικά με τα επεξεργασμένα δεδομένα

✓ Κατηγορίες δεδομένων

✓ Αιτιολόγηση της ανάγκης και της συνάφειας των δεδομένων

✓ Ελαχιστοποίηση των ελέγχων

Εξήγηση και αιτιολόγηση της ποιότητας των δεδομένων η οποία περιλαμβάνει:

✓ Έλεγχοι ποιότητας δεδομένων

✓ Τεκμηρίωση

Επεξήγηση και αιτιολόγηση της διάρκειας αποθήκευσης η οποία περιλαμβάνει:

✓ Τύπους δεδομένων όπως:

- Κοινά δεδομένα
- Αρχειοθετημένα δεδομένα
- Λειτουργικά ίχνη
- Τεχνικά αρχεία καταγραφής

✓ Διάρκεια αποθήκευσης

✓ Τεκμηρίωση της διάρκειας αποθήκευσης

✓ Μηχανισμός διαγραφής στο τέλος της προβλεπόμενης διάρκειας αποθήκευσης.

Αξιολόγηση των ελέγχων η οποία περιλαμβάνει:

✓ Ελέγχους που εγγυώνται την αναλογικότητα και την αναγκαιότητα της επεξεργασίας όπως :

- καθορισμένοι, σαφείς και νόμιμοι σκοποί
- νομιμότητα της επεξεργασίας και απαγόρευση της κατάχρησης βάσει του ισχύοντα κώδικα δεοντολογίας
- επαρκής, σχετική και περιορισμένη ελαχιστοποίηση δεδομένων
- ακριβής και ενημερωμένη ποιότητα δεδομένων
- περιορισμένη διάρκεια αποθήκευσης

✓ Αποδεκτοί / βελτιούμενοι

✓ Διορθωτικοί έλεγχοι

3.2.2 Αξιολόγηση των ελέγχων προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων

Προσδιορισμός και περιγραφή των ελέγχων για την ενημέρωση των υποκειμένων των δεδομένων, ο οποίος περιλαμβάνει:

✓ Απαλλαγή από την υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων

✓ Τεκμηρίωση

Σε περίπτωση που η επεξεργασία επωφελείται από την απαλλαγή από το δικαίωμα πληροφόρησης.

Διαφορετικά :

✓ Έλεγχοι για το δικαίωμα στην πληροφόρηση όπως:

- Παρουσίαση των όρων χρήσης και εμπιστευτικότητας
- Δυνατότητα πρόσβασης στους όρους χρήσης και εμπιστευτικότητας.
- Ευανάγνωστους και κατανοητούς όρους
- Λεπτομερής παρουσίαση των σκοπών επεξεργασίας δεδομένων, όπως συγκεκριμένοι στόχοι, αντιστοίχιση δεδομένων.
- Λεπτομερής παρουσίαση των συλλεγόμενων δεδομένων προσωπικού χαρακτήρα.
- Παρουσίαση των δικαιωμάτων του χρήστη, όπως απόσυρση συγκατάθεσης, διαγραφή δεδομένων.
- Πληροφορίες σχετικά με τη μέθοδο ασφαλούς αποθήκευσης δεδομένων.
- Ρυθμίσεις επικοινωνίας με τρίτους, όπως στοιχεία ταυτότητας και στοιχεία επικοινωνίας, σχετικά με θέματα εμπιστευτικότητας.

- Πληροφορίες για τον χρήστη σχετικά με οποιαδήποτε αλλαγή αφορά τα δεδομένα που συλλέγονται, τους σκοπούς και τις ρήτρες εμπιστευτικότητας
- Όσον αφορά τη διαβίβαση δεδομένων σε τρίτους:

▪ λεπτομερής παρουσίαση των σκοπών της μετάδοσης δεδομένων σε τρίτους

▪ λεπτομερής παρουσίαση των διαβιβαζόμενων προσωπικών δεδομένων και

▪ ένδειξη της ταυτότητας τρίτων φορέων

- ✓ Εκτέλεση.
- ✓ Τεκμηρίωση εκτέλεσης ή μη εκτέλεσης της εφαρμογής.

Προσδιορισμός και περιγραφή των ελέγχων για τη λήψη συγκατάθεσης ο οποίος περιλαμβάνει:

- ✓ Έλεγχοι για τη λήψη συγκατάθεσης όπως:
  - Πρόθεση συγκατάθεσης κατά την εγγραφή
  - Η συγκατάθεση κατανέμεται ανά κατηγορία δεδομένων ή τύπο επεξεργασίας.
  - Πρόθεση συγκατάθεσης πριν από την κοινή χρήση δεδομένων με άλλους χρήστες.
  - Η συγκατάθεση παρουσιάζεται σε κατανοητή και εύκολα προσπελάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα προσαρμοσμένη στον χρήστη και ιδίως αν αφορά παιδιά.
  - Παροχή συγκατάθεσης των γονέων για ανηλίκους κάτω των 13 ετών.
  - Για ένα νέο χρήστη πρέπει να ληφθεί εκ νέου η συναίνεση του.
  - Μετά από μακρά περίοδο χωρίς χρήση, πρέπει να ζητείται εκ νέου επιβεβαίωση της συγκατάθεσης.
  - Όπου υπάρχει συναίνεση για επεξεργασία ειδικών δεδομένων, αυτό να δηλώνεται σαφώς ότι λαμβάνει χώρα, με χαρακτηριστική οπτική ή ακουστική σήμανση.
- ✓ Εκτέλεση.
- ✓ Τεκμηρίωση εκτέλεσης της εφαρμογής ή μη εκτέλεσης της.

Προσδιορισμός και περιγραφή των ελέγχων για τα δικαιώματα πρόσβασης και φορητότητα των δεδομένων ο οποίος περιλαμβάνει:

Όταν η επεξεργασία των δεδομένων επωφελείται από απαλλαγή από το δικαίωμα πρόσβασης,

- ✓ Εξαίρεση από το δικαίωμα πρόσβασης.
- ✓ Τεκμηρίωση.
- ✓ Ρυθμίσεις για την ανταπόκριση στα πρόσωπα στα οποία αναφέρονται τα δεδομένα.

Διαφορετικά:

- ✓ Έλεγχοι για το δικαίωμα πρόσβασης όπως:
  - ➢ Δυνατότητα πρόσβασης σε όλα τα προσωπικά δεδομένα του χρήστη μέσω των κοινών διεπαφών.
  - ➢ Δυνατότητα ασφαλούς διαβούλευσης με τα ίχνη χρήσης που σχετίζονται με το χρήστη.
  - ➢ Δυνατότητα λήψης αρχείου όλων των προσωπικών δεδομένων που σχετίζονται με το χρήστη.
- ✓ Εσωτερικά δεδομένα.
- ✓ Εξωτερικά δεδομένα.
- ✓ Τεκμηρίωση.

Σε περίπτωση που το δικαίωμα μεταφοράς δεδομένων εφαρμόζεται κατά την επεξεργασία:

- ✓ Έλεγχοι για το δικαίωμα μεταφοράς δεδομένων όπως:
  - ➢ Δυνατότητα ανάκτησης των προσωπικών δεδομένων, σε επαναχρησιμοποιήσιμη εύκολη μορφή, έτσι ώστε να μεταφέρονται σε άλλη υπηρεσία.
- ✓ Εσωτερικά δεδομένα.
- ✓ Εξωτερικά δεδομένα.
- ✓ Τεκμηρίωση.

Προσδιορισμός και περιγραφή των ελέγχων για τα δικαιώματα διόρθωσης και διαγραφής ο οποίος περιλαμβάνει:

Όταν η επεξεργασία των δεδομένων, επωφελείται από εξαίρεση του δικαιώματος διόρθωσης και διαγραφής.

- ✓ Εξαίρεση από τα δικαιώματα διόρθωσης και διαγραφής.
- ✓ Αιτιολόγηση.
- ✓ Ρυθμίσεις για την ανταπόκριση των προσώπων, στα οποία αναφέρονται τα δεδομένα.

Διαφορετικά:

- ✓ Έλεγχοι για τα δικαιώματα διόρθωσης και διαγραφής όπως:
  - ➢ Δυνατότητα διόρθωσης προσωπικών δεδομένων.
  - ➢ Δυνατότητα διαγραφής προσωπικών δεδομένων.
  - ➢ Αναγραφή των προσωπικών δεδομένων που θα αποθηκευθούν, όπως τεχνικές απαιτήσεις, νομικές υποχρεώσεις.
  - ➢ Εφαρμογή του δικαιώματος της λήθης για ανηλίκους.
  - ➢ Εφαρμογή απλών βημάτων για τη διαγραφή δεδομένων πριν από τη καταστροφή μιας συσκευής.
  - ➢ Δυνατότητα διαγραφής δεδομένων σε περίπτωση κλοπής της συσκευής.
- ✓ Εσωτερικά δεδομένα.
- ✓ Εξωτερικά δεδομένα.
- ✓ Τεκμηρίωση.

Προσδιορισμός και περιγραφή των ελέγχων για τα δικαιώματα περιορισμού της επεξεργασίας και άσκησης ένστασης οποίος περιλαμβάνει:

Όταν η επεξεργασία των δεδομένων, επωφελείται από απαλλαγή από το δικαίωμα περιορισμού και άσκησης αντίρρησης.

- ✓ Απαλλαγή από τα δικαιώματα περιορισμού και αντίρρησης.
- ✓ Αιτιολόγηση.
- ✓ Ρυθμίσεις για την ανταπόκριση από τα πρόσωπα στα οποία αναφέρονται τα δεδομένα.

Διαφορετικά :

- ✓ Έλεγχοι για τα δικαιώματα περιορισμού και διατύπωσης αντιρρήσεων όπως:
  - ➢ Ενεργοποίηση της επιλογής "Απόρρητο".
  - ➢ Αλλαγή των προεπιλεγμένων ρυθμίσεων.

- Η επιλογή "Απόρρητο" να είναι διαθέσιμη κατά την επεξεργασία.
- Η επιλογή "Απόρρητο" να είναι διαθέσιμη μετά την επεξεργασία.
- Ύπαρξη συστήματος γονικού ελέγχου για παιδιά κάτω των 13 ετών.
- Συμμόρφωση όσον αφορά την παρακολούθηση, όπως cookies.
- Αποκλεισμός παιδιών ηλικίας κάτω των 13 ετών μέσω αυτοματοποιημένου προφίλ.
- Αποτελεσματικός αποκλεισμός της επεξεργασίας των δεδομένων του χρήστη όταν η συγκατάθεσή του αποσύρεται.

✓ Εσωτερικά δεδομένα.
✓ Εξωτερικά δεδομένα.
✓ Αιτιολόγηση.

Προσδιορισμός και περιγραφή των ελέγχων που επιβάλλονται στους υπαλλήλους που επεξεργάζονται τα δεδομένα ο οποίος περιλαμβάνει:

✓ Ονοματεπώνυμο υπαλλήλου που εκτελεί την επεξεργασία
✓ Σκοπός
✓ Πεδίο εφαρμογής
✓ Αναφορά του αντικειμένου που σχετίζεται η επεξεργασία των δεδομένων
✓ Συμμόρφωση με το άρθρο 28

Προσδιορισμός και περιγραφή των ελέγχων για τη μεταφορά των δεδομένων εκτός της Ευρωπαϊκής Ένωσης ο οποίος περιλαμβάνει:

✓ Τα σύνολα δεδομένων και η θέση αποθήκευσης τους
✓ Η χώρα αναγνωρίζει ότι παρέχει επαρκή προστασία από την ΕΕ
✓ Χώρα προορισμού
✓ Αιτιολόγηση και εποπτεία, όπως τυποποιημένες συμβατικές ρήτρες και εσωτερικοί εταιρικοί κανονισμοί

Αξιολόγηση των ελέγχων η οποία περιλαμβάνει:

✓ Έλεγχοι για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα όπως :
  - Πληροφορίες για τα υποκείμενα των δεδομένων, όπως δίκαιη και διαφανής επεξεργασία.
  - Λήψη συγκατάθεσης.

- Εφαρμογή των δικαιωμάτων πρόσβασης και μεταφοράς δεδομένων.
- Εφαρμογή των δικαιωμάτων διόρθωσης και διαγραφής.
- Εφαρμογή των δικαιωμάτων περιορισμού της επεξεργασίας και αντίκρουσης.
- Υπάλληλοι που επεξεργάζονται τα δεδομένα, οι οποίοι προσδιορίζονται και διέπονται από τον εκάστοτε κώδικα δεοντολογίας.
- Μεταφορά των δεδομένων, η οποία συμμορφώνεται με τις υποχρεώσεις που αφορούν τη διαβίβαση δεδομένων εκτός της Ευρωπαϊκής Ένωσης.

✓ Αποδεκτοί / βελτιούμενοι.

✓ Διορθωτικοί έλεγχοι.

3.3 Μελέτη κινδύνων ασφάλειας δεδομένων: πρότυπα

3.3.1 Αξιολόγηση των ελέγχων ασφαλείας

Περιγραφή και αξιολόγηση των ελέγχων που εφαρμόζονται για την αντιμετώπιση των κινδύνων που σχετίζονται με την ασφάλεια των δεδομένων και περιλαμβάνουν :

✓ Έλεγχοι που αφορούν ειδικά τα δεδομένα που επεξεργάζονται όπως:
- Κρυπτογράφηση.
- Ανωνυμοποίηση.
- Κατανομή δεδομένων, σε σχέση με το υπόλοιπο σύστημα πληροφοριών.
- Έλεγχος λογικής πρόσβασης.
- Ιχνηλασιμότητα.
- Παρακολούθηση ακεραιότητας.
- Αρχειοθέτηση.
- Πολιτικές Ασφάλειας εγγράφου.

✓ Εφαρμογή και τεκμηρίωση της διασφάλισης όπως:
- Περιγραφή των μέσων που εφαρμόζονται για τη διασφάλιση της εμπιστευτικότητας των αποθηκευμένων δεδομένων, στη βάση δεδομένων ή στους servers, καθώς και της διαδικασίας διαχείρισης των κλειδιών κρυπτογράφησης όπως δημιουργία, αποθήκευση, αλλαγή σε περίπτωση ύποπτων περιπτώσεων.

- Αναφορά εφαρμογής των μηχανισμών ανωνυμοποίησης, ποιοί και για ποιο σκοπό.
- Υπόδειξη προγραμματισμού ξεχωριστής επεξεργασίας δεδομένων, αν απαιτηθεί και πώς γίνεται.
- Καθορισμός των μέσων ελέγχου ταυτότητας που εφαρμόζονται.
- Κατά περίπτωση, καθορισμός των κανόνων που ισχύουν για τους κωδικούς πρόσβασης, όπως ελάχιστο μήκος, απαιτούμενοι χαρακτήρες, διάρκεια ισχύος, αριθμός αποτυχημένων προσπαθειών πριν από την πρόσβαση στον λογαριασμό.
- Υπόδειξη καταγραφής συμβάντων και πόσο καιρό τα ίχνη τους είναι αποθηκευμένα.
- Υπόδειξη εφαρμογής μηχανισμών παρακολούθησης της ακεραιότητας των αποθηκευμένων δεδομένων, ποιοί και για ποιο σκοπό.
- Καθορισμός μηχανισμών ελέγχου ακεραιότητας που εφαρμόζονται στις ροές δεδομένων.
- Περιγραφή διαδικασιών διαχείρισης αρχείων, όπως παράδοση, αποθήκευση και καθορισμός ρόλων και πολιτικής αρχειοθέτησης.
- Υπόδειξη τρόπου εκτύπωσης, αποθήκευσης, καταστροφής και ανταλλαγής, κατά τη χρήση εγγράφων χαρτιού που περιέχουν δεδομένα.

✓ Αποδεκτοί / βελτιούμενοι.

✓ Διορθωτικοί έλεγχοι.

Περιγραφή και αξιολόγηση των γενικών ελέγχων ασφαλείας οι οποίοι περιλαμβάνουν :

✓ Γενικοί έλεγχοι ασφαλείας σχετικά με το σύστημα, στο οποίο πραγματοποιείται η επεξεργασία όπως:

- Λειτουργική ασφάλεια.
- Περιορισμός κακόβουλου λογισμικού.
- Διαχείριση σταθμών εργασίας.
- Ασφάλεια ιστότοπου.
- Δημιουργία αντιγράφων ασφαλείας.
- Συντήρηση.
- Ασφάλεια καναλιών υπολογιστών (δίκτυα).

- Παρακολούθηση.
- Έλεγχος φυσικής πρόσβασης.
- Ασφάλεια υλικού.
- Αποφυγή πηγών κινδύνου.
- Προστασία από μη ανθρώπινες πηγές κινδύνων.

✓ Εφαρμογή και τεκμηρίωση των γενικών ελέγχων ασφαλείας όπως:

- Περιγραφή της πραγματοποίησης των ενημερώσεων του λογισμικού και της εφαρμογής διορθωτικών ελέγχων ασφάλειας.
- Εγκατάσταση και ενημέρωση, σε τακτά χρονικά διαστήματα στους σταθμούς εργασίας, λογισμικού προστασίας από ιούς.
- Λειτουργία λογισμικού τείχους προστασίας (firewall) και αυτόματου κλειδώματος σε σταθμούς εργασίας.
- Υπόδειξη του τρόπου διαχείρισης των αντιγράφων ασφαλείας.
- Περιγραφή της φυσικής συντήρησης του υλικού.
- Περιγραφή του είδους δικτύου στο οποίο πραγματοποιείται η επεξεργασία και καθορισμός των συστημάτων τείχους προστασίας, ανίχνευσης εισβολών ή άλλων ενεργών μέτρων υπεύθυνων για την εξασφάλιση της ασφάλειας του δικτύου.
- Υπόδειξη των μέσων με τα οποία υλοποιείται παρακολούθηση σε πραγματικό χρόνο του τοπικού δικτύου και των διαμορφώσεων υλικού και λογισμικού.
- Αναφορά του τρόπου διεξαγωγής του φυσικού ελέγχου πρόσβασης, σχετικά με τις εγκαταστάσεις που εξυπηρετούν την επεξεργασία δεδομένων.
- Αναφορά της θέσης της περιοχής και το αν είναι εκτεθειμένη σε περιβαλλοντικές καταστροφές.
- Περιγραφή των μέσων πρόληψης πυρκαγιάς, ανίχνευσης και κατάσβεσης, αποφυγής πλημμυρών και διασφάλισης της ηλεκτρικής παροχής στους σταθμούς εργασίας και στους servers.

✓ Αποδεκτοί / βελτιούμενοι

✓ Διορθωτικοί έλεγχοι

Περιγραφή και αξιολόγηση των οργανωτικών ελέγχων οι οποίοι περιλαμβάνουν:

✓ Έλεγχοι όπως:

- Οργάνωση.
- Πολιτική (διαχείριση κανόνων).
- Διαχείριση κινδύνου.
- Διαχείριση έργου.
- Διαχείριση περιστατικών παραβιάσεων δεδομένων.
- Διαχείριση προσωπικού.
- Σχέσεις με τρίτους.
- Εποπτεία.

✓ Εφαρμογή και τεκμηρίωση των οργανωτικών ελέγχων όπως:

- Ορισμός και ανάθεση ρόλων και ευθυνών για την προστασία δεδομένων και καθορισμός ενός προσώπου, υπεύθυνου για την εφαρμογή των νόμων και των κανονισμών περί απορρήτου.
- Αναφορά της αξιολόγησης των κινδύνων, για την προστασία της ιδιωτικής ζωής που προκύπτουν από νέες θεραπείες στα πρόσωπα στα οποία αναφέρονται τα δεδομένα, ανεξαρτήτως από το αν είναι συστηματικοί ή σύμφωνοι με ποια μέθοδο.
- Υπόδειξη ότι οι δοκιμές επεξεργασίας δεδομένων στους σταθμούς εργασίας, εκτελούνται σε μη πραγματικά ή ανώνυμα δεδομένα.
- Αναφορά τεκμηριωμένων και δοκιμασμένων διαδικασιών διαχείρισης δεδομένων.
- Αναφορά ενεργειών και ελέγχων που πραγματοποιούνται, στην περίπτωση που κάποιος υπάλληλος που έχει πρόσβαση στην επεξεργασία των δεδομένων, λύσει την υπαλληλική του σχέση με τον εκάστοτε φορέα.
- Υπόδειξη των ελέγχων ασφαλείας και των ρυθμίσεων που πραγματοποιούνται, κάθε φορά που τρίτα μέρη απαιτούν πρόσβαση στα δεδομένα.
- Αναφορά παρακολούθησης της αποτελεσματικότητας και επάρκειας των ελέγχων απορρήτου.

✓ Αποδεκτοί / βελτιούμενοι.

✓ Διορθωτικοί έλεγχοι.

3.3.2 Η αξιολόγηση του κινδύνου: πιθανές παραβιάσεις της ιδιωτικής ζωής

Ανάλυση και αξιολόγηση των κινδύνων η οποία περιλαμβάνει :

✓ Κινδύνους όπως :

- Αθέμιτη πρόσβαση στα δεδομένα.
- Ανεπιθύμητη αλλαγή των δεδομένων.
- Εξαφάνιση των δεδομένων.

✓ Πηγές κινδύνου.

✓ Απειλές.

✓ Πιθανές επιπτώσεις.

✓ Εφαρμογή ελέγχων για τη μείωση της σοβαρότητας και της πιθανότητας.

✓ Δριμύτητα.

✓ Πιθανότητα.

Αξιολόγηση των κινδύνων η οποία περιλαμβάνει :

✓ Κινδύνους όπως:

- Αθέμιτη πρόσβαση στα δεδομένα.
- Ανεπιθύμητη αλλαγή των δεδομένων.
- Εξαφάνιση των δεδομένων.

✓ Αποδεκτοί / βελτιούμενοι όπως:

- Ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να καθορίσει εάν οι υπάρχοντες ή προγραμματισμένοι έλεγχοι, που έχουν ήδη τεθεί σε εφαρμογή, περιορίζουν επαρκώς αυτούς τους κινδύνους, ώστε να καταστούν αποδεκτοί.

✓ Διορθωτικοί έλεγχοι όπως :

- Στην περίπτωση που υπάρχουν σοβαροί λόγοι, ο DPO πρέπει να αναφέρει τυχόν πρόσθετους ελέγχους που θα αποδειχθούν αναγκαίοι.

✓ Υπολειπόμενη σοβαρότητα

✓ Υπολειμματική πιθανότητα

3.4 Επικύρωση της PIA: πρότυπα

3.4.1 Παρασκευή του υλικού που απαιτείται για την επικύρωση

Αφορά την εκπόνηση της σύνθεσης, σχετικά με τη συμμόρφωση με τους κανόνες ελέγχου GDPR, που επιλέχθηκαν για τη διασφάλιση της συμμόρφωσης με τις θεμελιώδεις αρχές η οποία περιλαμβάνει:

✓ Έλεγχοι που έχουν επιλεγεί για να εξασφαλιστεί η συμμόρφωση με τις θεμελιώδεις αρχές οι οποίοι χωρίζονται σε:

- **Έλεγχοι που εγγυώνται την αναλογικότητα και την αναγκαιότητα της επεξεργασίας όπως** :
    - Σκοπός (-οι): καθορισμένος, ρητός και νόμιμος.
    - Βάση: νομιμότητα της επεξεργασίας, απαγόρευση της κατάχρησης.
    - Ελαχιστοποίηση δεδομένων: επαρκής, σχετική και περιορισμένη.
    - Ποιότητα δεδομένων: ακριβής και ενημερωμένη.
    - Διάρκεια αποθήκευσης: περιορισμένη.

- **Έλεγχοι για την προστασία των προσωπικών δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα όπως:**
    - Πληροφορίες για τα υποκείμενα των δεδομένων με δίκαιη και διαφανής επεξεργασία.
    - Λήψη συγκατάθεσης.
    - Η άσκηση του δικαιώματος πρόσβασης και του δικαιώματος μεταφοράς δεδομένων.
    - Εφαρμογή των δικαιωμάτων διόρθωσης και διαγραφής.
    - Εφαρμογή του δικαιώματος περιορισμού της επεξεργασίας και δικαίωμα αντίρρησης.
    - Μεταφορές: συμμόρφωση με τις υποχρεώσεις που αφορούν τη διαβίβαση δεδομένων εκτός της Ευρωπαϊκής Ένωσης.

✓ Εκτίμηση η οποία περιλαμβάνει τις παρακάτω ερμηνείες:

- Μη εφαρμόσιμη.
- Μη ικανοποιητική.
- Προγραμματισμένη βελτίωση.
- Δεκτή.

Εκπόνηση της σύνθεσης, όσον αφορά τη συμμόρφωση με τις ορθές πρακτικές ασφάλειας των ελέγχων που εφαρμόζονται για την αντιμετώπιση των κινδύνων, που σχετίζονται με την ασφάλεια των δεδομένων η οποία περιλαμβάνει:

✓ Έλεγχοι που εφαρμόζονται για την αντιμετώπιση των κινδύνων που σχετίζονται με την ασφάλεια των δεδομένων οι οποίοι χωρίζονται σε:

- **Έλεγχοι που αφορούν ειδικά τα δεδομένα που επεξεργάζονται όπως:**
  - Κρυπτογράφηση.
  - Ανωνυμοποίηση.
  - Κατανομή δεδομένων (σε σχέση με το υπόλοιπο σύστημα πληροφοριών).
  - Έλεγχος λογικής πρόσβασης.
  - Ιχνηλασιμότητα.
  - Παρακολούθηση ακεραιότητας.
  - Αρχειοθέτηση.
  - Ασφάλεια εγγράφου χαρτιού.

- **Γενικοί έλεγχοι ασφαλείας σχετικά με το σύστημα στο οποίο πραγματοποιείται η επεξεργασία όπως:**
  - Λειτουργική ασφάλεια.
  - Περιορισμός κακόβουλου λογισμικού.
  - Διαχείριση σταθμών εργασίας.
  - Ασφάλεια ιστότοπου.
  - Δημιουργία αντιγράφων ασφαλείας.
  - Συντήρηση.
  - Ασφάλεια καναλιών υπολογιστών (δίκτυα).
  - Παρακολούθηση.
  - Έλεγχος φυσικής πρόσβασης.
  - Ασφάλεια υλικού.
  - Αποφυγή πηγών κινδύνου.
  - Προστασία από μη ανθρώπινες πηγές κινδύνων.

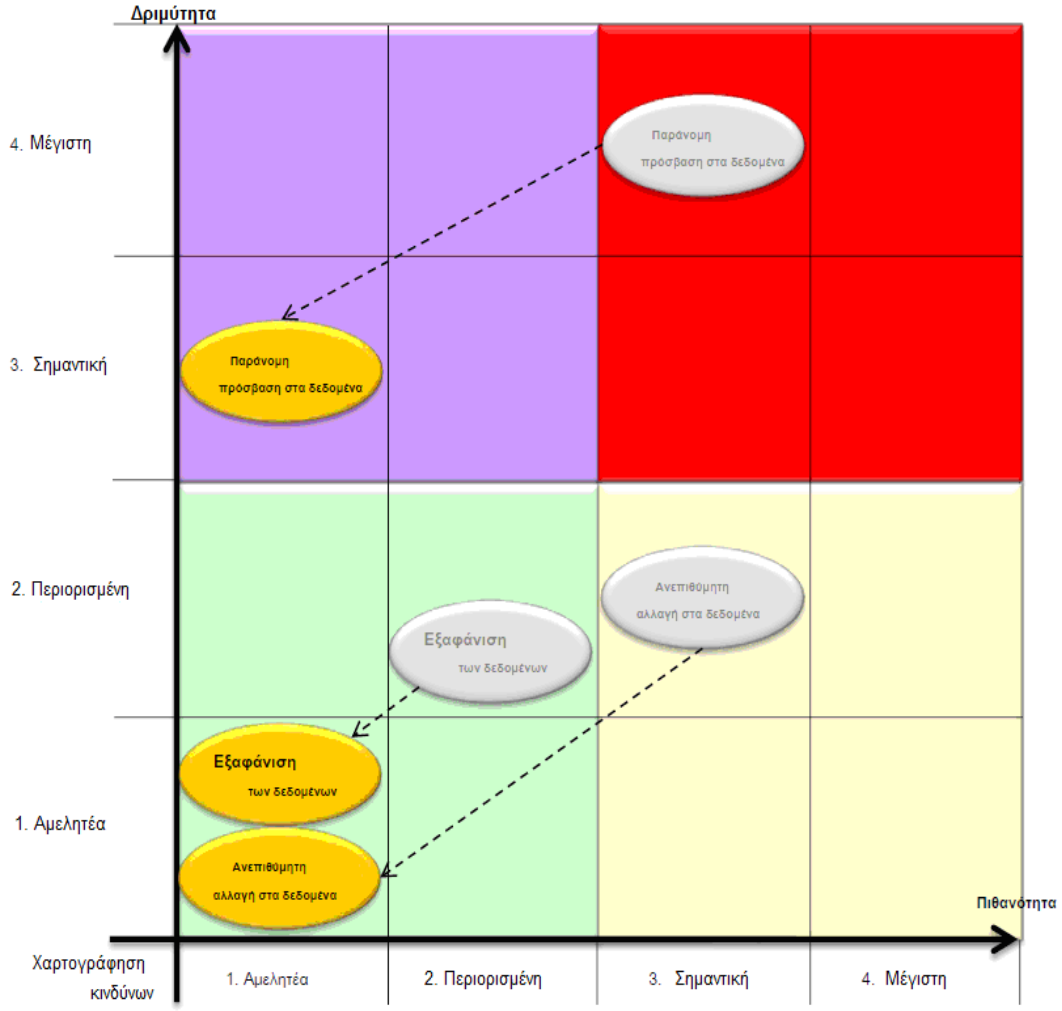
- **Έλεγχοι όπως:**
  - Οργάνωση.
  - Πολιτική (διαχείριση κανόνων).
  - Διαχείριση κινδύνου.
  - Διαχείριση έργου.
  - Διαχείριση περιστατικών και παραβιάσεων δεδομένων.

- Διαχείριση προσωπικού.
- Σχέσεις με τρίτους.
- Εποπτεία.

✓ Εκτίμηση η οποία περιλαμβάνει τις παρακάτω ερμηνείες:

- Μη εφαρμόσιμη.
- Μη ικανοποιητική.
- Προγραμματισμένη βελτίωση.
- Αποδεκτή.

Η παρακάτω γραφική απεικόνιση, χαρτογραφεί τους κινδύνους που σχετίζονται με την ασφάλεια των δεδομένων:



Εικόνα 3-4: Γραφική απεικόνιση κινδύνων που σχετίζονται με την ασφάλεια των δεδομένων
Πηγή: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

Εκπόνηση σχεδίου δράσης το οποίο περιλαμβάνει :

- Επιπρόσθετους ελέγχους.
- Διαχείριση δεδομένων.
- Συχνότητα.
- Δυσκολία.
- Κόστος.
- Πρόοδος.

Πρότυπο σχέδιο κειμένου, τεκμηρίωσης των συμβουλών του υπεύθυνου Προστασίας των δεδομένων.

Παράδειγμα:

Την ημέρα / μήνας / έτος, ο υπεύθυνος προστασίας δεδομένων του φορέα (όνομα φορέα) , εξέδωσε την ακόλουθη γνώμη σχετικά με τη συμμόρφωση της διεξαγόμενης μελέτης επεξεργασίας και εκτίμησης αντίκτυπου (PIA):

[Υπογραφή]

Πρότυπο σχέδιο κειμένου, τεκμηρίωσης της άποψης των υποκειμένων των δεδομένων ή των εκπροσώπων τους.

Παράδειγμα:

Τα υποκείμενα των δεδομένων ήταν / δεν ήταν διαβουλεύσιμα [και εξέφρασαν την ακόλουθη άποψη σχετικά με τη συμμόρφωση της επεξεργασίας με βάση τη διεξαχθείσα μελέτη]:

Ακολουθεί αιτιολόγηση της απόφασης του υπεύθυνου επεξεργασίας δεδομένων:

3.4.2 Η επίσημη επικύρωση της έκθεσης εκτίμησης αντίκτυπου

Πρότυπο σχέδιο κειμένου, της επίσημης επικύρωσης μελέτης του αντίκτυπου, της επεξεργασίας των προσωπικών δεδομένων.

Παράδειγμα:

Στις ημέρα / μήνας / έτος, ο Υπεύθυνος Επεξεργασίας Προσωπικών Δεδομένων του **Πρωτοδικείου Θεσσαλονίκης (ονομ/μο DPO)**, επικυρώνει την PIA για την επεξεργασία των προσωπικών δεδομένων που αποθηκεύονται, και επεξεργάζονται στο εν λόγω κατάστημα, βάσει της μελέτης που διεξήχθη.

Η εκτίμηση του αντίκτυπου της επεξεργασίας των προσωπικών δεδομένων καθώς και οι έλεγχοι που σχεδιάζονται, είναι πλήρως συμμορφωμένοι με τις θεμελιώδεις αρχές, που διέπουν την προστασία της ιδιωτικής ζωής και την αντιμετώπιση των κινδύνων για την ιδιωτική ζωή των υποκειμένων των δεδομένων. Ωστόσο, θα πρέπει να αποδειχθεί η εφαρμογή πρόσθετων ελέγχων, καθώς και η συνεχής βελτίωση της PIA.

[Υπογραφή]

4. Μελέτη περίπτωσης

Στη συνέχεια περιγράφεται η μελέτη περίπτωσης (case-study), Εκτίμησης Αντίκτυπου Δεδομένων, κατά τη διαδικασία Έκδοσης Πιστοποιητικών του Πρωτοδικείου Θεσσαλονίκης, η οποία υλοποιήθηκε με τη χρήση του Open Source λογισμικού "Private Impact Assesment" (PIA), της Γαλλικής Εθνικής Επιτροπής για την Πληροφορική και τις Ελευθερίες (CNIL), αξιοποιώντας τις οδηγίες της, όπως αυτές περιγράφηκαν αναλυτικά πιο πάνω.

Η επιλογή του συγκεκριμένου λογισμικού οφείλεται στο γεγονός ότι αποτελεί ένα δωρεάν και πλήρως παραμετροποίησιμο πρόγραμμα το οποίο δημιουργήθηκε από Δημόσια Αρχή και έχει, ήδη, αποδώσει τα μέγιστα αποτελέσματα ως προς την εκτέλεση της PIA, σε δημόσιους οργανισμούς και φορείς ανά την Ευρώπη, ανταποκρινόμενο στα πρότυπα και τις ιδιαιτερότητες ενός δημόσιου φορέα που επεξεργάζεται μεγάλο όγκο δεδομένων, συγκριτικά με τα υπόλοιπα λογισμικά που καλύπτουν κυρίως τις ανάγκες εναρμόνισης των ιδιωτικών επιχειρήσεων με τον Γενικό Κανονισμό, έτσι όπως αυτά παρουσιάστηκαν αναλυτικά στους πίνακες 3-1 και 3-2.

Η μελέτη περίπτωσης πραγματοποιήθηκε κατά το πρώτο δεκαπενθήμερο του Νοεμβρίου 2018. Το λογισμικό της CNIL, λόγω των περιορισμών που ισχύουν από την ανάδοχο εταιρεία του έργου "Ολοκληρωμένο Σύστημα Διαχείρισης Δικαστικών Υποθέσεων" (ΟΣΔΔΥ) από το Μάιο του 2017, εγκαταστάθηκε τοπικά σε ηλεκτρονικό υπολογιστή του Τμήματος Έκδοσης Πιστοποιητικών.

Μετά από σχετική ενημέρωση και παροχή αναλυτικών οδηγιών, ζητήθηκε από τους υπαλλήλους που εκτελούν την εισαγωγή των δεδομένων των έντυπων αιτήσεων για έκδοση πιστοποιητικών και ενημέρωση της εφαρμογής, να απαντήσουν ηλεκτρονικά στις ερωτήσεις των υποενοτήτων του λογισμικού και πιο συγκεκριμένα των ενοτήτων "Γενικό Πλαίσιο", "Θεμελιώδεις Αρχές" και από την ενότητα "Κίνδυνοι" τις υποενότητες "Αθέμιτη πρόσβαση στα δεδομένα", "Ανεπιθύμητη τροποποίηση των δεδομένων" και "Εξαφάνιση δεδομένων". Με την ολοκλήρωση των απαντήσεων, ο υπεύθυνος του τμήματος, αφού τις επικύρωσε, καθόρισε και την εκτίμησή του ως προς τη "Σοβαρότητα του κινδύνου ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα" και ως προς την "Πιθανότητα εκδήλωσης του κινδύνου σε σχέση με τις απειλές, τις πηγές κινδύνου και τα προγραμματισμένα μέτρα". Έπειτα επιλέγοντας το κουμπί "Αίτηση ελέγχου", για κάθε μια υποενότητα, κατέστησε αυτές διαθέσιμες προς επεξεργασία-αξιολόγηση. Η υποενότητα "Προγραμματισμένα ή

υπάρχοντα μέτρα" της ενότητας "Κίνδυνοι" συμπληρώθηκε υπό τις οδηγίες της αναδόχου εταιρείας του έργου μετά από επικοινωνία μαζί της, προκειμένου να καταγραφούν τα τρέχοντα μέτρα προστασίας που η ίδια εφαρμόζει.

Κατόπιν πραγματοποιήθηκε, η εξαγωγή των απαντήσεων σε αρχείο με μορφή .json και η άμεση εισαγωγή τους στο τρέχον project Εκτίμησης Αντίκτυπου με τη χρήση των εργαλείων, που περιλαμβάνει το συγκεκριμένο λογισμικό. Σκοπός η εκτίμηση του αντίκτυπου σχετικά με την προστασία δεδομένων και ο καθορισμός του κατά πόσο η επεξεργασία, κατά τα στάδια της κατάθεσης έντυπης αίτησης έκδοσης πιστοποιητικού αλλά και της εισαγωγής και αναζήτησης των δεδομένων στην εφαρμογή, ενδέχεται να επιφέρει υψηλό κίνδυνο.

4.1 Υλοποίηση Εκτίμησης Αντίκτυπου Προσωπικών Δεδομένων (PIA) Πρωτοδικείο Θεσσαλονίκης - Έκδοση Πιστοποιητικών


pia
Εκτίμηση αντικτύπου
Αξιολόγηση
Γενικό πλαίσιο
Αυτή η ενότητα σας παρέχει μια σαφή εικόνα της επεξεργασίας των εν λόγω προσωπικών δεδομένων.
Προεπισκόπηση
ΕΠΙΣΚΟΠΗΣΗ
Αυτό το τμήμα σας επιτρέπει να προσδιορίσετε και να παρουσιάσετε το αντικείμενο της μελέτης.
ΣΕ ΑΝΑΜΟΝΉ ΕΠΙΚΎΡΩΣΗΣ.
Αυτό το τμήμα έχει ελεγχθεί και αναμένει την συνολική επικύρωση της ΕΑ. Αν επιθυμείτε να αλλάξετε τον έλεγχο, πρέπει να ακυρώσετε το αίτημα επικύρωσης.
Ποια είναι η υπό εξέταση επεξεργασία;
ΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΠΡΩΤΟΔΙΚΕΙΟΥ
0 σχόλιο/α
20/11/2018
Σχόλιο
Ποιες είναι οι ευθύνες που συνδέονται με την επεξεργασία;
ΕΝΝΟΜΟ ΣΥΜΦΕΡΟΝ ΑΙΤΟΥΝΤΑ
ΟΡΘΗ ΚΑΤΑΧΩΡΙΣΗ ΣΤΟΙΧΕΙΩΝ
ΠΡΟΣΚΟΜΙΣΗ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ ΣΕ ΠΕΡΙΠΤΩΣΗ ΜΗ ΑΥΤΟΠΡΟΣΩΠΗΣ ΠΑΡΟΥΣΙΑΣ
0 σχόλιο/α
20/11/2018
Σχόλιο
Υπάρχουν πρότυπα που ισχύουν για την επεξεργασία;
ΜΕΧΡΙ ΚΑΙ ΣΗΜΕΡΑ ΔΕΝ ΕΧΟΥΝ ΚΥΡΩΘΕΙ ΜΕ ΝΟΜΟ Η ΟΔΗΓΙΑ ΚΑΙ Ο ΚΑΝΟΝΙΣΜΟΣ ΤΗΣ Ε.Ε ΣΤΗΝ ΕΛΛΑΔΑ ΜΕ ΣΥΝΕΠΕΙΑ ΝΑ ΜΗΝ ΕΧΟΥΝ ΚΑΤΑΡΤΙΣΤΕΙ ΟΙ ΑΠΑΙΤΟΥΜΕΝΟΙ ΚΩΔΙΚΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Αποδεκτό
20/11/2018
Το υποτμήμα ελέγχθηκε, σε αναμονή τελικής επικύρωσης
Όλα τα πεδία πρέπει να συμπληρωθούν
Ακύρωση αιτήματος επικύρωσης
Δεδομένα, διαδικασίες και υποστηρικτικά περιουσιακά στοιχεία »

Αξιολόγηση

Γενικό πλαίσιο

Προεπισκόπηση

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

ΔΕΔΟΜΈΝΑ, ΔΙΑΔΙΚΑΣΊΕΣ ΚΑΙ ΥΠΟΣΤΗΡΙΚΤΙΚΆ ΠΕΡΙΟΥΣΙΑΚΆ ΣΤΟΙΧΕΊΑ

Αυτό το τμήμα σας επιτρέπει να ορίσετε και να περιγράψετε λεπτομερώς το αντικείμενο της επεξεργασίας.

ΣΕ ΑΝΑΜΟΝΉ ΕΠΙΚΎΡΩΣΗΣ.

Αυτό το τμήμα έχει ελεγχθεί και αναμένει την συνολική επικύρωση της ΕΑ. Αν επιθυμείτε να αλλάξετε τον έλεγχο, πρέπει να ακυρώσετε το αίτημα επικύρωσης.

Ποιά προσωπικά δεδομένα δέχονται επεξεργασία;

- ΕΠΩΝΥΜΟ
- ΟΝΟΜΑ
- ΠΑΤΡΩΝΥΜΟ
- ΜΗΤΡΩΝΥΜΟ
- ΓΕΝΟΣ
- ΟΝΟΜΑ ΣΥΖΥΓΟΥ
- ΑΦΜ
- ΔΙΕΥΘΥΝΣΗ ΚΑΤΟΙΚΙΑΣ
- ΤΗΛΕΦΩΝΟ ΕΠΙΚΟΙΝΩΝΙΑΣ
- ΗΜΕΡΟΜΗΝΙΑ & ΤΟΠΟΣ ΓΕΝΝΗΣΗΣ

0 σχόλιο/α

20/11/2018 Σχόλιο

Πώς λειτουργεί ο κύκλος ζωής των δεδομένων και των διαδικασιών;

ΕΠΗΡΕΑΖΕΤΑΙ ΣΕ ΜΕΓΑΛΟ ΒΑΘΜΟ ΑΠΟ ΤΑ ΤΡΙΑ ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ BIG DATA: VOLUME, VARIETY, VELOCITY. ΤΑ ΟΠΟΙΑ ΚΑΘΟΡΙΖΟΥΝ:

- ΤΗΝ ΚΑΤΑΧΩΡΙΣΗ
- ΤΗΝ ΑΠΟΘΗΚΕΥΣΗ
- ΤΗ ΜΕΤΑΦΟΡΑ
- ΤΗΝ ΑΝΑΚΤΗΣΗ
- ΤΗΝ ΑΝΑΠΑΡΑΓΩΓΗ
- ΤΗΝ ΑΝΑΛΥΣΗ-ΤΑΞΙΝΟΜΗΣΗ-ΣΥΝΘΕΣΗ
- ΤΗ ΔΙΑΓΡΑΦΗ

0 σχόλιο/α

20/11/2018 Σχόλιο

Ποια είναι τα περιουσιακά στοιχεία που υποστηρίζουν τα δεδομένα;

- ΥΛΙΚΟ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΑ ΜΕΣΑ ΕΝΗΜΕΡΩΣΗΣ ΔΕΔΟΜΕΝΩΝ
- ΛΟΓΙΣΜΙΚΟ
- ΣΥΝΔΕΣΗ ΥΠΟΛΟΓΙΣΤΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

0 σχόλιο/α

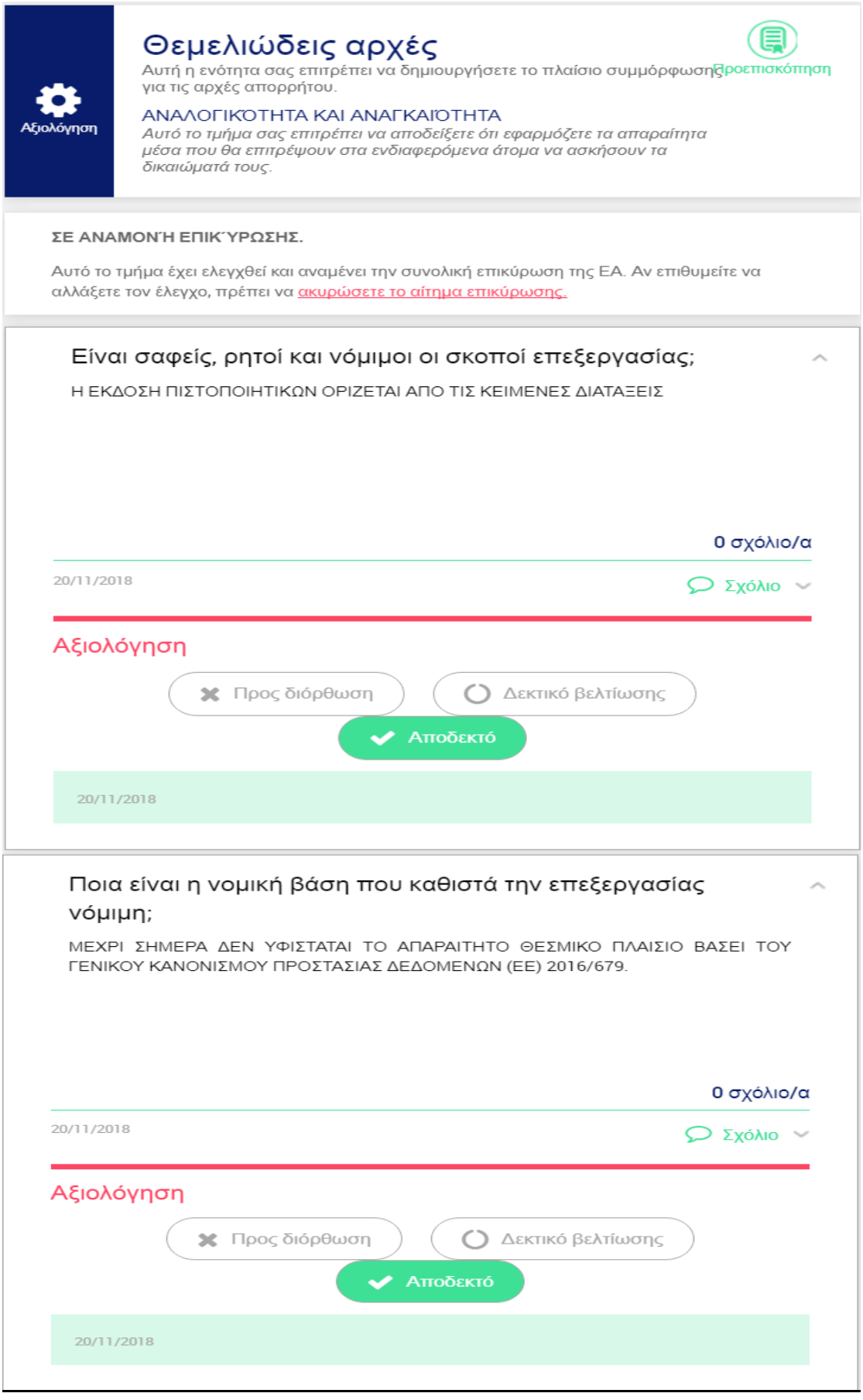
20/11/2018 Σχόλιο

Το υποτμήμα ελέγχθηκε, σε αναμονή τελικής επικύρωσης

Όλα τα πεδία πρέπει να συμπληρωθούν

Ακύρωση αιτήματος επικύρωσης

« Επισκόπηση Αναλογικότητα και αναγκαιότητα »


Αξιολόγηση
Θεμελιώδεις αρχές
Αυτή η ενότητα σας επιτρέπει να δημιουργήσετε το πλαίσιο συμμόρφωσης για τις αρχές απορρήτου.
Προεπισκόπηση
ΑΝΑΛΟΓΙΚΌΤΗΤΑ ΚΑΙ ΑΝΑΓΚΑΙΌΤΗΤΑ
Αυτό το τμήμα σας επιτρέπει να αποδείξετε ότι εφαρμόζετε τα απαραίτητα μέσα που θα επιτρέψουν στα ενδιαφερόμενα άτομα να ασκήσουν τα δικαιώματά τους.
ΣΕ ΑΝΑΜΟΝΉ ΕΠΙΚΎΡΩΣΗΣ.
Αυτό το τμήμα έχει ελεγχθεί και αναμένει την συνολική επικύρωση της ΕΑ. Αν επιθυμείτε να αλλάξετε τον έλεγχο, πρέπει να ακυρώσετε το αίτημα επικύρωσης.
Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;
Η ΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΟΡΙΖΕΤΑΙ ΑΠΟ ΤΙΣ ΚΕΙΜΕΝΕΣ ΔΙΑΤΑΞΕΙΣ
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Ποια είναι η νομική βάση που καθιστά την επεξεργασίας νόμιμη;
ΜΕΧΡΙ ΣΗΜΕΡΑ ΔΕΝ ΥΦΙΣΤΑΤΑΙ ΤΟ ΑΠΑΡΑΙΤΗΤΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΒΑΣΕΙ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018

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 ΔΕΔΟΜΕΝΑ ΠΟΥ ΕΧΟΥΝ ΑΝΑΦΕΡΘΕΙ ΣΤΗΝ ΥΠΟΕΝΟΤΗΤΑ "ΔΙΑΔΙΚΑΣΙΕΣ" ΕΙΝΑΙ ΤΑ ΕΛΑΧΙΣΤΑ ΑΠΑΡΑΙΤΗΤΑ ΓΙΑ ΤΗΝ ΕΚΔΟΣΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ.

0 σχόλιο/α

20/11/2018 Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

Τα δεδομένα είναι ακριβή και ενημερωμένα;

ΔΙΑΣΥΝΔΕΣΗ ΜΕ ΥΠΗΡΕΣΙΕΣ ΠΡΟΣ ΕΠΙΒΕΒΑΙΩΣΗ ΤΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ ΤΩΝ ΔΗΛΩΘΕΝΤΩΝ ΑΠΟ ΤΟΝ ΑΙΤΟΥΝΤΑ ΣΤΟΙΧΕΙΩΝ.

0 σχόλιο/α

20/11/2018 Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;

ΜΕΧΡΙ ΣΗΜΕΡΑ ΥΦΙΣΤΑΝΤΑΙ ΠΡΩΤΟΚΟΛΛΑ ΚΑΤΑΣΤΡΟΦΗΣ ΜΟΝΟ ΤΟΥ ΦΥΣΙΚΟΥ ΑΡΧΕΙΟΥ ΜΕΤΑ ΤΗΝ ΠΑΡΟΔΟ ΤΟΥ ΧΡΟΝΟΥ ΔΙΑΦΥΛΑΞΗΣ ΠΟΥ ΟΡΙΖΕΙ Ο ΝΟΜΟΣ. ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΑΠΟΘΗΚΕΥΣΗ ΔΕΔΟΜΕΝΩΝ ΕΛΛΕΙΠΕΙ ΤΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ.

0 σχόλιο/α

20/11/2018 Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

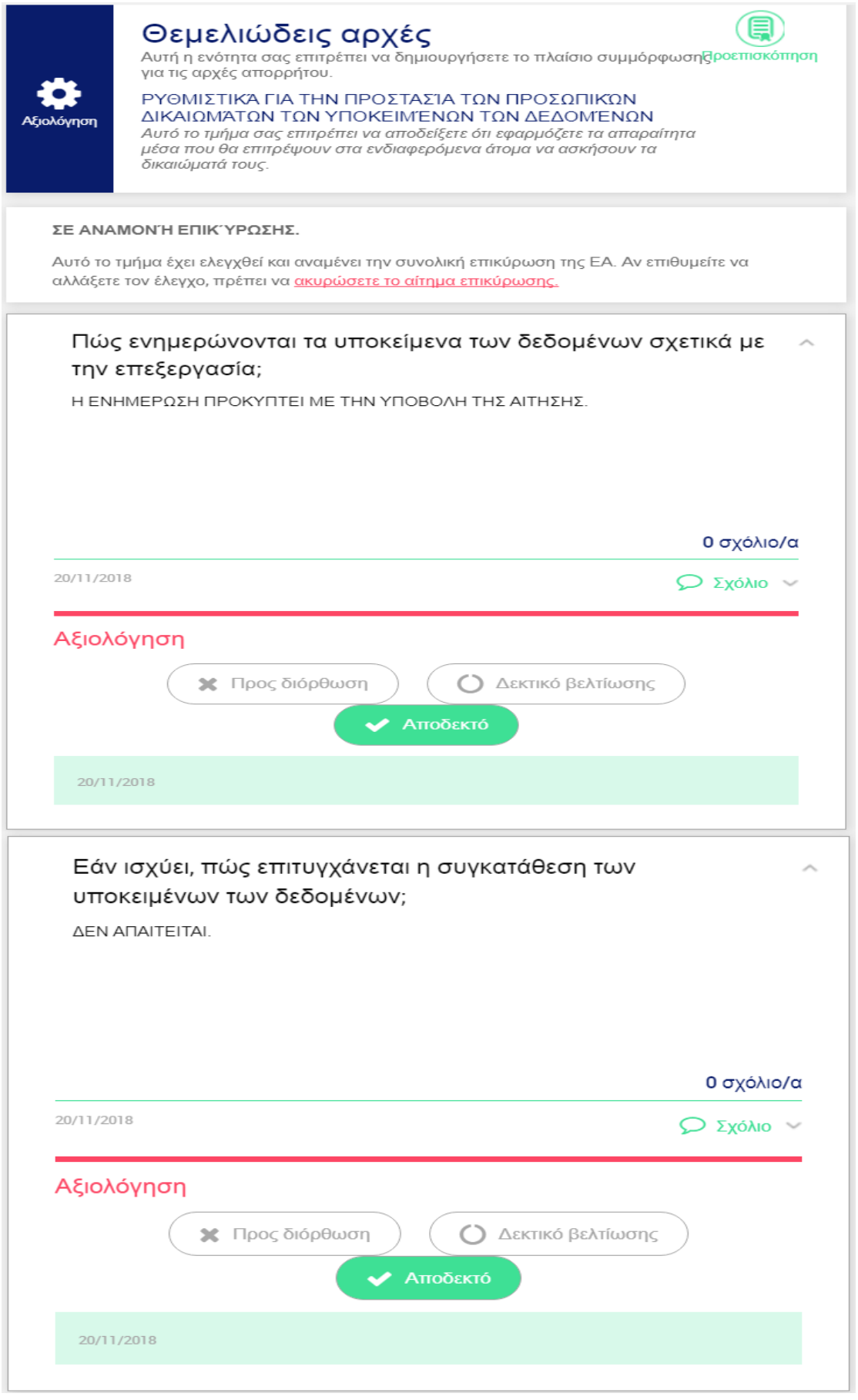
Το υποτμήμα ελέγχθηκε, σε αναμονή τελικής επικύρωσης

Όλα τα πεδία πρέπει να συμπληρωθούν

Ακύρωση αιτήματος επικύρωσης

« Δεδομένα, διαδικασίες και υποστηρικτικά περιουσιακά στοιχεία

Ρυθμιστικά για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων »


Αξιολόγηση
Θεμελιώδεις αρχές
Αυτή η ενότητα σας επιτρέπει να δημιουργήσετε το πλαίσιο συμμόρφωσης για τις αρχές απορρήτου.
Προεπισκόπηση
ΡΥΘΜΙΣΤΙΚΆ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΊΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΙΚΑΙΩΜΆΤΩΝ ΤΩΝ ΥΠΟΚΕΙΜΈΝΩΝ ΤΩΝ ΔΕΔΟΜΈΝΩΝ
Αυτό το τμήμα σας επιτρέπει να αποδείξετε ότι εφαρμόζετε τα απαραίτητα μέσα που θα επιτρέψουν στα ενδιαφερόμενα άτομα να ασκήσουν τα δικαιώματά τους.
ΣΕ ΑΝΑΜΟΝΉ ΕΠΙΚΎΡΩΣΗΣ.
Αυτό το τμήμα έχει ελεγχθεί και αναμένει την συνολική επικύρωση της ΕΑ. Αν επιθυμείτε να αλλάξετε τον έλεγχο, πρέπει να ακυρώσετε το αίτημα επικύρωσης.
Πώς ενημερώνονται τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία;
Η ΕΝΗΜΕΡΩΣΗ ΠΡΟΚΥΠΤΕΙ ΜΕ ΤΗΝ ΥΠΟΒΟΛΗ ΤΗΣ ΑΙΤΗΣΗΣ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Εάν ισχύει, πώς επιτυγχάνεται η συγκατάθεση των υποκειμένων των δεδομένων;
ΔΕΝ ΑΠΑΙΤΕΙΤΑΙ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018

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

ΔΕΝ ΥΦΙΣΤΑΤΑΙ ΠΡΟΣ ΤΟ ΠΑΡΟΝ ΑΥΤΗ Η ΔΥΝΑΤΟΤΗΤΑ.

0 σχόλιο/α

20/11/2018

Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

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

ΠΡΟΒΛΕΠΕΤΑΙ Η ΔΥΝΑΤΟΤΗΤΑ ΑΜΕΣΗΣ ΔΙΟΡΘΩΣΗΣ ΑΝΑΚΡΙΒΩΝ ΔΕΔΟΜΕΝΩΝ ΑΛΛΑ ΟΧΙ ΔΙΑΓΡΑΦΗΣ ΑΥΤΩΝ.

0 σχόλιο/α

20/11/2018

Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

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

ΔΕ ΣΧΕΤΙΖΕΤΑΙ ΜΕ ΤΟ ΔΗΜΟΣΙΟ ΦΟΡΕΑ.

0 σχόλιο/α

20/11/2018

Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

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

ΠΡΟΣΔΙΟΡΙΖΟΝΤΑΙ ΑΠΟ ΤΟΝ ΕΣΩΤΕΡΙΚΟ ΚΑΝΟΝΙΣΜΟ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ ΠΡΩΤΟΔΙΚΕΙΟΥ.

0 σχόλιο/α

20/11/2018

Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

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

ΑΠΟΤΕΛΕΙ ΑΝΤΙΚΕΙΜΕΝΟ ΔΙΕΥΡΕΥΝΗΣΗΣ ΤΗΣ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ.

0 σχόλιο/α

20/11/2018

Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

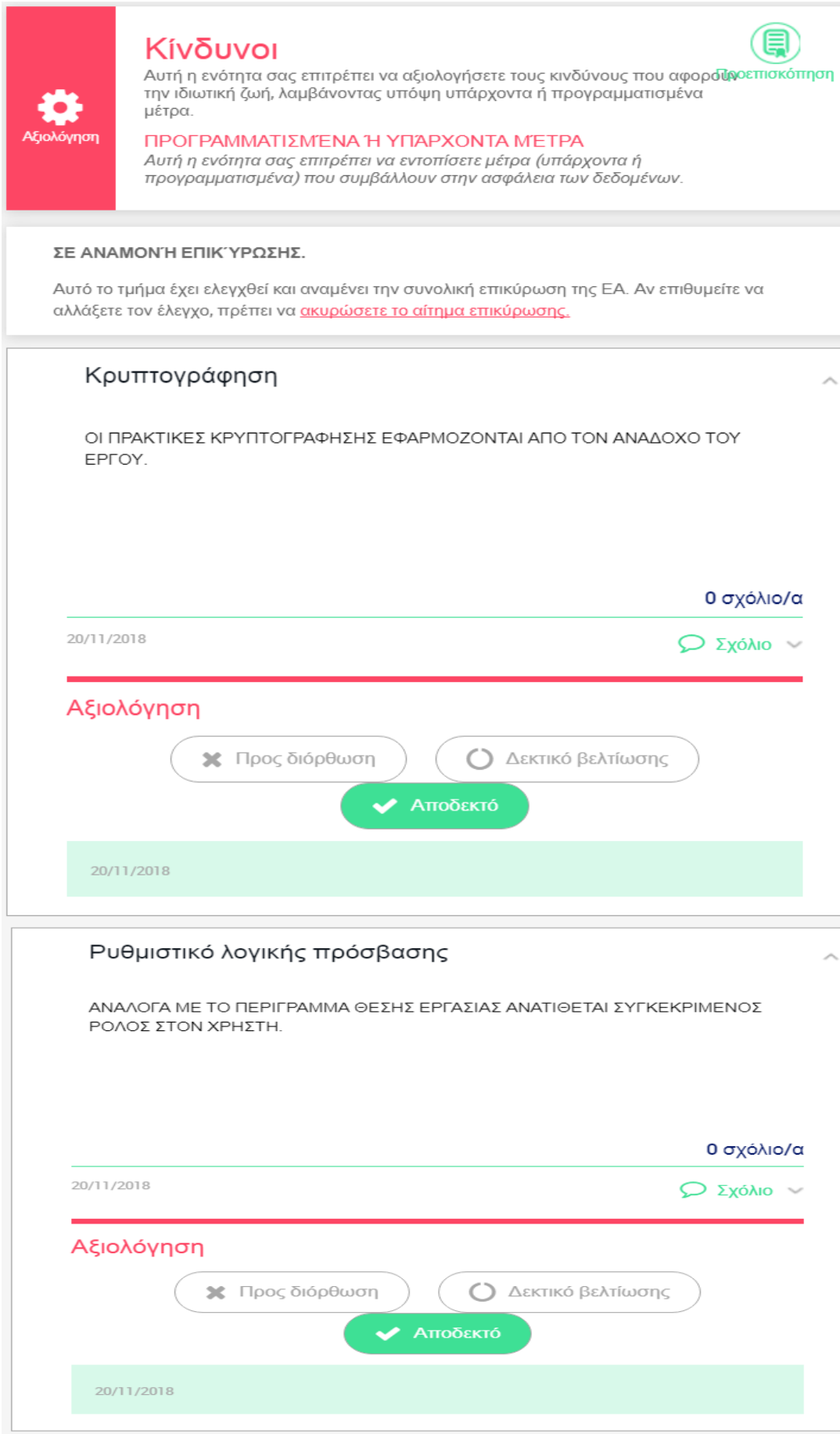
Το υποτμήμα ελέγχθηκε, σε αναμονή τελικής επικύρωσης

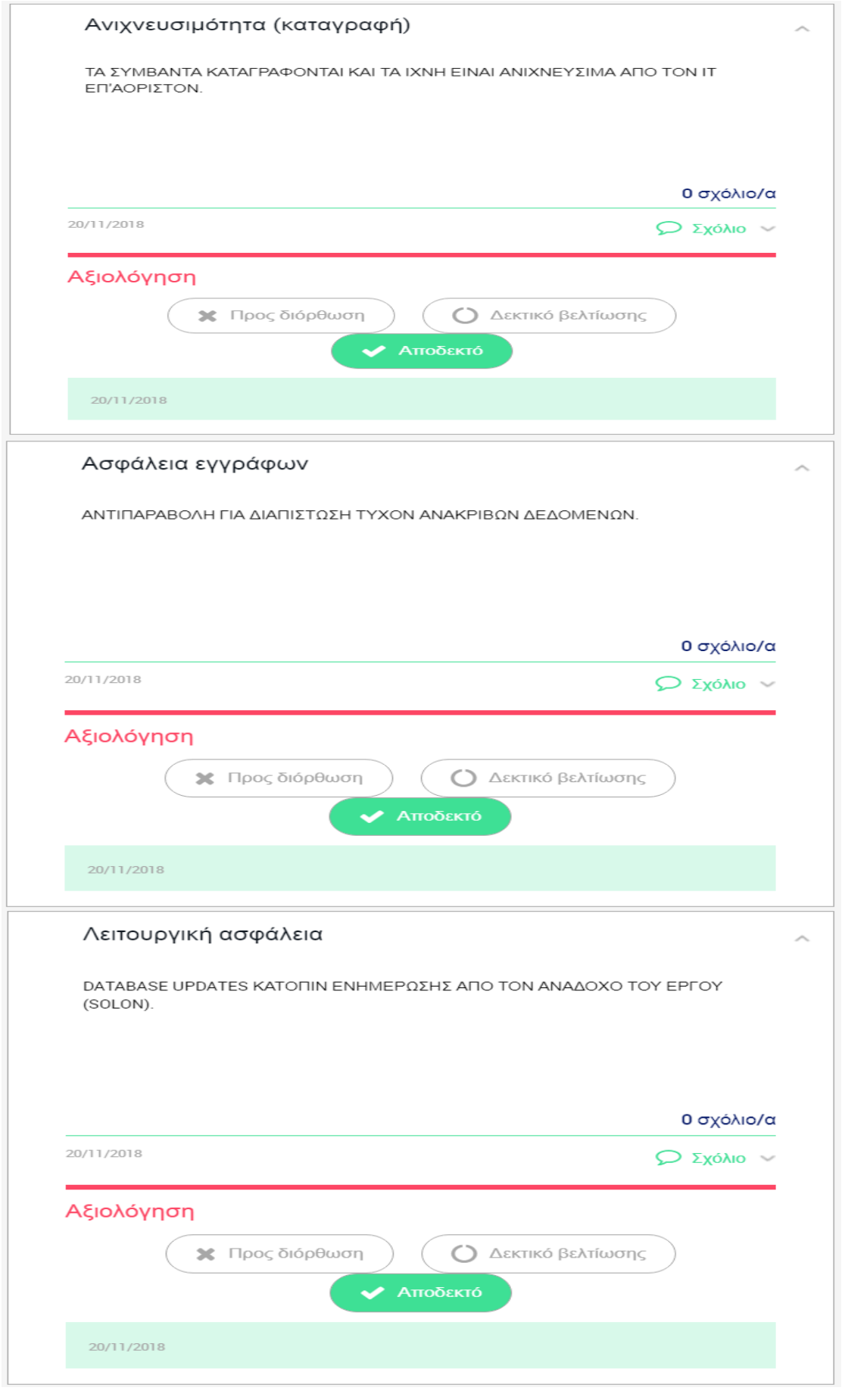
Όλα τα πεδία πρέπει να συμπληρωθούν

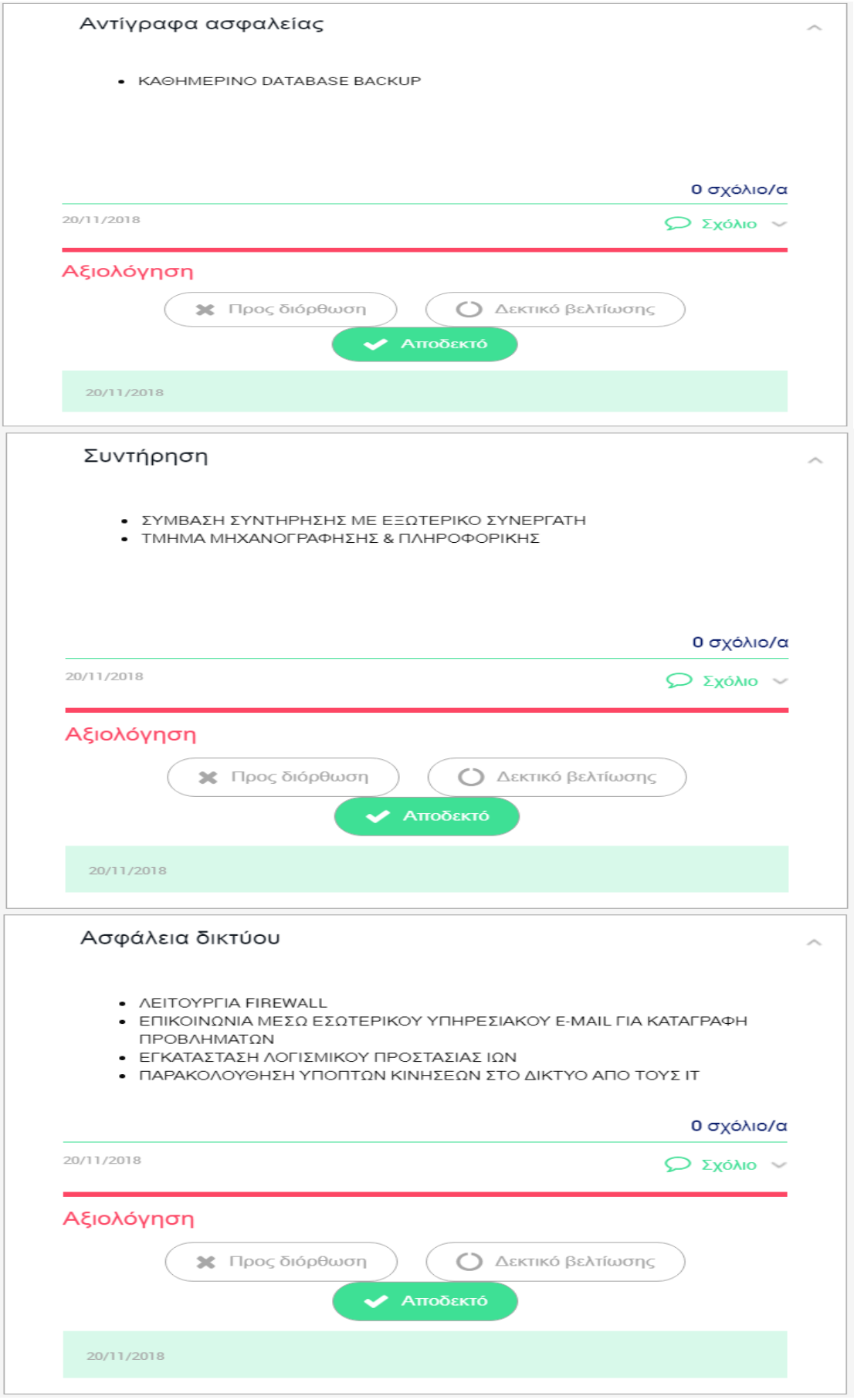
Ακύρωση αιτήματος επικύρωσης

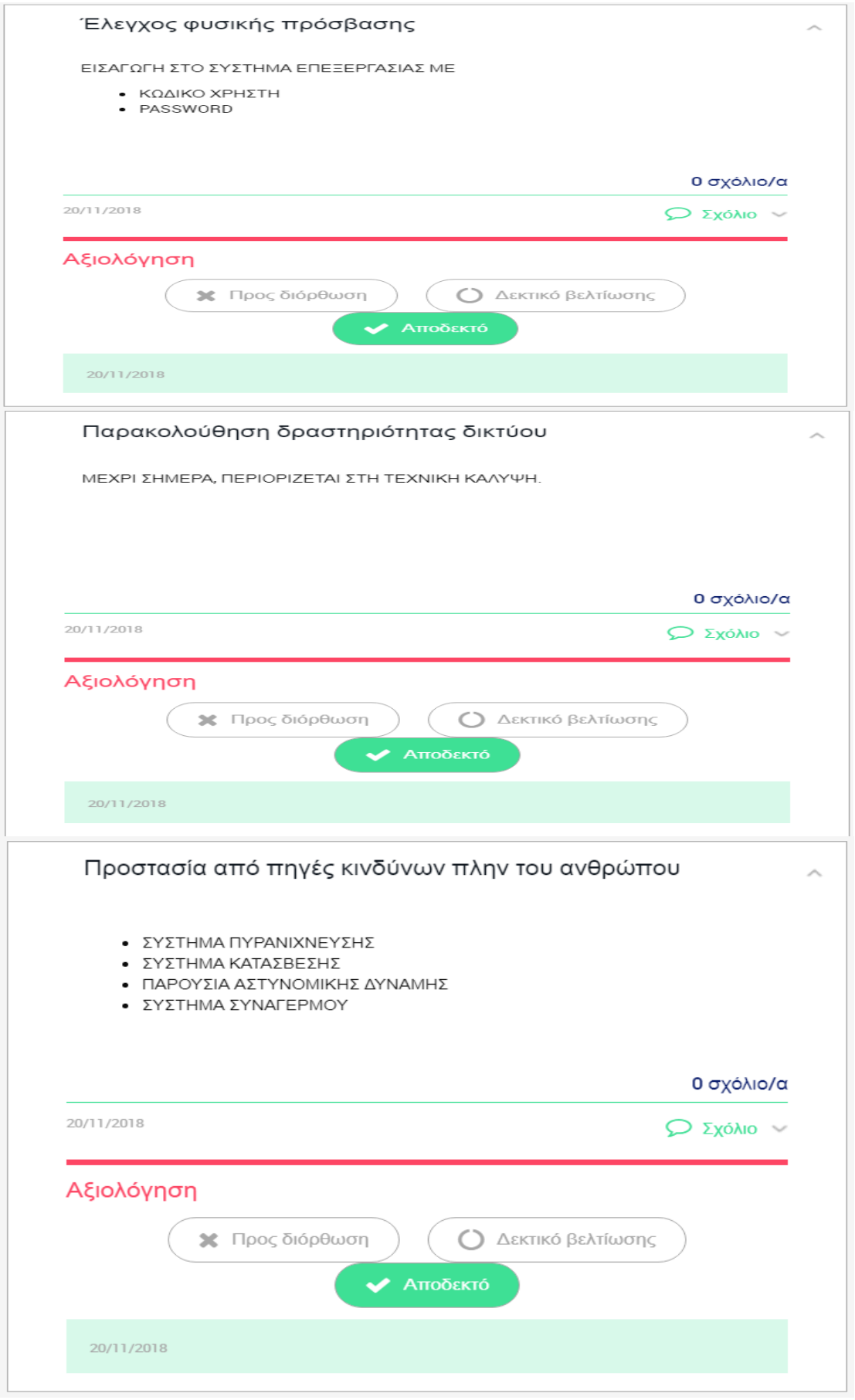
« Αναλογικότητα και αναγκαιότητα

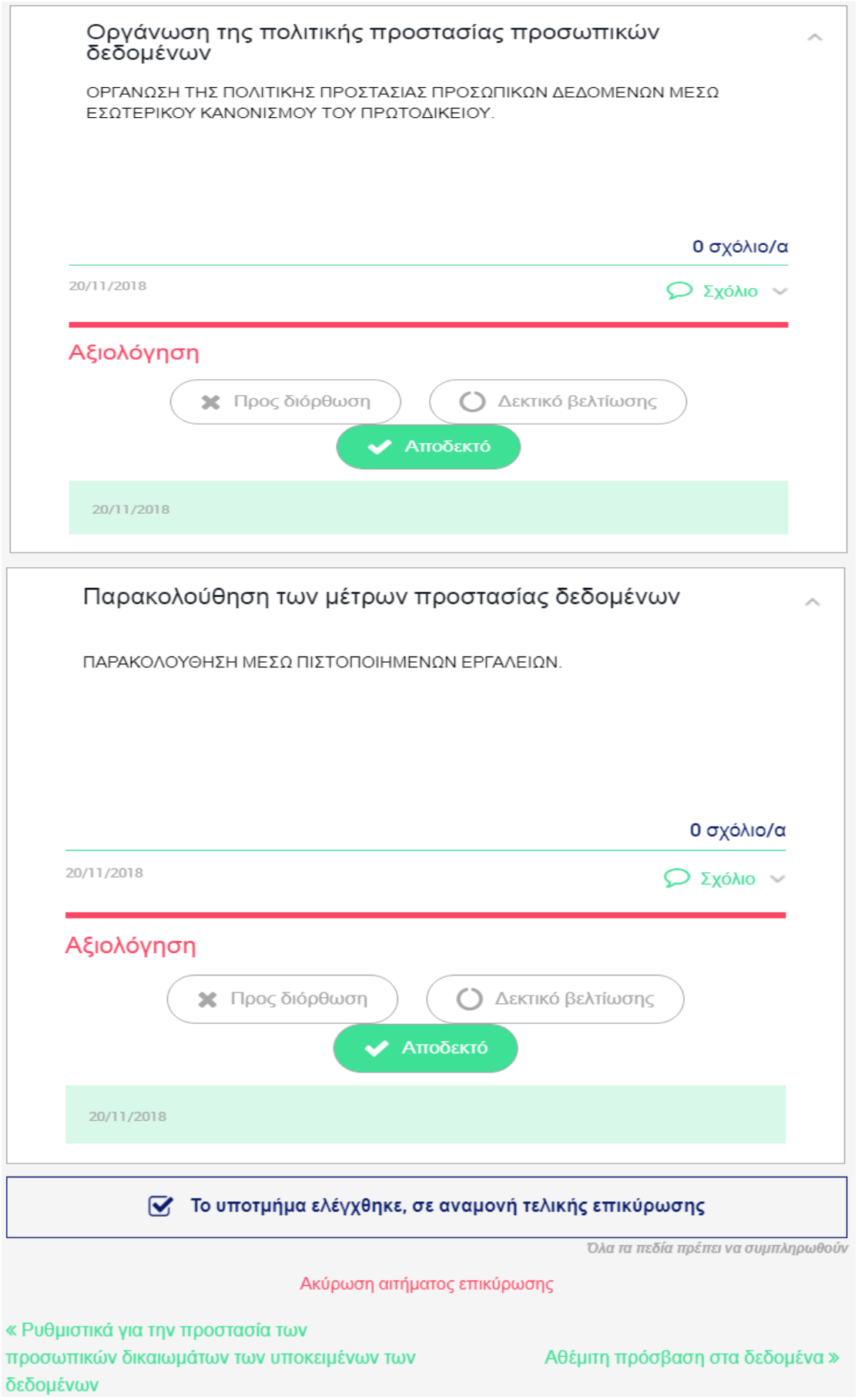
Προγραμματισμένα ή υπάρχοντα μέτρα »

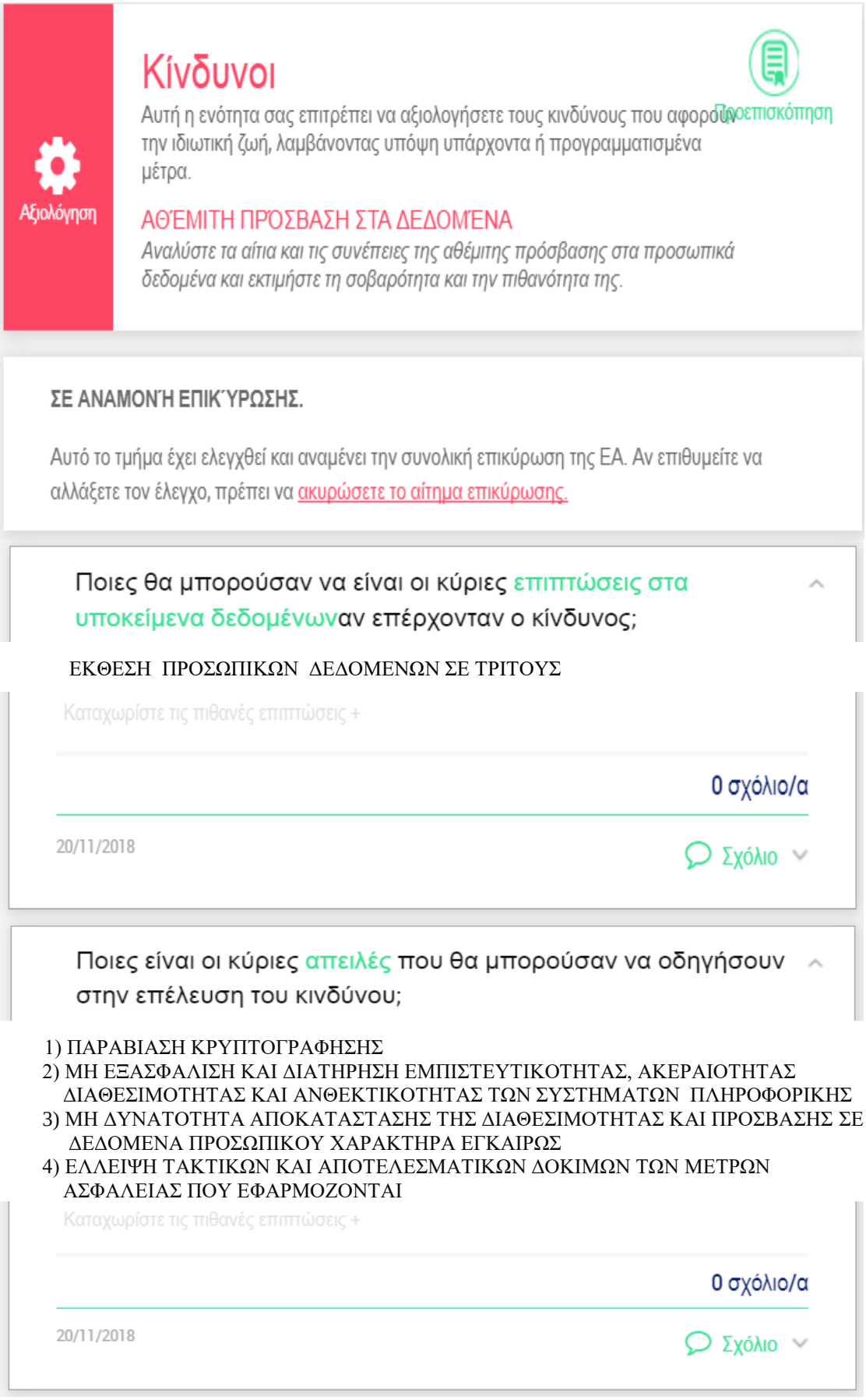

Αξιολόγηση
Κίνδυνοι
Αυτή η ενότητα σας επιτρέπει να αξιολογήσετε τους κινδύνους που αφορούν την ιδιωτική ζωή, λαμβάνοντας υπόψη υπάρχοντα ή προγραμματισμένα μέτρα.
Προεπισκόπηση
ΠΡΟΓΡΑΜΜΑΤΙΣΜΈΝΑ Ή ΥΠΆΡΧΟΝΤΑ ΜΈΤΡΑ
Αυτή η ενότητα σας επιτρέπει να εντοπίσετε μέτρα (υπάρχοντα ή προγραμματισμένα) που συμβάλλουν στην ασφάλεια των δεδομένων.
ΣΕ ΑΝΑΜΟΝΉ ΕΠΙΚΎΡΩΣΗΣ.
Αυτό το τμήμα έχει ελεγχθεί και αναμένει την συνολική επικύρωση της ΕΑ. Αν επιθυμείτε να αλλάξετε τον έλεγχο, πρέπει να ακυρώσετε το αίτημα επικύρωσης.
Κρυπτογράφηση
ΟΙ ΠΡΑΚΤΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΕΦΑΡΜΟΖΟΝΤΑΙ ΑΠΟ ΤΟΝ ΑΝΑΔΟΧΟ ΤΟΥ ΕΡΓΟΥ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Ρυθμιστικό λογικής πρόσβασης
ΑΝΑΛΟΓΑ ΜΕ ΤΟ ΠΕΡΙΓΡΑΜΜΑ ΘΕΣΗΣ ΕΡΓΑΣΙΑΣ ΑΝΑΤΙΘΕΤΑΙ ΣΥΓΚΕΚΡΙΜΕΝΟΣ ΡΟΛΟΣ ΣΤΟΝ ΧΡΗΣΤΗ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018


Ανιχνευσιμότητα (καταγραφή)
ΤΑ ΣΥΜΒΑΝΤΑ ΚΑΤΑΓΡΑΦΟΝΤΑΙ ΚΑΙ ΤΑ ΙΧΝΗ ΕΙΝΑΙ ΑΝΙΧΝΕΥΣΙΜΑ ΑΠΟ ΤΟΝ ΙΤ ΕΠ'ΑΟΡΙΣΤΟΝ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Ασφάλεια εγγράφων
ΑΝΤΙΠΑΡΑΒΟΛΗ ΓΙΑ ΔΙΑΠΙΣΤΩΣΗ ΤΥΧΟΝ ΑΝΑΚΡΙΒΩΝ ΔΕΔΟΜΕΝΩΝ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Λειτουργική ασφάλεια
DATABASE UPDATES ΚΑΤΟΠΙΝ ΕΝΗΜΕΡΩΣΗΣ ΑΠΟ ΤΟΝ ΑΝΑΔΟΧΟ ΤΟΥ ΕΡΓΟΥ (SOLON).
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018


Αντίγραφα ασφαλείας
ΚΑΘΗΜΕΡΙΝΟ DATABASE BACKUP
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Συντήρηση
ΣΥΜΒΑΣΗ ΣΥΝΤΗΡΗΣΗΣ ΜΕ ΕΞΩΤΕΡΙΚΟ ΣΥΝΕΡΓΑΤΗ
ΤΜΗΜΑ ΜΗΧΑΝΟΓΡΑΦΗΣΗΣ & ΠΛΗΡΟΦΟΡΙΚΗΣ
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Ασφάλεια δικτύου
ΛΕΙΤΟΥΡΓΙΑ FIREWALL
ΕΠΙΚΟΙΝΩΝΙΑ ΜΕΣΩ ΕΣΩΤΕΡΙΚΟΥ ΥΠΗΡΕΣΙΑΚΟΥ E-MAIL ΓΙΑ ΚΑΤΑΓΡΑΦΗ ΠΡΟΒΛΗΜΑΤΩΝ
ΕΓΚΑΤΑΣΤΑΣΗ ΛΟΓΙΣΜΙΚΟΥ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΥΠΟΠΤΩΝ ΚΙΝΗΣΕΩΝ ΣΤΟ ΔΙΚΤΥΟ ΑΠΟ ΤΟΥΣ IT
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018


Έλεγχος φυσικής πρόσβασης
ΕΙΣΑΓΩΓΗ ΣΤΟ ΣΥΣΤΗΜΑ ΕΠΕΞΕΡΓΑΣΙΑΣ ΜΕ
ΚΩΔΙΚΟ ΧΡΗΣΤΗ
PASSWORD
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Παρακολούθηση δραστηριότητας δικτύου
ΜΕΧΡΙ ΣΗΜΕΡΑ, ΠΕΡΙΟΡΙΖΕΤΑΙ ΣΤΗ ΤΕΧΝΙΚΗ ΚΑΛΥΨΗ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Προστασία από πηγές κινδύνων πλην του ανθρώπου
ΣΥΣΤΗΜΑ ΠΥΡΑΝΙΧΝΕΥΣΗΣ
ΣΥΣΤΗΜΑ ΚΑΤΑΣΒΕΣΗΣ
ΠΑΡΟΥΣΙΑ ΑΣΤΥΝΟΜΙΚΗΣ ΔΥΝΑΜΗΣ
ΣΥΣΤΗΜΑ ΣΥΝΑΓΕΡΜΟΥ
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018


Οργάνωση της πολιτικής προστασίας προσωπικών δεδομένων
ΟΡΓΑΝΩΣΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕΣΩ ΕΣΩΤΕΡΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΤΟΥ ΠΡΩΤΟΔΙΚΕΙΟΥ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Παρακολούθηση των μέτρων προστασίας δεδομένων
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΜΕΣΩ ΠΙΣΤΟΠΟΙΗΜΕΝΩΝ ΕΡΓΑΛΕΙΩΝ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Το υποτμήμα ελέγχθηκε, σε αναμονή τελικής επικύρωσης
Όλα τα πεδία πρέπει να συμπληρωθούν
Ακύρωση αιτήματος επικύρωσης
« Ρυθμιστικά για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων
Αθέμιτη πρόσβαση στα δεδομένα »


Αξιολόγηση
Κίνδυνοι
Προεπισκόπηση
Αυτή η ενότητα σας επιτρέπει να αξιολογήσετε τους κινδύνους που αφορούν την ιδιωτική ζωή, λαμβάνοντας υπόψη υπάρχοντα ή προγραμματισμένα μέτρα.
ΑΘΈΜΙΤΗ ΠΡΌΣΒΑΣΗ ΣΤΑ ΔΕΔΟΜΈΝΑ
Αναλύστε τα αίτια και τις συνέπειες της αθέμιτης πρόσβασης στα προσωπικά δεδομένα και εκτιμήστε τη σοβαρότητα και την πιθανότητα της.
ΣΕ ΑΝΑΜΟΝΉ ΕΠΙΚΎΡΩΣΗΣ.
Αυτό το τμήμα έχει ελεγχθεί και αναμένει την συνολική επικύρωση της ΕΑ. Αν επιθυμείτε να αλλάξετε τον έλεγχο, πρέπει να ακυρώσετε το αίτημα επικύρωσης.
Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα δεδομένωναν επέρχονταν ο κίνδυνος;
ΕΚΘΕΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΟΥΣ
Καταχωρίστε τις πιθανές επιπτώσεις +
0 σχόλιο/α
20/11/2018
Σχόλιο
Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;
1) ΠΑΡΑΒΙΑΣΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ
2) ΜΗ ΕΞΑΣΦΑΛΙΣΗ ΚΑΙ ΔΙΑΤΗΡΗΣΗ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ, ΑΚΕΡΑΙΟΤΗΤΑΣ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ ΚΑΙ ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
3) ΜΗ ΔΥΝΑΤΟΤΗΤΑ ΑΠΟΚΑΤΑΣΤΑΣΗΣ ΤΗΣ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ ΚΑΙ ΠΡΟΣΒΑΣΗΣ ΣΕ ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΕΓΚΑΙΡΩΣ
4) ΕΛΛΕΙΨΗ ΤΑΚΤΙΚΩΝ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΩΝ ΔΟΚΙΜΩΝ ΤΩΝ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΕΦΑΡΜΟΖΟΝΤΑΙ
Καταχωρίστε τις πιθανές επιπτώσεις +
0 σχόλιο/α
20/11/2018
Σχόλιο

Ποιές είναι οι πηγές κινδύνου;

1) ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΠΟΥ ΣΥΛΛΕΓΟΝΤΑΙ ΚΑΙ ΑΠΟΘΗΚΕΥΟΝΤΑΙ ΧΩΡΙΣ ΛΟΓΟ
2) ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΠΟΥ ΔΕ ΔΙΑΧΕΙΡΙΖΟΝΤΑΙ ΣΩΣΤΑ
3) ΜΗ ΚΑΘΟΡΙΣΜΕΝΗ ΠΕΡΙΟΔΟΣ ΔΙΑΤΗΡΗΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ
4) ΜΗ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΙ ΕΛΕΓΧΟΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
5) ΠΑΘΗΤΙΚΗ ΔΙΑΡΡΟΗ ΔΕΔΟΜΕΝΩΝ (ΥΠΟΚΛΟΠΗ ΠΛΗΡΟΦΟΡΙΩΝ ΔΥΣΚΟΛΟΣ ΕΝΤΟΠΙΣΜΟΣ)
6) ΕΝΕΡΓΗΤΙΚΗ ΔΙΑΡΡΟΗ ΔΕΔΟΜΕΝΩΝ (ΜΕΤΑΒΟΛΗ ΔΕΔΟΜΕΝΩΝ)

Καταχωρίστε τις πιθανές επιπτώσεις +

0 σχόλιο/α

20/11/2018 Σχόλιο

Ποιά από τα εντοπισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

ΚΡΥΠΤΟΓΡΑΦΗΣΗ, ΑΣΦΑΛΕΙΑ ΕΓΓΡΑΦΩΝ, ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ, ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΠΗΓΕΣ ΚΙΝΔΥΝΩΝ ΠΛΗΝ ΤΟΥ ΑΝΘΡΩΠΟΥ, ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΤΩΝ ΜΕΤΡΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΈΝΩΝ, ΑΝΙΧΝΕΥΣΙΜΌΤΗΤΑ (ΚΑΤΑΓΡΑΦΉ).

Καταχωρίστε τις πιθανές επιπτώσεις +

0 σχόλιο/α

20/11/2018 Σχόλιο

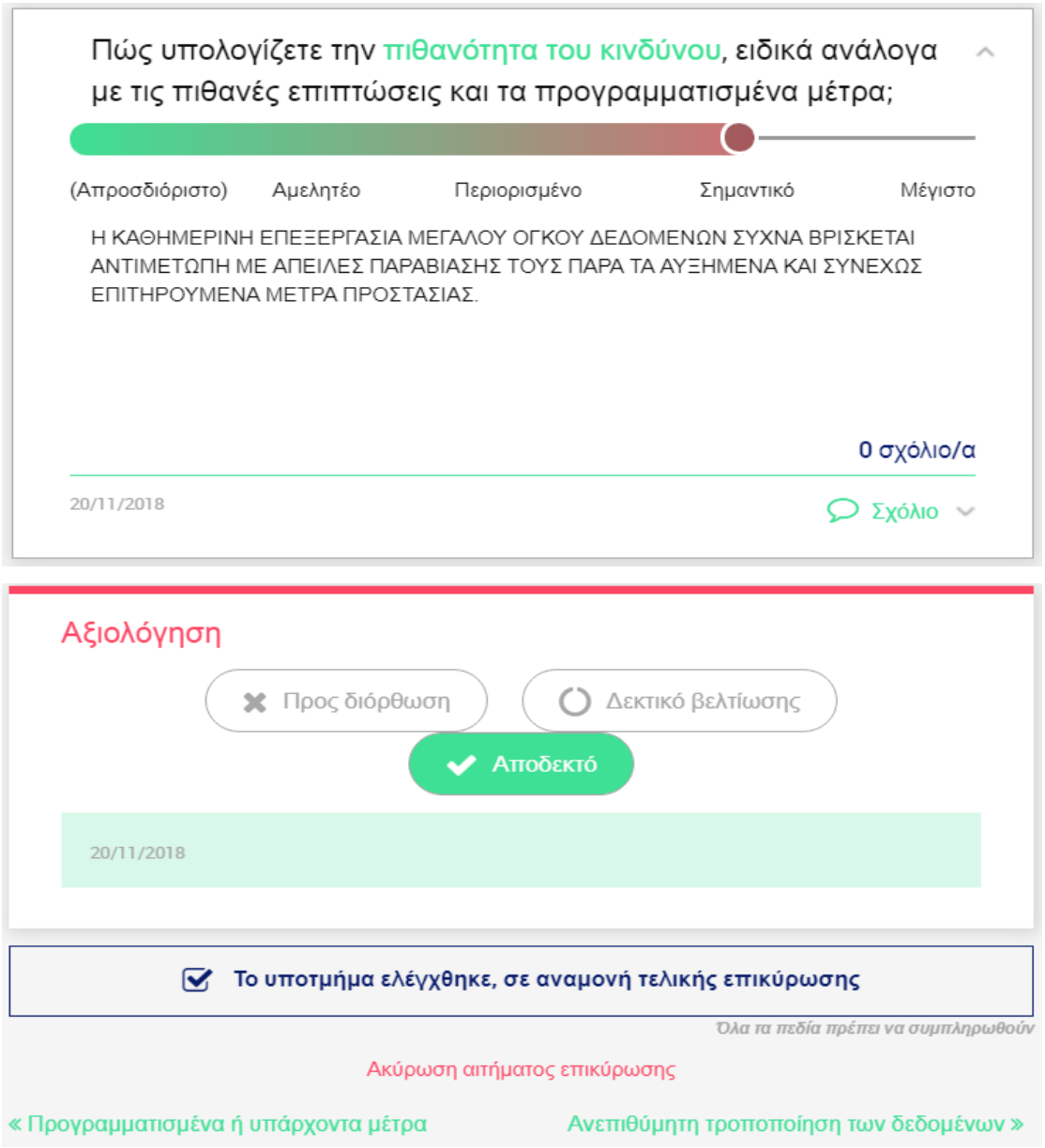
Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

(Απροσδιόριστο) Αμελητέο Περιορισμένο Σημαντικό Μέγιστο

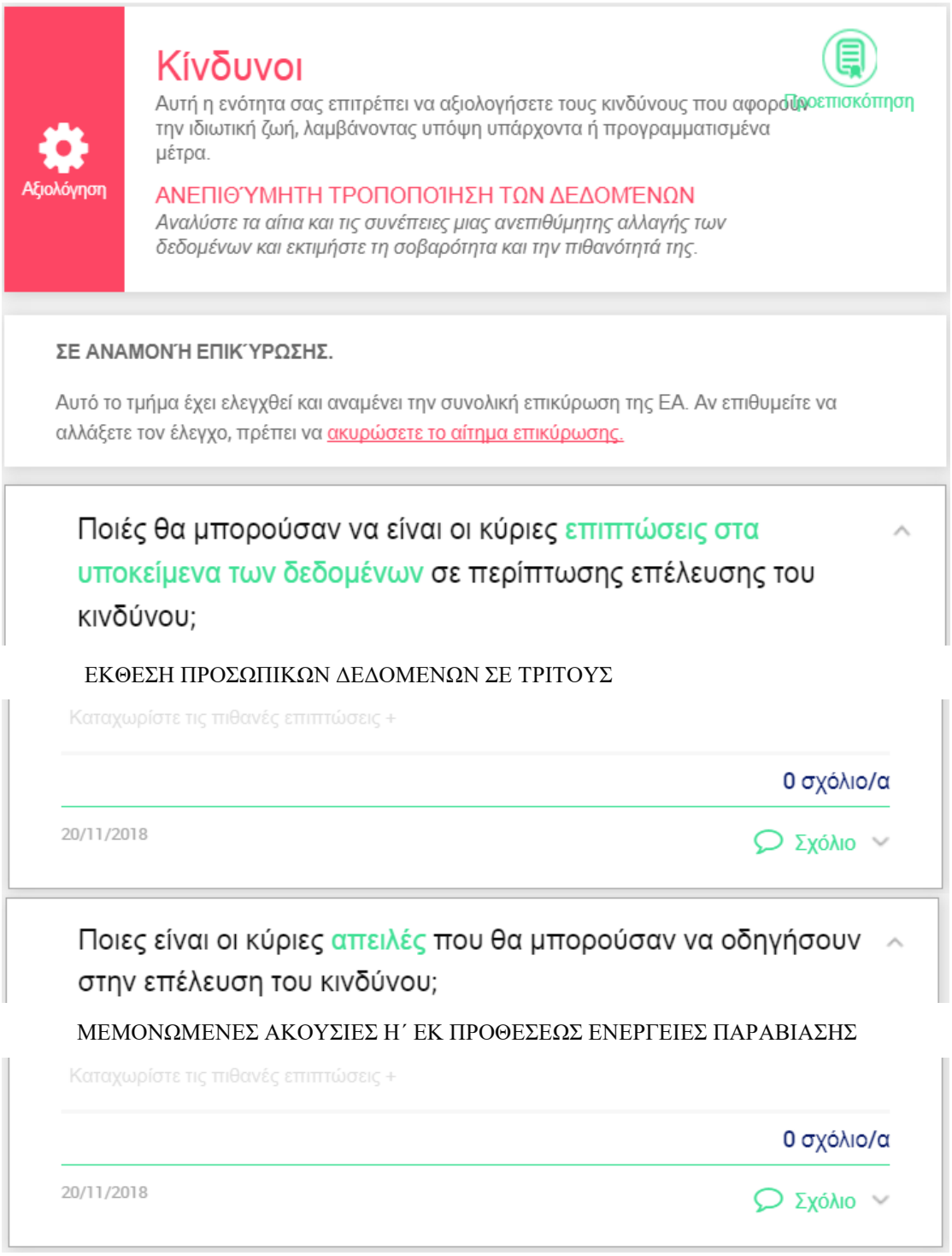
Η ΜΗ ΤΗΡΗΣΗ ΕΓΚΕΚΡΙΜΕΝΩΝ ΜΗΧΑΝΙΣΜΩΝ- ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΘΙΣΤΟΥΝ "ΣΗΜΑΝΤΙΚΟ" ΤΟΝ ΠΑΡΑΓΟΝΤΑ "ΣΟΒΑΡΟΤΗΤΑ ΚΙΝΔΥΝΟΥ" ΔΕΔΟΜΕΝΟΥ ΟΤΙ ΤΑ ΥΠΟΚΕΙΜΕΝΑ ΕΝΔΕΧΕΤΑΙ ΝΑ ΑΝΤΙΜΕΤΩΠΙΣΟΥΝ ΣΗΜΑΝΤΙΚΕΣ ΥΛΙΚΕΣ ΚΑΙ ΗΘΙΚΕΣ ΣΥΝΕΠΕΙΕΣ.

0 σχόλιο/α

20/11/2018 Σχόλιο


Πώς υπολογίζετε την πιθανότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;
(Απροσδιόριστο)
Αμελητέο
Περιορισμένο
Σημαντικό
Μέγιστο
Η ΚΑΘΗΜΕΡΙΝΗ ΕΠΕΞΕΡΓΑΣΙΑ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΣΥΧΝΑ ΒΡΙΣΚΕΤΑΙ ΑΝΤΙΜΕΤΩΠΗ ΜΕ ΑΠΕΙΛΕΣ ΠΑΡΑΒΙΑΣΗΣ ΤΟΥΣ ΠΑΡΑ ΤΑ ΑΥΞΗΜΕΝΑ ΚΑΙ ΣΥΝΕΧΩΣ ΕΠΙΤΗΡΟΥΜΕΝΑ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ.
0 σχόλιο/α
20/11/2018
Σχόλιο

Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Το υποτμήμα ελέγχθηκε, σε αναμονή τελικής επικύρωσης
Όλα τα πεδία πρέπει να συμπληρωθούν
Ακύρωση αιτήματος επικύρωσης
« Προγραμματισμένα ή υπάρχοντα μέτρα
Ανεπιθύμητη τροποποίηση των δεδομένων »


Αξιολόγηση
Κίνδυνοι
Αυτή η ενότητα σας επιτρέπει να αξιολογήσετε τους κινδύνους που αφορούν την ιδιωτική ζωή, λαμβάνοντας υπόψη υπάρχοντα ή προγραμματισμένα μέτρα.
Προεπισκόπηση
ΑΝΕΠΙΘΎΜΗΤΗ ΤΡΟΠΟΠΟΊΗΣΗ ΤΩΝ ΔΕΔΟΜΈΝΩΝ
Αναλύστε τα αίτια και τις συνέπειες μιας ανεπιθύμητης αλλαγής των δεδομένων και εκτιμήστε τη σοβαρότητα και την πιθανότητά της.
ΣΕ ΑΝΑΜΟΝΉ ΕΠΙΚΎΡΩΣΗΣ.
Αυτό το τμήμα έχει ελεγχθεί και αναμένει την συνολική επικύρωση της ΕΑ. Αν επιθυμείτε να αλλάξετε τον έλεγχο, πρέπει να ακυρώσετε το αίτημα επικύρωσης.
Ποιές θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα των δεδομένων σε περίπτωσης επέλευσης του κινδύνου;
ΕΚΘΕΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΟΥΣ
Καταχωρίστε τις πιθανές επιπτώσεις +
0 σχόλιο/α
20/11/2018
Σχόλιο
Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;
ΜΕΜΟΝΩΜΕΝΕΣ ΑΚΟΥΣΙΕΣ Η΄ ΕΚ ΠΡΟΘΕΣΕΩΣ ΕΝΕΡΓΕΙΕΣ ΠΑΡΑΒΙΑΣΗΣ
Καταχωρίστε τις πιθανές επιπτώσεις +
0 σχόλιο/α
20/11/2018
Σχόλιο

Ποιές είναι οι πηγές κινδύνου;

1) ΚΑΚΟΒΟΥΛΟΣ ΥΠΑΛΛΗΛΟΣ ΠΟΥ ΑΞΙΟΠΟΙΕΙ ΤΗ ΠΡΟΣΒΑΣΗ ΤΟΥ ΣΤΟ ΣΥΣΤΗΜΑ
2) ΑΜΕΛΗΣ ΥΠΑΛΛΗΛΟΣ ΠΟΥ ΔΕΝ ΑΝΤΙΛΑΜΒΑΝΕΤΑΙ ΤΗ ΠΡΑΞΗ ΤΟΥ ΣΤΗ ΠΡΟΣΠΑΘΕΙΑ ΝΑ ΕΞΥΠΗΡΕΤΗΣΕΙ
3) ΣΦΑΛΜΑ, ΔΟΛΟΣ, ΚΑΤΑΣΚΟΠΕΙΑ ΚΑΙ ΑΔΕΞΙΟΤΗΤΑ ΥΠΑΛΛΗΛΟΥ
4) HACKING

Καταχωρίστε τις πιθανές επιπτώσεις +

0 σχόλιο/α

20/11/2018

Σχόλιο

Ποιά από τα προσδιορισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

ΡΥΘΜΙΣΤΙΚΟ ΛΟΓΙΚΗΣ ΠΡΟΣΒΑΣΗΣ, ΑΝΙΧΝΕΥΣΙΜΟΤΗΤΑ (ΚΑΤΑΓΡΑΦΗ), ΈΛΕΓΧΟΣ ΦΥΣΙΚΗΣ ΠΡΟΣΒΑΣΗΣ, ΑΣΦΑΛΕΙΑ ΕΓΓΡΑΦΩΝ, ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΤΩΝ ΜΕΤΡΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ, ΛΕΙΤΟΥΡΓΙΚΗ ΑΣΦΑΛΕΙΑ.

Καταχωρίστε τις πιθανές επιπτώσεις +

0 σχόλιο/α

20/11/2018

Σχόλιο

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

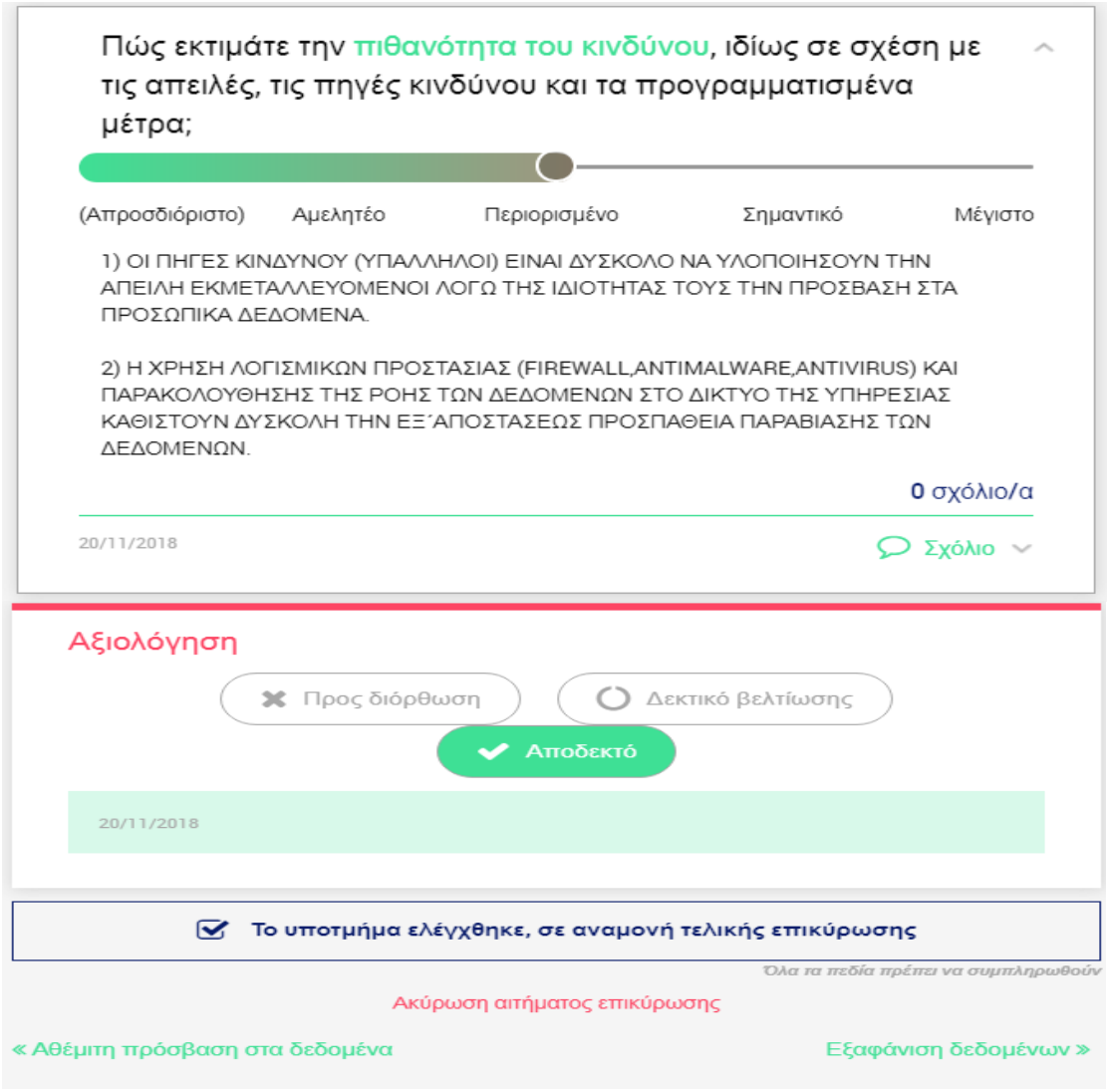
(Απροσδιόριστο) Αμελητέο Περιορισμένο Σημαντικό Μέγιστο

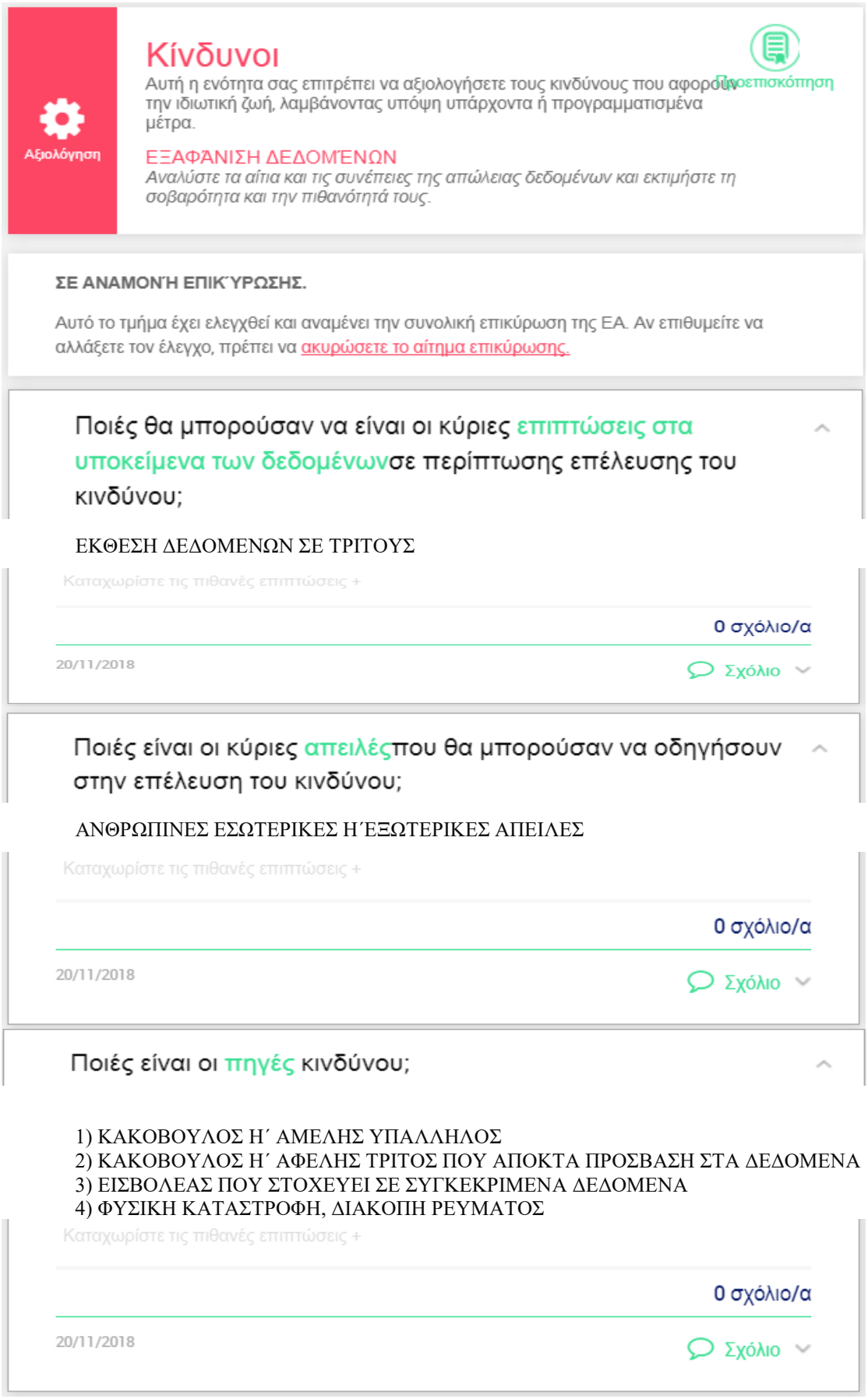
ΤΟ ΜΕΓΕΘΟΣ ΤΟΥ ΚΙΝΔΥΝΟΥ ΣΕ ΤΥΧΟΝ ΑΝΕΠΙΘΥΜΗΤΗ ΤΡΟΠΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ ΧΑΡΑΚΤΗΡΙΖΕΤΑΙ ΩΣ ΜΕΓΙΣΤΟ ΔΙΟΤΙ ΤΑ ΥΠΟΚΕΙΜΕΝΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΕΝΔΕΧΕΤΑΙ ΝΑ ΑΝΤΙΜΕΤΩΠΙΣΟΥΝ ΣΗΜΑΝΤΙΚΕΣ ΥΛΙΚΕΣ ΚΑΙ ΗΘΙΚΕΣ ΣΥΝΕΠΕΙΕΣ

0 σχόλιο/α

20/11/2018

Σχόλιο


Πώς εκτιμάτε την πιθανότητα του κινδύνου, ιδίως σε σχέση με τις απειλές, τις πηγές κινδύνου και τα προγραμματισμένα μέτρα;
(Απροσδιόριστο)
Αμελητέο
Περιορισμένο
Σημαντικό
Μέγιστο
1) ΟΙ ΠΗΓΕΣ ΚΙΝΔΥΝΟΥ (ΥΠΑΛΛΗΛΟΙ) ΕΙΝΑΙ ΔΥΣΚΟΛΟ ΝΑ ΥΛΟΠΟΙΗΣΟΥΝ ΤΗΝ ΑΠΕΙΛΗ ΕΚΜΕΤΑΛΛΕΥΟΜΕΝΟΙ ΛΟΓΩ ΤΗΣ ΙΔΙΟΤΗΤΑΣ ΤΟΥΣ ΤΗΝ ΠΡΟΣΒΑΣΗ ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ.
2) Η ΧΡΗΣΗ ΛΟΓΙΣΜΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ (FIREWALL,ANTIMALWARE,ANTIVIRUS) ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΤΗΣ ΡΟΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΚΤΥΟ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΚΑΘΙΣΤΟΥΝ ΔΥΣΚΟΛΗ ΤΗΝ ΕΞΑΠΟΣΤΑΣΕΩΣ ΠΡΟΣΠΑΘΕΙΑ ΠΑΡΑΒΙΑΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ.
0 σχόλιο/α
20/11/2018
Σχόλιο
Αξιολόγηση
Προς διόρθωση
Δεκτικό βελτίωσης
Αποδεκτό
20/11/2018
Το υποτμήμα ελέγχθηκε, σε αναμονή τελικής επικύρωσης
Όλα τα πεδία πρέπει να συμπληρωθούν
Ακύρωση αιτήματος επικύρωσης
« Αθέμιτη πρόσβαση στα δεδομένα
Εξαφάνιση δεδομένων »


Αξιολόγηση
Κίνδυνοι
Αυτή η ενότητα σας επιτρέπει να αξιολογήσετε τους κινδύνους που αφορούν την ιδιωτική ζωή, λαμβάνοντας υπόψη υπάρχοντα ή προγραμματισμένα μέτρα.
Προεπισκόπηση
ΕΞΑΦΆΝΙΣΗ ΔΕΔΟΜΈΝΩΝ
Αναλύστε τα αίτια και τις συνέπειες της απώλειας δεδομένων και εκτιμήστε τη σοβαρότητα και την πιθανότητά τους.
ΣΕ ΑΝΑΜΟΝΉ ΕΠΙΚΎΡΩΣΗΣ.
Αυτό το τμήμα έχει ελεγχθεί και αναμένει την συνολική επικύρωση της ΕΑ. Αν επιθυμείτε να αλλάξετε τον έλεγχο, πρέπει να ακυρώσετε το αίτημα επικύρωσης.
Ποιές θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα των δεδομένωνσε περίπτωσης επέλευσης του κινδύνου;
ΕΚΘΕΣΗ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΟΥΣ
Καταχωρίστε τις πιθανές επιπτώσεις +
0 σχόλιο/α
20/11/2018
Σχόλιο
Ποιές είναι οι κύριες απειλέςπου θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;
ΑΝΘΡΩΠΙΝΕΣ ΕΣΩΤΕΡΙΚΕΣ Η΄ΕΞΩΤΕΡΙΚΕΣ ΑΠΕΙΛΕΣ
Καταχωρίστε τις πιθανές επιπτώσεις +
0 σχόλιο/α
20/11/2018
Σχόλιο
Ποιές είναι οι πηγές κινδύνου;
1) ΚΑΚΟΒΟΥΛΟΣ Η΄ ΑΜΕΛΗΣ ΥΠΑΛΛΗΛΟΣ
2) ΚΑΚΟΒΟΥΛΟΣ Η΄ ΑΦΕΛΗΣ ΤΡΙΤΟΣ ΠΟΥ ΑΠΟΚΤΑ ΠΡΟΣΒΑΣΗ ΣΤΑ ΔΕΔΟΜΕΝΑ
3) ΕΙΣΒΟΛΕΑΣ ΠΟΥ ΣΤΟΧΕΥΕΙ ΣΕ ΣΥΓΚΕΚΡΙΜΕΝΑ ΔΕΔΟΜΕΝΑ
4) ΦΥΣΙΚΗ ΚΑΤΑΣΤΡΟΦΗ, ΔΙΑΚΟΠΗ ΡΕΥΜΑΤΟΣ
Καταχωρίστε τις πιθανές επιπτώσεις +
0 σχόλιο/α
20/11/2018
Σχόλιο

Ποιά από τα προσδιορισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

ΈΛΕΓΧΟΣ ΦΥΣΙΚΗΣ ΠΡΟΣΒΑΣΗΣ, ΑΝΙΧΝΕΥΣΙΜΟΤΗΤΑ (ΚΑΤΑΓΡΑΦΗ), ΣΥΝΤΗΡΗΣΗ, ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΠΗΓΕΣ ΚΙΝΔΥΝΩΝ ΠΛΗΝ ΤΟΥ ΑΝΘΡΩΠΟΥ, ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ, ΛΕΙΤΟΥΡΓΙΚΗ ΑΣΦΑΛΕΙΑ, ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Καταχωρίστε τις πιθανές επιπτώσεις +

0 σχόλιο/α

20/11/2018

Σχόλιο

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

(Απροσδιόριστο) Αμελητέο Περιορισμένο Σημαντικό Μέγιστο

ΤΟ ΕΠΙΠΕΔΟ ΣΟΒΑΡΟΤΗΤΑΣ ΤΟΥ ΚΙΝΔΥΝΟΥ ΧΑΡΑΚΤΗΡΙΖΕΤΑΙ ΩΣ "ΜΕΓΙΣΤΟ" ΔΙΟΤΙ ΤΥΧΟΝ ΟΡΙΣΤΙΚΗ ΑΠΩΛΕΙΑ ΔΕΔΟΜΕΝΩΝ ΘΑ ΣΗΜΑΙΝΕΙ ΤΗΝ ΠΑΤΑΓΩΔΗ ΑΠΟΤΥΧΙΑ ΤΩΝ ΜΕΤΡΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ.

0 σχόλιο/α

20/11/2018

Σχόλιο

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

(Απροσδιόριστο) Αμελητέο Περιορισμένο Σημαντικό Μέγιστο

1) ΤΟΣΟ ΟΙ ΥΠΑΛΛΗΛΟΙ ΟΣΟ ΚΑΙ ΟΙ ΣΥΝΑΛΛΑΣΣΟΜΕΝΟΙ ΠΟΛΙΤΕΣ, ΕΙΝΑΙ ΔΥΣΚΟΛΟ ΝΑ ΥΛΟΠΟΙΗΣΟΥΝ ΤΗΝ ΣΥΓΚΕΚΡΙΜΕΝΗ ΑΠΕΙΛΗ ΕΚΜΕΤΑΛΛΕΥΟΜΕΝΟΙ ΤΗΝ ΠΡΟΣΒΑΣΗ ΤΟΥΣ ΣΤΟ ΣΥΣΤΗΜΑ Η΄ΤΗΝ ΕΓΓΥΤΗΤΑ ΤΟΥΣ ΣΤΟ ΧΩΡΟ (ΚΛΟΠΗ ΕΓΓΡΑΦΩΝ) ΑΝΤΙΣΤΟΙΧΑ.

2) Η ΧΡΗΣΗ ΛΟΓΙΣΜΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ (FIREWALL,ANTIMALWARE,ANTIVIRUS) ΚΑΙ Η ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΤΗΣ ΡΟΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΚΤΥΟ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΚΑΘΙΣΤΟΥΝ ΔΥΣΚΟΛΗ ΤΗΝ ΕΞ΄ΑΠΟΣΤΑΣΕΩΣ ΠΡΟΣΠΑΘΕΙΑ ΔΙΑΓΡΑΦΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ.

3) ΚΑΘΗΜΕΡΙΝΟ ONLINE DATABASE BACKUP, ΑΛΛΑ ΚΑΙ ΣΥΝΟΛΙΚΟ DATABASE BACKUP ΜΕΤΑ ΤΟ ΠΕΡΑΣ ΤΟΥ ΩΡΑΡΙΟΥ ΔΙΑΣΦΑΛΙΖΕΙ ΤΗ ΤΗΡΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΑΚΟΜΑ ΚΑΙ ΣΕ ΠΕΡΙΠΤΩΣΗ ΟΡΙΣΤΙΚΗΣ ΔΙΑΓΡΑΦΗΣ.

0 σχόλιο/α

20/11/2018

Σχόλιο

Αξιολόγηση

Προς διόρθωση | Δεκτικό βελτίωσης | Αποδεκτό

20/11/2018

Το υποτμήμα ελέγχθηκε, σε αναμονή τελικής επικύρωσης

Όλα τα πεδία πρέπει να συμπληρωθούν

Ακύρωση αιτήματος επικύρωσης

« Ανεπιθύμητη τροποποίηση των δεδομένων

Επιθεώρηση κινδύνων »

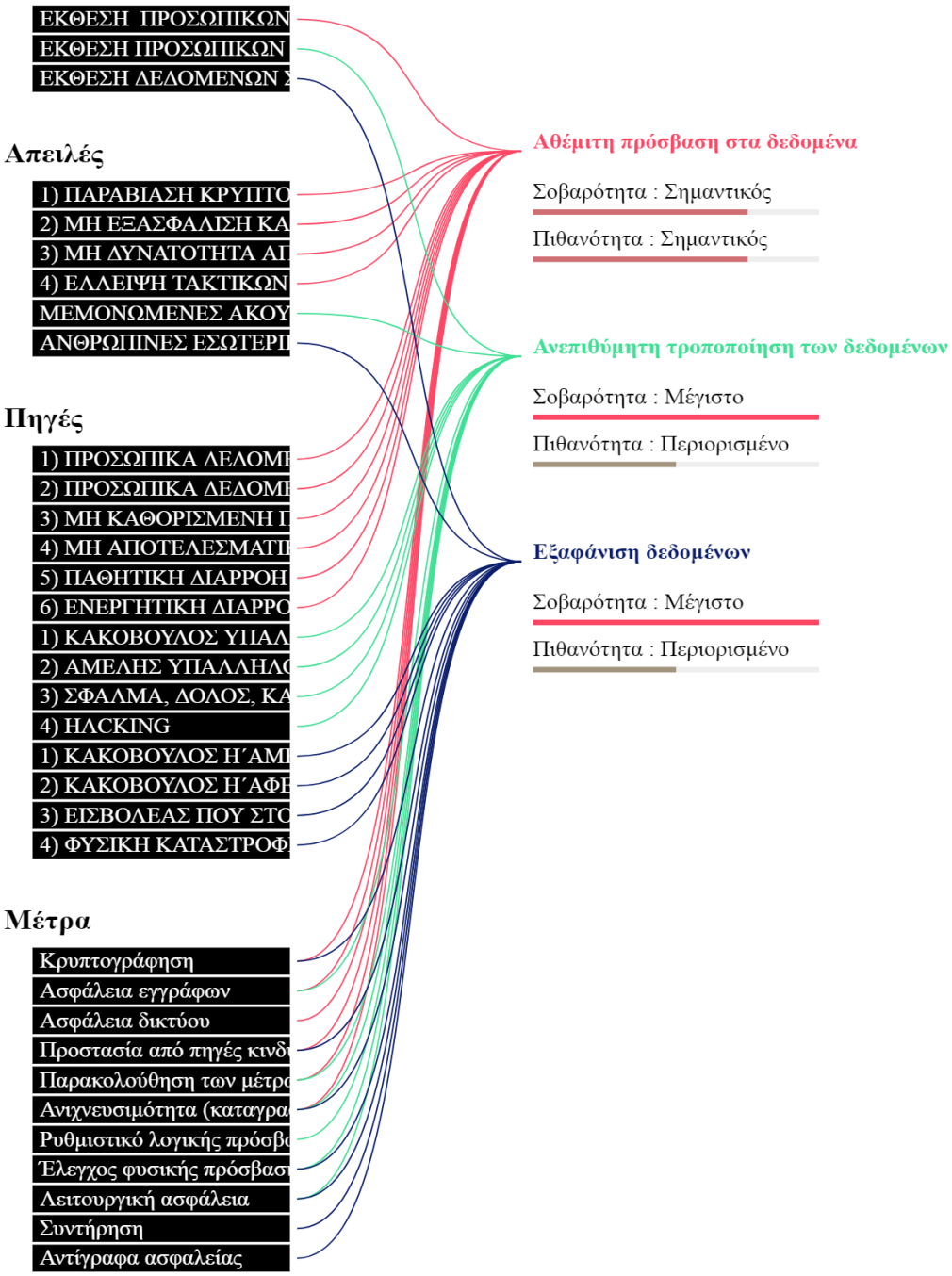
Κίνδυνοι

Προεπισκόπηση

Αυτή η ενότητα σας επιτρέπει να αξιολογήσετε τους κινδύνους που αφορούν την ιδιωτική ζωή, λαμβάνοντας υπόψη υπάρχοντα ή προγραμματισμένα μέτρα.

ΕΠΙΘΕΩΡΗΣΗ ΚΙΝΔΥΝΩΝ

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



« Εξαφάνιση δεδομένων

Χαρτογράφηση κινδύνων »

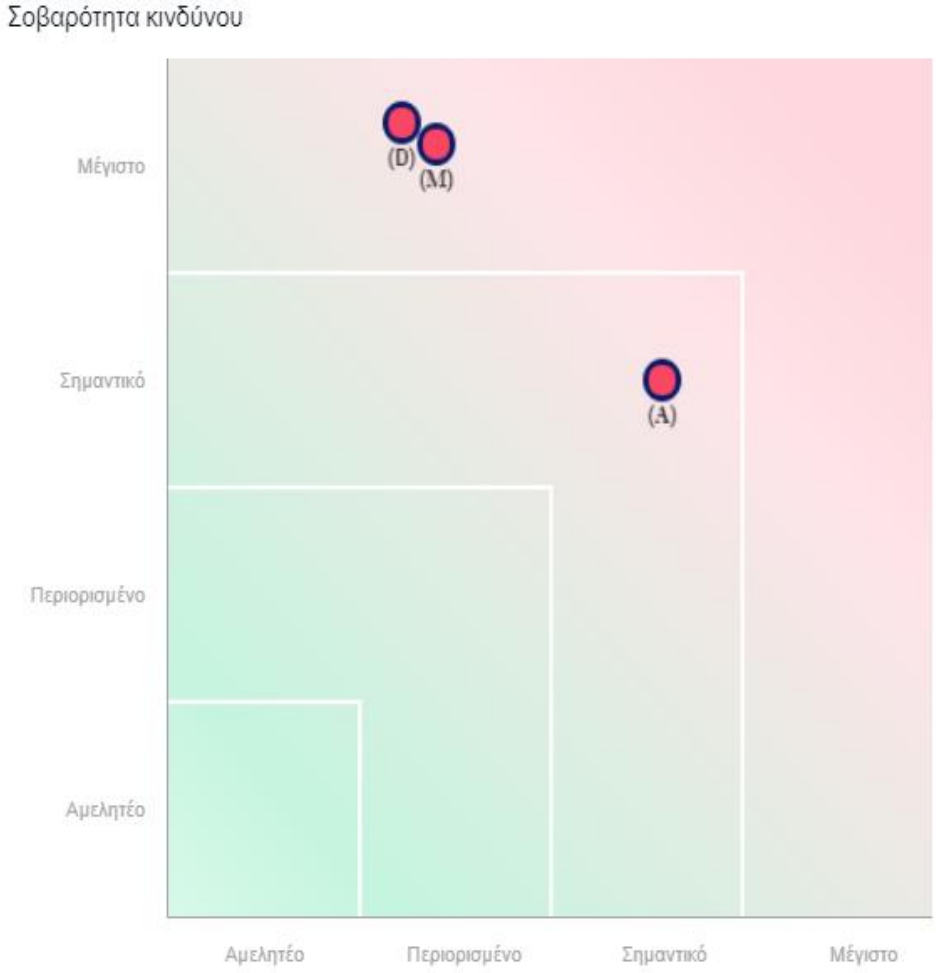
Επικύρωση

Προεπισκόπηση

Αυτή η ενότητα σας επιτρέπει να προετοιμάσετε και να επισημοποιήσετε την επικύρωση της ΕΑ.

ΧΑΡΤΟΓΡΆΦΗΣΗ ΚΙΝΔΎΝΩΝ

Αυτή η απεικόνιση σας επιτρέπει να έχετε μια συνολική και συνθετική άποψη των κινδύνων, πριν και μετά την εφαρμογή των συμπληρωματικών μέτρων.



- Προγραμματισμένα ή υπάρχοντα μέτρα
- Με εφαρμοσμένα τα διορθωτικά μέτρα
- (A)θέμιτη πρόσβαση στα προσωπικά δεδομένα
- (M)η επιθύμητη τροποποίηση των προσωπικών δεδομένων
- (E)ξαφάνιση προσωπικών δεδομένων

18/11/2018

« Επιθεώρηση κινδύνων

Σχέδιο δράσης »

Επικύρωση

Αυτή η ενότητα σας επιτρέπει να προετοιμάσετε και να επισημοποιήσετε την επικύρωση της ΕΑ.

Εμφάνιση σχεδίου δράσης

ΣΧΈΔΙΟ ΔΡΆΣΗΣ

Σχεδιάστε λεπτομερώς την εφαρμογή των πρόσθετων μέτρων που εντοπίστηκαν κατά τη διάρκεια της ΕΑ. Το σχέδιο δράσης ενημερώνεται αυτόματα κατά την αξιολόγηση των διαφόρων στοιχείων που περιλαμβάνονται στην ΕΑ.

Επισκόπηση

Θεμελιώδεις αρχές

- Σκοποί
- Νομική βάση
- Επαρκή δεδομένα
- Ακρίβεια δεδομένων
- Διάρκεια αποθήκευσης
- Πληροφορίες για τα υποκείμενα των δεδομένων
- Λήψη συγκατάθεσης
- Πληροφορίες για τα υποκείμενα των δεδομένων
- Δικαίωμα διόρθωσης και διαγραφής
- Δικαίωμα περιορισμού και εναντίωσης
- Υπεργολαβία
- Μεταφορές

Προγραμματισμένα ή υπάρχοντα μέτρα

- Κρυπτογράφηση
- Ρυθμιστικό λογικής πρόσβασης
- Ανιχνευσιμότητα (καταγραφή)
- Ασφάλεια εγγράφων
- Λειτουργική ασφάλεια
- Αντίγραφα ασφαλείας
- Συντήρηση
- Ασφάλεια δικτύου
- Έλεγχος φυσικής πρόσβασης
- Παρακολούθηση δραστηριότητας δικτύου
- Προστασία από πηγές κινδύνων πλην του ανθρώπου
- Οργάνωση της πολιτικής προστασίας προσωπικών δεδομένων
- Παρακολούθηση των μέτρων προστασίας δεδομένων

Κίνδυνοι

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

Μέτρα δεκτικά βελτίωσης
Μέτρα αποδεκτά

Θεμελιώδεις αρχές

Δεν καταγράφηκε κανένα σχέδιο δράσης.

Προγραμματισμένα ή υπάρχοντα μέτρα

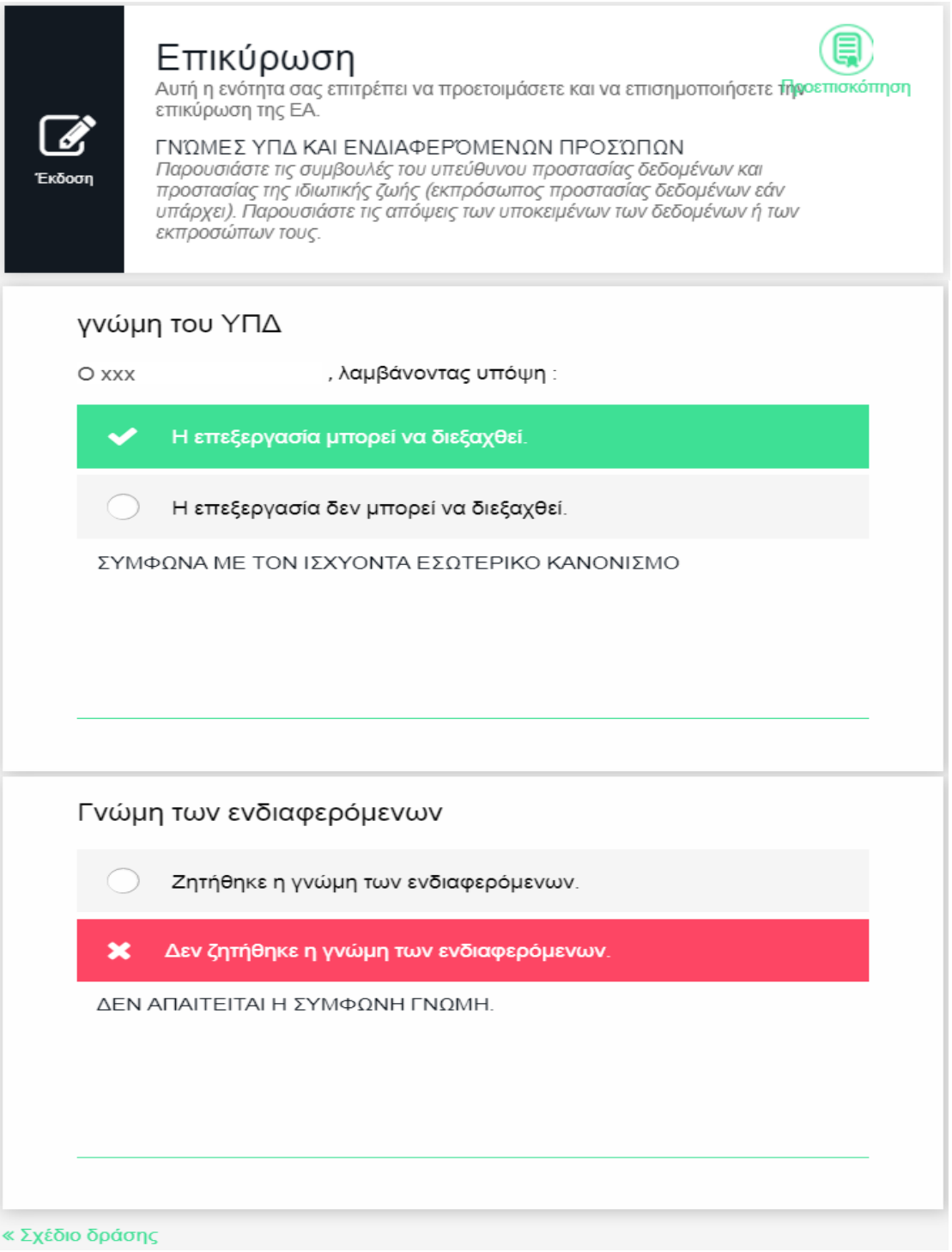
Δεν καταγράφηκε κανένα σχέδιο δράσης.

Κίνδυνοι

Δεν καταγράφηκε κανένα σχέδιο δράσης.

« Χαρτογράφηση κινδύνων

Γνώμες ΥΠΔ και ενδιαφερόμενων προσώπων »



« Σχέδιο δράσης

Συμπέρασμα

Αποτυπώνοντας τα αποτελέσματα της μελέτης περίπτωσης με την εφαρμογή του ανοικτού λογισμικού της CNIL, διαπιστώνουμε ότι, μέσω αυτού, επιχειρείται, με μεθοδικό και αποτελεσματικό τρόπο, η εισαγωγή της διαδικασίας έκδοσης πιστοποιητικών του Πρωτοδικείου Θεσσαλονίκης, στο νέο πλαίσιο προστασίας των δεδομένων. Συγκεκριμένα και σύμφωνα με την υποενότητα “Επιθεώρηση κινδύνων”, σε όλα τα επιμέρους στάδια επεξεργασίας, από την έντυπη κατάθεση αιτήσεων έκδοσης πιστοποιητικών έως και την ενημέρωση και αναζήτηση αυτών στην εφαρμογή, ενδέχεται να ελλοχεύουν κίνδυνοι με σημείο αναφοράς είτε την πιθανότητα εκδήλωσής τους η οποία κυμαίνεται από "Περιορισμένη" ως "Σημαντική", είτε τη σοβαρότητα εκδήλωσής τους η οποία κυμαίνεται από "Σημαντική" έως "Μέγιστη", στην υποενότητα, δε, "Χαρτογράφηση κινδύνων" παρατίθεται με τη μορφή διαγράμματος η συνολική εικόνα των κινδύνων, με άξονες τη "Σοβαρότητα" και τη "Πιθανότητα".

Στο "Σχέδιο δράσης" αποτυπώνεται με τον, πλέον, πρόσφορο τρόπο, ότι όλα τα τρέχοντα μέτρα που καταγράφηκαν κατά τη δημιουργία της PIA και που σχετίζονται με τις "Θεμελιώδεις αρχές", τα "Προγραμματισμένα μέτρα" και τους "Κινδύνους", χαρακτηρίζονται ως "Μέτρα Αποδεκτά", χωρίς, φυσικά, να αποκλείεται η προσθήκη βελτιωτικών παραμέτρων στα, ήδη, υπάρχοντα ή νέων μεθόδων διαχείρισης δεδομένων, οι οποίες και θα αποτελέσουν το μελλοντικό αντικείμενο ανάλυσης και σχεδιασμού των υπευθύνων στον τομέα της δικαιοσύνης. Και, τούτο, διότι η ΕΑΠΔ αποτελεί διαρκή διαδικασία και όχι μεμονωμένη, αυτοτελή πράξη.

Ιδιαίτερη μνεία, όμως, χρήζουν και τα οφέλη από την εκτέλεση και την ολοκλήρωση της εκτίμησης αντίκτυπου, τα οποία εντοπίζονται και διαμορφώνουν τόσο την εσωτερική όσο και την εξωτερική εικόνα του Τμήματος Έκδοσης Πιστοποιητικών του Πρωτοδικείου Θεσσαλονίκης, και ομαδοποιούνται ως εξής:

Εσωτερικά οφέλη όπως:

- διαχείριση των κινδύνων που περιλαμβάνει την αναγνώριση και τον περιορισμό τους
- αποφυγή πολυδάπανων επαναπροσδιορισμών της διαδικασίας επεξεργασίας, εάν, εκ προοιμίου, έχουν οριοθετηθεί οι ενδεχόμενοι κίνδυνοι και απειλές, σύμφωνα με τις αρχές της εξ’ ορισμού και της εκ σχεδιασμού προστασίας των

δεδομένων (άρθρο 35 παρ. 1 και 10, αιτιολογικές σκέψεις 90 και 93 σε συνδυασμό με το άρθρο 25 και αιτιολογική σκέψη 78).

- αποφυγή επιβολής κυρώσεων, στο πλαίσιο του κατασταλτικού ελέγχου, από την αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων, λόγω μη συμμόρφωσης με το Γενικό Κανονισμό
- βελτίωση του τρόπου διαχείρισης των δεδομένων, γνωρίζοντας τις πιθανές απειλές
- ενίσχυση και βελτίωση των μέτρων ασφαλείας σχετικά με την προστασία των δεδομένων
- βελτίωση της τεχνογνωσίας σε θέματα προστασίας και ασφάλειας των δεδομένων

και

Εξωτερικά οφέλη όπως:

- ενίσχυση της αξιοπιστίας του φορέα
- εναρμόνιση με τον Γενικό Κανονισμό

Ειδικότερα, η εφαρμογή του λογισμικού PIA, θα επιφέρει ένα νέο επίπεδο ασφάλειας, ακεραιότητας και διαφάνειας στη συλλογή, αποθήκευση και χρήση των προσωπικών δεδομένων που διαχειρίζεται το ανωτέρω Τμήμα του Πρωτοδικείου. Ως εκ τούτου, ένα νέο ρυθμιστικό πλαίσιο είναι απολύτως απαραίτητο, προκειμένου να θεσπιστούν οργανωτικά και τεχνολογικά μέτρα, που θα εξασφαλίζουν τη συμμόρφωση με τον Κανονισμό, ακόμη και αν απαιτούν, μια μικρή περίοδο προσαρμογής.

Η πολιτεία οφείλει να προβεί άμεσα σε μία ριζική επανεξέταση της επιχειρούμενης στρατηγικής της που αφορά τα προσωπικά δεδομένα, αλλά και να βελτιώσει νομοτεχνικά τις εσωτερικές διαδικασίες χειρισμού τους. Η μετάβαση στη νέα εποχή του GDPR, ειδικά στο χώρο της ψηφιακής δικαιοσύνης, θα πρέπει να περιλαμβάνει την πρόβλεψη και υλοποίηση όλων των απαιτούμενων παραμέτρων, ικανών για την επίλυση προβλημάτων αναφορικά με τις διαδικασίες και εφαρμογές καθώς και την κατάρτιση πολιτικής διαχείρισης των προσωπικών δεδομένων και της προστασίας αυτών, με στόχο να καταστεί το GDPR ένα δυναμικό εργαλείο, το οποίο θα συμβάλει καίρια στη διασφάλιση των δεδομένων των πολιτών.

Κεφάλαιο 4: Μεγάλα δεδομένα και ψηφιακό δικαστήριο

Εισαγωγή

Στη σύγχρονη ψηφιακή εποχή, η πολυεπίπεδη επενέργεια της ραγδαίας τεχνολογικής προόδου στον τομέα της δικαιοσύνης, αποτελεί μια παράμετρο μείζονος σημασίας για την υλοποίηση του ολοένα πιο επιτακτικού αιτήματος για "ψηφιακό δικαστήριο". Επιπτώσεις που σχετίζονται με νομικές μεταρρυθμίσεις, με οποιαδήποτε λεπτομερή εξέταση των τεχνικών διαδικασιών, του τύπου και της ποιότητας της συμμετοχής των πολιτών στο νέο ψηφιοποιημένο δικαστήριο αλλά και με την εξαγωγή θετικών πρόσημων, μέσω της βελτιωμένης πρόσβασης στη δικαιοσύνη.

Σ' ένα τέτοιο περιβάλλον, τα εργαλεία και τα συστήματα αποτελούν δυνητικά τα εχέγγυα για την αποτελεσματικότητα, τη συμμετοχή και την προσβασιμότητα, χωρίς να παραβλέπει κανείς την πιθανότητα αλλοίωσης βασικών αρχών του δικανικού συστήματος.

Σε μία πρώιμη προσπάθεια να προδιαγράψουμε τον τρόπο με τον οποίο η χρήση της τεχνολογίας των μεγάλων δεδομένων θα μεταμορφώσει τον τρόπο λειτουργίας της δικαιοσύνης, καταλήξαμε ότι για τη ριζική αναδιάρθρωση του ψηφιακού δικαστηρίου, απαιτείται η εισαγωγή πολυάριθμων τεχνολογικών καινοτομιών, όπως η εφαρμογή καθολικής ηλεκτρονικής κατάθεσης, η ψηφιοποίηση αρχείων, η ενσωμάτωση συστημάτων διαχείρισης και καταγραφής ήχου καθώς και η ανάπτυξη ηλεκτρονικών συστημάτων υποστήριξης των ακροαματικών διαδικασιών.

Δεδομένου ότι στο χώρο της δικαιοσύνης πρέπει να αντανακλάται η πρόοδος της κοινωνίας, όσον αφορά την αξιοποίηση της τεχνολογικής προόδου, εντούτοις η αυτοματοποίηση μεγάλου όγκου δεδομένων και η αυξανόμενη επικράτηση των ψηφιακών εφαρμογών, εγείρει κρίσιμα ζητήματα.

Ειδικότερα, έχουν καταγραφεί διάφορες απόψεις αναφορικά με την τεράστια "αξία" της λογικής των Big Data, με κοινό σημείο τη μέγιστη συμβολή τους στην επίλυση διαχρονικών προβλημάτων. Σε τί ακριβώς συνίσταται αυτή; Κατά κύριο λόγο, στην επιτάχυνση της απονομής δικαιοσύνης [24], στο μέτρο που επηρεάζεται από αμιγώς εξωγενείς λειτουργικούς παράγοντες. Σε καμία περίπτωση, η έλευση των Big Data δε συνεπάγεται την υποκατάσταση του ρόλου του φυσικού δικαστή, αλλά, αντίθετα, αποτελεί χρήσιμο εργαλείο, εφόσον δεν παραβιάζονται θεμελιώδεις δικανικές αρχές.

Η συζήτηση για την εισαγωγή νέων τεχνολογιών στον τομέα της δικαιοσύνης, έχει εγείρει έντονες επιφυλάξεις οι οποίες σχετίζονται με τη χρήση και επεξεργασία τους, την ψηφιακή πνευματική ιδιοκτησία, την ασφάλεια, τα ανθρώπινα δικαιώματα και τη δεοντολογική συμμόρφωση στο γενικό κανονισμό για την προστασία των προσωπικών δεδομένων. Μ' αυτό τον τρόπο, διαμορφώνεται ένα προφίλ κινδύνου [25], ικανού να αποδομήσει το ευάλωτο δικαστικό σύστημα, στο μέτρο που δε θα προβλεφθεί η επαρκής προστασία του, μέσω κρυπτογράφησης, επαλήθευσης των στοιχείων ταυτότητας των χρηστών και συστήματος ανάκτησης των δεδομένων.

Αδιαμφισβήτητα, το εύρος των δεδομένων δημιουργεί προκλήσεις και στον τομέα της ασφάλειας, αναδεικνύοντάς τον, σε μείζονα προτεραιότητα, με απώτερο σκοπό την παροχή υπηρεσιών με διαφάνεια και ακεραιότητα προς τους τελικούς χρήστες. Για το λόγο αυτό ως αναγκαία συνθήκη προτείνεται ο σχεδιασμός κατάλληλων πολιτικών ασφαλείας, οι οποίες θα εξυπηρετούν τις ολοένα αυξανόμενες απαιτήσεις όσων αναζητούν πρόσβαση σε πληροφορίες.

Μέσα από αυτή τη θεωρητική προσέγγιση, διαπιστώνουμε ότι έχουν ωριμάσει οι συνθήκες για το λεγόμενο "ψηφιακό δικαστήριο", με τη χρήση των Big Data. Δεδομένου ότι υπάρχει, πλέον, διαθέσιμη τεχνολογία και εργαλεία που επιτρέπουν την πλήρη αξιοποίηση τους, ειδικά στη λήψη αποφάσεων, αντιλαμβάνεται κανείς τα πολλαπλά οφέλη που παρέχουν. Μέσω της επεξεργασίας του τεράστιου όγκου πληροφοριών, επιτυγχάνεται η άμεση κατηγοριοποίηση, ο συσχετισμός και ο εντοπισμός των χρήσιμων δεδομένων, ενώ θα πρέπει να σημειωθεί ότι η "ορθή" χρήση τους δε στηρίζεται, αποκλειστικά και μόνο, στην ανάπτυξη μιας τεχνολογίας ή ενός λογισμικού.

4.1 Ψηφιακή τεχνολογία και δικαστήριο

Τις τελευταίες δύο δεκαετίες, πολλοί έχουν επιδιώξει να ενσωματώσουν και να επεκτείνουν τις διαδικασίες στην ψηφιακή δικαιοσύνη [8], με σκοπό την ουσιαστική μεταμόρφωση των δικαστικών πρακτικών και το μεγαλύτερο ορθολογισμό των δαπανών. Η χρήση της τεχνολογίας στο ακροατήριο περιλαμβάνει κάθε σύστημα ή μέθοδο που χρησιμοποιείται με τη μορφή ηλεκτρονικού εξοπλισμού με σκοπό να προσφέρει ένα σαφές όφελος στη δικαστική διαδικασία. Κατά συνέπεια, ο προσδιορισμός της "επιτυχίας" με τον εκσυγχρονισμό του δικαστηρίου, ασχολείται, κατά κύριο λόγο, με την ποσοτικοποίηση του οικονομικού αντισταθμίσματος που συνδέεται με τη μείωση της παραδοσιακής κατανομής πόρων και την αναπροσαρμογή των δικαστικών πρακτικών και διαδικασιών.

4.2 Αποτελέσματα - συγκρίσεις

Οι αξιοσημείωτες τεχνολογικές εξελίξεις [28], όπως έχουν, ήδη, αναπτυχθεί, επιδρούν αποφασιστικά στον τρόπο αποθήκευσης, διαχείρισης και επεξεργασίας των δεδομένων. Ως καταλυτικός παράγοντας της διαδικασίας, αναδεικνύεται η ταχύτητα, η οποία εξαρτάται άμεσα από τους υπολογιστικούς πόρους των διαθέσιμων υποδομών όπως μνήμη, επεξεργαστική ισχύς, αποθηκευτικές λύσεις και δικτυακός εξοπλισμός. Ειδικότερα, η απαίτηση των Big Data για περισσότερο αποθηκευτικό χώρο, δεν παρουσιάζεται ως μία στατική κατάσταση αλλά θα πρέπει να προβλέπεται δυνατότητα επέκτασης ανάλογα με το διαχειρίσιμο όγκο και ταυτόχρονη ευελιξία στην πρόσβαση των διαθέσιμων πληροφοριών, χωρίς επιβάρυνση του λειτουργικού συστήματος. Επομένως, για την εξαγωγή των μέγιστων δυνατών αποτελεσμάτων σε επίπεδο διαχείρισης δεδομένων, απαιτείται η υποστήριξη υποδομής με δυνατότητα χαμηλής χρονικής καθυστέρησης (latency) και δυναμικών δομών αρχειοθέτησης και οργάνωσης.

Η κατάλληλη χρήση της τεχνολογίας για την προβολή ή αναπαραγωγή αποδεικτικών στοιχείων, πρόκειται να αλλάξει τη δυναμική της δικαιοσύνης με τον πλέον παραγωγικό και αποτελεσματικό τρόπο, καθώς μπορεί να αυξήσει τις δυνατότητες ελέγχου της διαδικασίας, να θέσει χρονικά όρια που σχετίζονται με τη λήψη αποφάσεων και να αυξήσει την αίσθηση της συμμετοχής όλων των εμπλεκομένων, βελτιώνοντας την κατανόηση των γεγονότων. Μολονότι, πολλές φορές, χρησιμοποιούνται αποδεικτικά στοιχεία για επεξηγηματικούς ή ουσιαστικούς σκοπούς, η πολυπλοκότητά τους δεν ανταποκρίνεται στις προσδοκίες που υπαγορεύουν σήμερα οι ακροαματικές διαδικασίες, διότι εστιάζουν:

- στη συνεχή ανάγκη για οπτικό κίνητρο αλλά και ενίσχυση του λεκτικού περιεχομένου της διαδικασίας.
- στην ενίσχυση της υπερασπιστικής ή κατηγορητικής γραμμής των δικηγόρων και
- στην ολοένα αυξανόμενη απαίτηση, υπαλλήλων, μαρτύρων, κατηγορουμένων και ενόρκων για χρήση μέσων τεχνολογίας.

Ως εκ τούτου, η ενσωμάτωση της σύγχρονης ψηφιακής τεχνολογίας στην δικαστική αίθουσα, επιτρέπει την εμπεριστατωμένη ανάλυση του συνόλου των πληροφοριών, διευκολύνοντας το έργο της σύνθεσης του δικαστηρίου για την κατανόηση της υπόθεσης, παρέχοντας περισσότερη ευελιξία και συμβάλλοντας στην αποτελεσματικότερη δικαστική διαδικασία.

Στα πλαίσια της παρούσας μελέτης και προς εξαγωγή ασφαλών συμπερασμάτων, επιχειρήθηκε η καταγραφή απόψεων, συναφών με το υπό διερεύνηση ζήτημα, προκειμένου να διαπιστωθούν τα σημεία σύγκλισης και απόκλισης σε ένα από τα πλέον διευρυμένα πεδία, αυτό της χρήσης των Big Data στις δικαστικές διαδικασίες.

Συγκρίνοντας την επιχειρηματολογία των επιλεγέντων αρθρογράφων, παρατηρούμε (πίνακας 4-1) ότι δεν υπάρχει κοινή γραμμή για το σύνολο των προβλημάτων, τα οποία δυνητικά θεραπεύονται, με τη χρήση των Big Data. Εστιάζουν σε προοπτικές, οι οποίες ανοίγονται στον τομέα της δικαιοσύνης, διατυπώνουν σκέψεις και καταλήγουν στην ανάγκη για διευρυμένη και ουσιαστική ενσωμάτωση της λογικής των μεγάλων δεδομένων, κατά την απαιτούμενη αναδιοργάνωση των δομών του δικαστηρίου.

Ειδικότερα και υπό την προϋπόθεση της χρήσης των Big Data, η συντριπτική πλειοψηφία διαπραγματεύεται ως κυρίαρχο θέμα την ανάλυση του όγκου των δεδομένων σε συνδυασμό με το δικαίωμα πρόσβασης των εμπλεκομένων σ' αυτά [13]. Στην πιο τεχνοκρατική προσέγγιση, αναδεικνύεται η γραφειοκρατία και το λειτουργικό κόστος των παρεχόμενων υπηρεσιών, ως μείζον πρόβλημα. Οι πιο θεωρητικοί υπεραμύνονται της διατήρησης της θέσης του φυσικού δικαστή, προκειμένου να διατηρηθεί αναλλοίωτος ο ρόλος του, κατά τη διεξαγωγή της δίκης. Το πολυσύνθετο του ζητήματος της ψηφιοποίησης της δικαιοσύνης, έρχεται στην επιφάνεια με τον, πλέον, εμφατικό τρόπο από την πλευρά των επιφυλακτικών, οι οποίοι προβάλλουν την απαίτηση για πολιτικές ασφάλειας, ως την πλέον αδιαμφισβήτητη δικλείδα για την "ορθή" χρήση των μεγάλων δεδομένων.

Μέσα από την εκτενή αναφορά των δυνατοτήτων των Big Data, διαπιστώνεται η ενδεχόμενη υπερβολική έκθεση των δικαστικών διαδικασιών σε κακόβουλους χειρισμούς, με αλυσιδωτές συνέπειες ακόμη και στον ευαίσθητο χώρο των προσωπικών δεδομένων. Στη σκέψη και μόνο, προκαλούνται έντονες αντιδράσεις όχι μόνο από μερίδα θεωρητικών αλλά και από αμιγώς τεχνοκρατικούς παράγοντες. Για όλα τα παραπάνω, με την παρούσα εργασία, κρίνεται επιβεβλημένη η ανάδειξη σε προτεραιότητα του τομέα της ασφάλειας, για λόγους τόσο δεοντολογίας όσο και διατήρησης του αδιάβλητου της δικαιοσύνης.

Στον παρακάτω πίνακα, παρουσιάζεται συνοπτικά ο βαθμός εστίασης των επιλεγμένων άρθρων, στα προβλήματα που αναζητούν επίλυση στην πορεία προς το

ψηφιακό δικαστήριο, μέσω της τεχνολογίας των Big Data, χρησιμοποιώντας τη κλίμακα H: High M: Medium και L: Low.

Πίνακας 4-1: Σύγκριση βαθμού ανάλυσης προβλημάτων

α/α	PAPERS	ΑΟΔ	ΓΡΑΦ	ΛΚ	ΕΑΔ	ΠΡΟΣΒ	ΡΟΛΟΣ ΔΙΚ	ΑΣΦ
1	Big Data Analytics.[16]	H		L	H	H		
2	Big Data and the Demand for Court and Legal Services [2]	H				H		
3	Courtroom Technology [10]			H			M	
4	The digital courtroom: Four key considerations for local authorities sharing court bundles electronically. [24]	L	H	H		H		H
5	The future of the courts [28]	H				H	M	
6	The Challenges facing Justice in the future: Judges confronted with the advent of Big Data Analytics [13]	H	L	L	L	M	H	
7	Revolutionize Judicial system and process [25]	H				H		H

H: High	ΑΟΔ: Ανάλυση Όγκου Δεδομένων
M: Medium	ΓΡΑΦ: Γραφειοκρατία
L: Low	ΛΚ: Λειτουργικό Κόστος
	ΕΑΔ: Επιβράδυνση Απονομής Δικαιοσύνης
	ΠΡΟΣΒ: Πρόσβαση των εμπλεκομένων στα δεδομένα
	ΡΟΛΟΣ ΔΙΚ: Υποκατάσταση ρόλου Δικαστή
	ΑΣΦ: Ασφάλεια δεδομένων

4.3 Προτάσεις υλοποίησης

Παρά τις πρώτες ανησυχίες σχετικά με τη χρήση του ηλεκτρονικού εξοπλισμού στη δικαστική αίθουσα [11],[14], ολοένα αυξάνονται οι φωνές που ζητούν τη πλήρη ψηφιοποίηση της διαδικασίας.

Βάσει των υφιστάμενων τεχνολογικών υποδομών, μία αίθουσα δικαστηρίου δυνητικά περιλαμβάνει τις παρακάτω παροχές:

- ✓ Η/Υ
- ✓ Συστήματα καταγραφής της ακροαματικής διαδικασίας

- ✓ Μικροφωνικές εγκαταστάσεις
- ✓ Πρόσβαση στο Διαδίκτυο μέσω σύνδεσης wi-fi
- ✓ Παρουσίαση αποδεικτικών στοιχείων μέσω βίντεο

Στόχος είναι όλες οι αίθουσες να είναι εξοπλισμένες με βασικές υποδομές ώστε να παρέχουν ψηφιακές υπηρεσίες, πλήρως εναρμονισμένες με τις ταχείς εξελίξεις στην τεχνολογία. Η ορθή χρήση της μπορεί να βοηθήσει και να υποστηρίξει την αποτελεσματική παρουσίαση της υπόθεσης στο δικαστήριο, όμως, δεν παύει να αποτελεί ένα εργαλείο που πρέπει να χρησιμοποιηθεί κατάλληλα καθώς από μόνο του, δεν μπορεί να μετατρέψει ένα χαμένο επιχείρημα σε κερδοφόρο, αλλά ούτε και θα αποκρύψει ή θα βελτιώσει την ανεπαρκή υπεράσπιση.

Η εισαγωγή σύγχρονων τεχνολογικών δυνατοτήτων και πρακτικών, πλέον των υφιστάμενων, περιλαμβάνει:

- **Στατικές εικόνες**

Ο πρώτος και ευκολότερος τύπος τεχνολογίας είναι οι στατικές εικόνες που προβάλλονται σε μεγάλη οθόνη από προβολικές συσκευές ή μέσω ηλεκτρονικού υπολογιστή. Η προβολή μπορεί να είναι γράφημα, διάγραμμα, αντικείμενο δύο ή τριών διαστάσεων ή φωτογραφία. Αυτός ο τύπος τεχνολογίας χρησιμοποιείται γενικά ως "αποδεικτικά" ή "επεξηγηματικά" στοιχεία και είναι μη αμφιλεγόμενος. Στη πιο διευρυμένη μορφή της, η τεχνολογία αυτή αποτελείται από στατικές εικόνες όπως γράμμα, συμβόλαιο, διάγραμμα, φωτογραφία, χάρτη οι οποίες αποθηκεύονται και προβάλλονται από έναν υπολογιστή, με ειδικές δυνατότητες σχολιασμού μέσω λογισμικού. Για παράδειγμα, μια παράγραφος μπορεί να διευρυνθεί ανάλογα με την υπόλοιπη σύμβαση ή μια συγκεκριμένη πρόταση της εν λόγω παραγράφου μπορεί να επισημανθεί με χρώμα. Η στατική εικόνα χρησιμοποιείται προκειμένου να δοθεί προσοχή σε σημαντικές πτυχές ενός εκθέματος. Η γραφική παρουσίαση των στοιχείων μέσω ενός προγράμματος ηλεκτρονικών υπολογιστών είναι πιο εντυπωσιακή και ευκρινής.

- **Animations**

Ένα δυναμικά κινούμενο σχέδιο είναι απλώς μια ακολουθία εικονογραφήσεων που όταν βιντεοσκοπηθεί δημιουργεί την ψευδαίσθηση ότι τα εικονογραφημένα αντικείμενα βρίσκονται σε κίνηση. Με τη χρήση των animations, δεν υπάρχει πρόθεση

να αναδημιουργηθεί ή να προσομοιωθεί ένα γεγονός, αλλά μια κινούμενη εικόνα αποτελεί ένα διαφορετικό αποδεικτικό μέσο μαρτυρίας. Αυτός ο τύπος στοιχείων που παράγονται από υπολογιστή, δεν παρουσιάζει ιδιαίτερα προβλήματα, για την αποδοχή του ως παραδεκτό στοιχείο.

- **Επαναδημιουργίες (Re-Creations)**

Οι επαναδημιουργίες είναι απλά δυναμικές κινούμενες εικόνες με την τεχνική έννοια του όρου, που παράγονται από έναν υπολογιστή αλλά η πηγή των δεδομένων εισόδου είναι διαφορετική και περισσότερο πολύπλοκη, εισάγοντας επιστημονικά δεδομένα ή δεδομένα κατόπιν συλλογής και έρευνας. Η είσοδος των δεδομένων δεν είναι απλώς μια περιγραφή ενός μάρτυρα σχετική με κάποιο γεγονός που βίωσε αλλά προσδιορίζονται και επιβεβαιώνονται συνολικά και ανεξάρτητα πριν αξιοποιηθούν. Στη συνέχεια, επεξεργάζονται από ειδικό λογισμικό το οποίο δημιουργεί μια εικόνα ή αποτέλεσμα αυτού που "πρέπει να έχει συμβεί" εισάγοντας όλες τις επιστημονικές παραμέτρους και υποθέσεις. Η παραγόμενη γενική εικόνα πρέπει να βασίζεται στην εγκυρότητα των δεδομένων εισόδου, στις επιστημονικές παραδοχές που έγιναν, στην αξιόπιστη εισαγωγή των πληροφοριών στο λογισμικό επεξεργασίας των δεδομένων, ώστε το τελικό αποτέλεσμα να μπορεί να χαρακτηριστεί ως "επαναδημιουργία" του γεγονότος που έχει συμβεί στο παρελθόν.

- **Προσομοιώσεις (simulations)**

Οι προσομοιώσεις είναι προβλέψιμες. Σκοπός αυτής είναι να δημιουργεί νέα στοιχεία από προϋπάρχοντα δεδομένα, με την εισαγωγή μαθηματικών τύπων ή άλλων επιστημονικών δεδομένων σε ένα υπολογιστή, έτσι ώστε ο υπολογιστής να μπορεί να δημιουργήσει ένα μοντέλο, βασιζόμενος στα δεδομένα και τις επιστημονικές υποθέσεις, για το τί πρέπει να έχει ή θα μπορούσε πραγματικά να συμβεί. Βασική διαφορά μεταξύ προσομοίωσης και επαναδημιουργίας ή κινούμενης εικόνας είναι ότι η πρώτη χρησιμοποιείται από ένα εμπειρογνώμονα για να καταλήξει στην άποψή του, ενώ η τελευταία χρησιμοποιείται για να απεικονίσει τη γνώμη του έτσι ώστε να μπορεί να είναι ορατή στο δικαστήριο. Ένας εμπειρογνώμονας βασίζει τη μαρτυρία της γνώμης του σε μια προσομοίωση, σε αντίθεση με μια απλή απεικόνιση της γνώμης του με επαναδημιουργία ή animation.

- **Συστήματα εικονικής πραγματικότητας**

Η τεχνολογία διεισδύει στο χώρο της δικαιοσύνης με αυξητικό ρυθμό. Σήμερα, περισσότερο από ποτέ, είναι ρεαλιστικό να πιστεύουμε ότι τα συστήματα εικονικής πραγματικότητας θα γίνουν πραγματικότητα στο δικαστικό σώμα στο εγγύς μέλλον.

Ως έννοια χρησιμοποιείται συνήθως για να περιγράψει μία ή άλλη μορφή γραφικής αναδημιουργίας, μέσω υπολογιστή, σε μια δεδομένη τοποθεσία. Στη πιο βασική της μορφή, η εικονική πραγματικότητα δίνει στο χρήστη τη δυνατότητα να μετακινείται μέσω μιας ακριβούς εικόνας ενός τόπου, όπως εμφανίζεται στην οθόνη του υπολογιστή. Η υιοθέτηση τέτοιων συστημάτων επιτρέπει στους δικαστές και τους μάρτυρες να βιώσουν μια επαναδημιουργία σαν να ήταν πραγματικά εκεί. Τα συστήματα εικονικής πραγματικότητας βασίζονται επίσης στην εισαγωγή μαθηματικών τύπων και επιστημονικών υποθέσεων σε έναν υπολογιστή, με στόχο τη δημιουργία ενός πειστικού περιβάλλοντος τέλεσης του συμβάντος.

- **Video conferencing**

Η τηλεδιάσκεψη επιτρέπει στους μάρτυρες να καταθέσουν εξ' αποστάσεως, μέσω μιας σύνδεσης εικόνας και ήχου στην αίθουσα του δικαστηρίου. Η χρήση της εξοικονομεί στο δικαστήριο σημαντικό χρόνο και κόστος, επιτρέποντας παράλληλα στους διαδίκους να προσκομίσουν αποδεικτικά στοιχεία που διαφορετικά δεν θα ήταν διαθέσιμα. Είναι ιδιαίτερα χρήσιμο όταν ένας μάρτυρας είναι μη αξιόπιστος και έχει, ιδιαίτερα, μεγάλη αξία για τους μάρτυρες που είναι προστατευόμενοι, άτομα με ειδικές ανάγκες ή εκτός δικαιοδοσίας. Για τη χρήση της όμως έχουν διατυπωθεί οι εξής επιφυλάξεις:

- ✓ **κίνδυνος από μη σχετικές πληροφορίες:** αν και η χρήση της τηλεδιάσκεψης παρουσιάζει μια σημαντική ευκαιρία για να εξοικονομηθεί χρόνος και κόστος, τα εμπλεκόμενα μέρη θα πρέπει να εξετάσουν προσεκτικά και σε κάθε περίπτωση αν τα στοιχεία που παρουσιάζονται, θα βοηθήσουν πραγματικά το δικαστήριο, αντισταθμίζοντας τα παραπάνω οφέλη.
- ✓ **τεχνικές δυσκολίες:** σχεδόν πάντοτε, υπάρχουν τεχνικές δυσκολίες στη δημιουργία και τη διατήρηση μιας σύνδεσης μεταξύ του δικαστηρίου και των μαρτύρων, καθώς παράγοντες όπως η αργή ταχύτητα του δικτύου ή η ανεπαρκής συντήρηση του εξοπλισμού, αποτελούν την βασική αιτία των δυσκολιών σε μια τηλεδιάσκεψη.

- **Ηλεκτρονικό αποθετήριο εγγράφων**

Ένα ηλεκτρονικό αποθετήριο εγγράφων είναι, όπως υποδηλώνει το όνομά του, ένα ηλεκτρονικό αντίγραφο όλων των εγγράφων που περιέχονται στο δικαστήριο. Η συγκεκριμένη βάση δεδομένων μπορεί να είναι εγκατεστημένη είτε σε τοπικό server είτε σε περιβάλλον cloud server, προστατεύεται πλήρως και είναι προσβάσιμη μέσω μοναδικών κωδικών ασφαλείας, από όλα τα εμπλεκόμενα μέρη μια δίκης και τη σύνθεση του δικαστηρίου, επιτρέποντας τους να προσθέτουν, να σχολιάζουν, να επισημαίνουν και να αναζητούν όλα τα σχετικά έγγραφα.

Μεταξύ των πλεονεκτημάτων της χρήσης ενός ηλεκτρονικού αποθετηρίου περιλαμβάνονται:

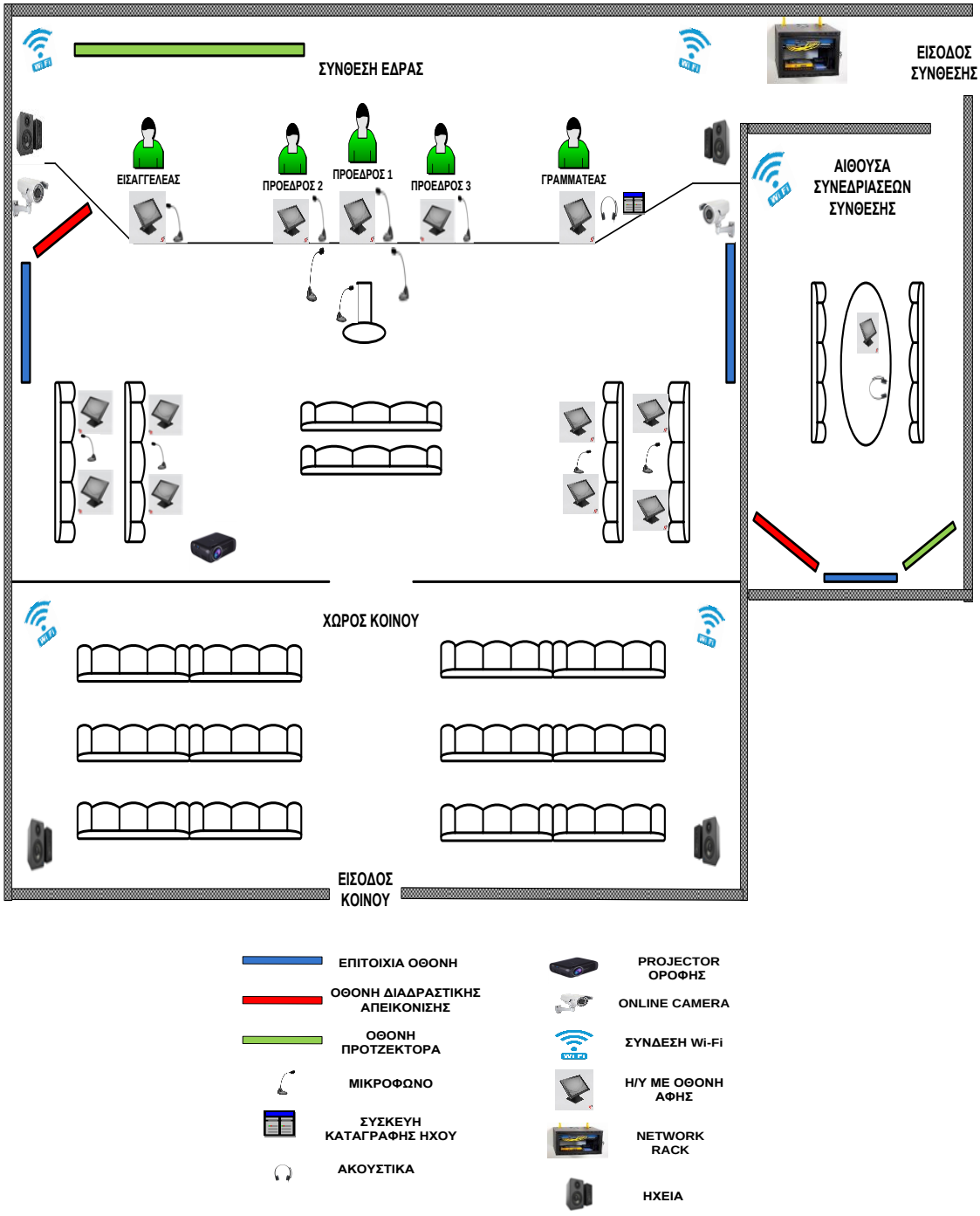
- η αδιάλειπτη πρόσβαση στα σχετικά έγγραφα.
- η πλοήγηση στα αποδεικτικά στοιχεία μέσω υπερσυνδέσμων, η οποία βελτιώνει δραματικά το χρονικό διάστημα εύρεσης αναλυτικών πληροφοριών προκειμένου να στοχοθετηθούν επαρκώς τα αποδεικτικά στοιχεία.
- η διαθεσιμότητα ψηφιακών αντιγράφων όλων των εγγράφων, νόμων, δεδικασμένων περιπτώσεων και η δυνατότητα αναζήτησής τους με την ύπαρξη λέξεων - κλειδιών.
- η ανάκτηση εγγράφων, τα οποία έχουν αποθηκευτεί με ειδικό αριθμό αναγνώρισης, δίνοντας τη δυνατότητα για την εύκολη πρόσβαση κατά τη διάρκεια των διαδικασιών, κάτι που εξοικονομεί χρόνο όταν πρόκειται για μικρά έγγραφα ή σε περιπτώσεις όπου ένα έγγραφο είναι ιδιαίτερα σημαντικό.
- το δικαίωμα για υποβολή ενστάσεων επί των αποδεικτικών στοιχείων, καθώς η χρήση του ηλεκτρονικού αποθετηρίου εξυπηρετεί τους σκοπούς της άσκησης αντιρρήσεων επί των αποφάσεων, εφόσον αυτές είναι αποτυπωμένες με τη μορφή ηλεκτρονικού εγγράφου.

Ωστόσο, υπάρχουν και ορισμένοι περιορισμοί στη χρήση του ηλεκτρονικού αποθετηρίου, που αναλύονται ως εξής:

- υπερβολικά αποδεικτικά στοιχεία: λόγω της ευκολίας με την οποία μπορούν να χρησιμοποιηθούν τα έγγραφα και να προστεθούν στη βάση δεδομένων, πιθανό να εισάγονται οποιαδήποτε δυνητικά σχετικά έγγραφα, κάτι που θα δημιουργήσει μεγάλη δυσφορία, ως προς το ποιά θα εξεταστούν επί της ουσίας.
- μη τήρηση των πρωτοκόλλων που σχετίζονται με την αξιολογική σημασία των εισαχθέντων στοιχείων στο αποθετήριο πληροφοριών.

4.4 Γραφική απεικόνιση ψηφιακής αίθουσας δικαστηρίου

Για την οπτική απεικόνιση των παραπάνω προτεινόμενων τρόπων υλοποίησης του ψηφιακού δικαστηρίου, προτείνεται η επέκταση των υφιστάμενων τεχνολογικών υποδομών του ακροατηρίου, η οποία παρουσιάζεται και επεξηγείται στο παρακάτω σχεδιάγραμμα:



Εικόνα 4-1 : Γραφική απεικόνιση ψηφιακής αίθουσας δικαστηρίου

Επίλογος

Συνοψίζοντας, η επικράτηση της τεχνολογίας των Big Data στον τομέα της δικαιοσύνης, αναμένεται να αλλάξει ριζικά τον τρόπο δόμησης των δικαστικών υπηρεσιών, καταργώντας σε μεγάλο βαθμό τις παραδοσιακές γραφειοκρατικές πολιτικές διαχείρισης των πληροφοριών. Για την επίτευξη των μέγιστων αποτελεσμάτων, απαιτείται η επανεξέταση των κλασσικών δομών, σε σχέση με την πρόσβαση, τον έλεγχο, την ασφάλεια και άλλες βασικές έννοιες διαχείρισης των δεδομένων, πλήρως εναρμονισμένες με τις διατάξεις του Γενικού Κανονισμού, προκειμένου να φιλοξενήσουν τη νέα πραγματικότητα. Νέες στρατηγικές θα αναπτυχθούν για να εξασφαλίσουν ότι τα δικαστήρια είναι έτοιμα να αγκαλιάσουν και να αφομοιώσουν τις ευκαιρίες της σύγχρονης εποχής, ελαχιστοποιώντας, παράλληλα, τους νέους κινδύνους που δεν παρουσιάζονται, πλέον, στο χαρτί αλλά σε ένα ψηφιακό περιβάλλον. Βασικές αξίες της δικαιοσύνης όπως διαφάνεια, ακεραιότητα και ανεξαρτησία, αρχικά θα επηρεαστούν και, ίσως, αμφισβητηθούν ακούσια ως συνέπεια της ενσωμάτωσης των Big Data και του GDPR στη δικαστική λογική. Κοιτώντας, όμως, μακροπρόθεσμα είναι δεδομένη η βελτίωση της ποιότητας των δικαστικών υπηρεσιών, η οποία θα συμβάλλει καίρια στη θεραπεία χρόνιων προβλημάτων και θα δημιουργήσει τις κατάλληλες συνθήκες για πρόσβαση όλων στη δικαιοσύνη και ταχύτητα στην απονομή αυτής. Η συνεισφορά της παρούσας μελέτης έγκειται, σ' αυτό ακριβώς το σημείο, της απόδειξης ότι, μέσω της αξιοποίησης της τεχνολογίας των μεγάλων δεδομένων και της εναρμόνισης της στη νέα εποχή που διέπεται από τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων, δεν επιτυγχάνεται απλά και μόνο μια τεχνοκρατική αλλαγή αλλά διαφοροποιείται αποφασιστικά και η λογική της συμπεριφοράς τόσο των πολιτών όσο και των παρόχων των δικαστικών και νομικών υπηρεσιών, οδηγώντας, αναπόφευκτα, σε δομικές αλλαγές, βασιζόμενες σε ψηφιακά κριτήρια. Η επίσημη θέσπιση υποχρεωτικής ηλεκτρονικής κατάθεσης δικογράφων, η επέκταση της ηλεκτρονικής διακυβέρνησης στο σύνολο των δικαστικών διαδικασιών, η αυτοματοποιημένη κατηγοριοποίηση των υποθέσεων ανάλογα με τη βαρύτητα τους, σε συνδυασμό με τις προς υλοποίηση προτάσεις που παρουσιάστηκαν στο κεφάλαιο 4, συνθέτουν τα χαρακτηριστικά του μελλοντικού ψηφιακού δικαστηρίου. Παρόλο που ο χρόνος είναι αμείλικτος, κανείς δεν μπορεί να προβλέψει το απαιτούμενο χρονοδιάγραμμα μιας αναδιοργάνωσης τέτοιου βεληνεκούς καθώς και τους κινδύνους που, ενδεχομένως, θα αναδειχθούν, εντούτοις, αποτελεί, πλέον, κοινή ομολογία η

ανάγκη για μετάβαση στη ψηφιακή δικαιοσύνη, ακόμη και από τους λειτουργούς αυτής. Είναι, ακόμη, στα σπάργανα αλλά έχει ανοίξει ο δρόμος...

Παράρτημα Α

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης

I

(Νομοθετικές πράξεις)

ΚΑΝΟΝΙΣΜΟΙ

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 27ης Απριλίου 2016

για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας

95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

ΚΕΦΑΛΑΙΟ II

Αρχές

Άρθρο 5

Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

1. Τα δεδομένα προσωπικού χαρακτήρα:

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

β) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν

θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»),

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

δ) είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»)

ε) διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»),

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

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

Άρθρο 9

Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα

1. Απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση,

καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

2. Η παράγραφος 1 δεν εφαρμόζεται στις ακόλουθες περιπτώσεις:

α) το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,

γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,

δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων,

ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,

στ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,

ζ) η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων,

η) η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3,

θ) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου, ή

ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίουτης Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

3. Τα δεδομένα προσωπικού χαρακτήρα που αναφέρονται στην παράγραφο 1 μπορεί να τύχουν επεξεργασίας για τους σκοπούς που προβλέπονται στην παράγραφο 2 στοιχείο η), όταν τα δεδομένα αυτά υποβάλλονται σε επεξεργασία από ή υπό την ευθύνη επαγγελματία που υπόκειται στην υποχρέωση τήρησης του επαγγελματικού απορρήτου βάσει του δικαίου της Ένωσης ή κράτους μέλους ή βάσει κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς ή από άλλο πρόσωπο το οποίο υπέχει επίσης υποχρέωση

τήρησης του απορρήτου βάσει του δικαίου της Ένωσης ή κράτους μέλους ή βάσει κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς.

4. Τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία.

Άρθρο 22

Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο.

2. Η παράγραφος 1 δεν εφαρμόζεται όταν η απόφαση: α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων, β) επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων ή γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

3. Στις περιπτώσεις που αναφέρονται στην παράγραφο 2 στοιχεία α) και γ), ο υπεύθυνος επεξεργασίας των δεδομένων εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, τουλάχιστον του δικαιώματος εξασφάλισης ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης.

4. Οι αποφάσεις που αναφέρονται στην παράγραφο 2 δεν βασίζονται στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που αναφέρονται στο άρθρο 9 παράγραφος 1, εκτός αν ισχύει το άρθρο 9 παράγραφος 2 στοιχείο α) ή ζ) και αν υφίστανται κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.

ΚΕΦΑΛΑΙΟ IV

Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία

Τμήμα 1

Γενικές υποχρεώσεις

Άρθρο 24

Ευθύνη του υπευθύνου επεξεργασίας

1. Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο.

2. Όταν δικαιολογείται σε σχέση με τις δραστηριότητες επεξεργασίας, τα μέτρα που αναφέρονται στην παράγραφο 1 περιλαμβάνουν την εφαρμογή κατάλληλων πολιτικών για την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας.

3. Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας όπως αναφέρεται στο άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας.

Άρθρο 28

Εκτελών την επεξεργασία

1. Όταν η επεξεργασία πρόκειται να διενεργηθεί για λογαριασμό υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.

2. Ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας. Σε περίπτωση γενικής γραπτής άδειας, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για τυχόν σκοπούμενες αλλαγές που αφορούν την προσθήκη ή την αντικατάσταση των άλλων εκτελούντων την επεξεργασία, παρέχοντας με τον τρόπο αυτό τη δυνατότητα στον υπεύθυνο επεξεργασίας να αντιταχθεί σε αυτές τις αλλαγές.

3. 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. Η εν λόγω σύμβαση ή άλλη νομική πράξη προβλέπει ειδικότερα ότι ο εκτελών την επεξεργασία:

α) επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, μεταξύ άλλων όσον αφορά τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, εκτός εάν υποχρεούται προς τούτο βάσει του δικαίου της Ένωσης ή του δικαίου του κράτους μέλους στο οποίο υπόκειται ο εκτελών την επεξεργασία· σε αυτήν την περίπτωση, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για την εν λόγω

νομική απαίτηση πριν από την επεξεργασία, εκτός εάν το εν λόγω δίκαιο απαγορεύει αυτού του είδους την ενημέρωση για σοβαρούς λόγους δημόσιου συμφέροντος,

β) διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας,

γ) λαμβάνει όλα τα απαιτούμενα μέτρα δυνάμει του άρθρου 32,

δ) τηρεί τους όρους που αναφέρονται στις παραγράφους 2 και 4 για την πρόσληψη άλλου εκτελούντος την επεξεργασία,

ε) λαμβάνει υπόψη τη φύση της επεξεργασίας και επικουρεί τον υπεύθυνο επεξεργασίας με τα κατάλληλα τεχνικά και οργανωτικά μέτρα, στον βαθμό που αυτό είναι δυνατό, για την εκπλήρωση της υποχρέωσης του υπευθύνου επεξεργασίας να απαντά σε αιτήματα για άσκηση των προβλεπόμενων στο κεφάλαιο III δικαιωμάτων του υποκειμένου των δεδομένων,

στ) συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 32 έως 36, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία,

ζ) κατ' επιλογή του υπευθύνου επεξεργασίας, διαγράφει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας μετά το πέρας της παροχής υπηρεσιών επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, εκτός εάν το δίκαιο της Ένωσης ή του κράτους μέλους απαιτεί την αποθήκευση των δεδομένων προσωπικού χαρακτήρα,

η) θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που θεσπίζονται στο παρόν άρθρο και επιτρέπει και διευκολύνει τους ελέγχους, περιλαμβανομένων των επιθεωρήσεων, που διενεργούνται από τον υπεύθυνο επεξεργασίας ή από άλλον ελεγκτή εντεταλμένο από τον υπεύθυνο επεξεργασίας.

Όσον αφορά το πρώτο εδάφιο στοιχείο η), ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας, εάν, κατά την άποψή του, κάποια εντολή

παραβιάζει τον παρόντα κανονισμό ή άλλες ενωσιακές ή εθνικές διατάξεις περί προστασίας δεδομένων.

4. Όταν ο εκτελών την επεξεργασία προσλαμβάνει άλλον εκτελούντα για τη διενέργεια συγκεκριμένων δραστηριοτήτων επεξεργασίας για λογαριασμό του υπευθύνου επεξεργασίας, οι ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων που προβλέπονται στη σύμβαση ή στην άλλη νομική πράξη μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, κατά τα προβλεπόμενα στην παράγραφο 3, επιβάλλονται στον άλλον αυτόν εκτελούντα μέσω σύμβασης ή άλλης νομικής πράξης σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους, ιδίως ώστε να παρέχονται επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, ούτως ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού. Όταν ο άλλος εκτελών την επεξεργασία αδυνατεί να ανταποκριθεί στις σχετικές με την προστασία των δεδομένων υποχρεώσεις του, ο αρχικός εκτελών παραμένει πλήρως υπόλογος έναντι του υπευθύνου επεξεργασίας για την εκπλήρωση των υποχρεώσεων του άλλου εκτελούντος την επεξεργασία.

5. Η τήρηση εκ μέρους του εκτελούντος την επεξεργασία εγκεκριμένου κώδικα δεοντολογίας όπως αναφέρεται στο άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 δύναται να χρησιμοποιηθεί ως στοιχείο για να αποδειχθεί ότι παρέχει επαρκείς διαβεβαιώσεις σύμφωνα με τις παραγράφους 1 και 4 του παρόντος άρθρου.

6. Με την επιφύλαξη ατομικής σύμβασης μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, η σύμβαση ή η άλλη νομική πράξη που αναφέρεται στις παραγράφους 3 και 4 του παρόντος άρθρου μπορεί να βασίζεται, εν όλω ή εν μέρει, σε τυποποιημένες συμβατικές ρήτρες που αναφέρονται στις παραγράφους 7 και 8 του παρόντος άρθρου, μεταξύ άλλων όταν αποτελούν μέρος πιστοποίησης που χορηγείται στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία σύμφωνα με τα άρθρα 42 και 43.

7. Η Επιτροπή μπορεί να θεσπίσει τυποποιημένες συμβατικές ρήτρες για τα θέματα που αναφέρονται στις παραγράφους 3 και 4 του παρόντος άρθρου και σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 93 παράγραφος 2.

8. Μια εποπτική αρχή μπορεί να θεσπίσει τυποποιημένες συμβατικές ρήτρες για τα θέματα που αναφέρονται στις παραγράφους 3 και 4 του παρόντος άρθρου και σύμφωνα με τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63.

9. Η σύμβαση ή η άλλη νομική πράξη που αναφέρεται στις παραγράφους 3 και 4 υφίσταται γραπτώς, μεταξύ άλλων σε ηλεκτρονική μορφή.

10. Με την επιφύλαξη των άρθρων 82, 83 και 84, εάν ο εκτελών την επεξεργασία καθορίσει κατά παράβαση του παρόντος κανονισμού τους σκοπούς και τα μέσα της επεξεργασίας, ο εκτελών την επεξεργασία θεωρείται υπεύθυνος επεξεργασίας για τη συγκεκριμένη επεξεργασία.

Άρθρο 33

Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή

1. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

2. Ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας αμελλητί, μόλις αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα.

3. Η γνωστοποίηση που αναφέρεται στην παράγραφο 1 κατ' ελάχιστο:

α) περιγράφει τη φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα,

β) ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες,

γ) περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα,

δ) περιγράφει τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

4. Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.

5. Ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην εποπτική αρχή να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο.

Άρθρο 34

Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων

1. Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.

2. Στην ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 1 του παρόντος άρθρου περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρονται στο άρθρο 33 παράγραφος 3 στοιχεία β), γ) και δ).

3. Η ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 1 δεν απαιτείται, εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις:

α) ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση,

β) ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει ο αναφερόμενος στην παράγραφο 1 υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων,

γ) προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

4. Εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, η εποπτική αρχή μπορεί, έχοντας εξετάσει την πιθανότητα επέλευσης υψηλού κινδύνου από την παραβίαση των δεδομένων προσωπικού χαρακτήρα, να του ζητήσει να το πράξει ή μπορεί να αποφασίσει ότι πληρούται οποιαδήποτε από τις προϋποθέσεις που αναφέρονται στην παράγραφο 3.

Τμήμα 3

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση

Άρθρο 35

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

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

β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

4. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

5. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

6. Πριν από την έκδοση των καταλόγων που αναφέρονται στις παραγράφους 4 και 5, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63, εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση.

7. Η εκτίμηση περιέχει τουλάχιστον:

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

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

γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

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

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

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

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

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

Άρθρο 36

Προηγούμενη διαβούλευση

1. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη της εποπτικής αρχής πριν από την επεξεργασία, όταν η δυνάμει του άρθρου 35 εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας.

2. Όταν η εποπτική αρχή φρονεί ότι η σχεδιαζόμενη επεξεργασία που αναφέρεται στην παράγραφο 1 παραβαίνει τον παρόντα κανονισμό, ιδίως εάν ο υπεύθυνος επεξεργασίας δεν έχει προσδιορίσει ή μετριάσει επαρκώς τον κίνδυνο, η εποπτική αρχή παρέχει γραπτώς συμβουλές στον υπεύθυνο επεξεργασίας εντός προθεσμίας μέχρι οκτώ εβδομάδων από την παραλαβή του αιτήματος διαβούλευσης, και, όπου απαιτείται, στον εκτελούντα την επεξεργασία, ενώ δύναται να χρησιμοποιήσει οποιαδήποτε από τις εξουσίες της που αναφέρονται στο άρθρο 58. Η εν λόγω προθεσμία μπορεί να παραταθεί κατά έξι εβδομάδες, λόγω της πολυπλοκότητας που χαρακτηρίζει τη σχεδιαζόμενη επεξεργασία. Η εποπτική αρχή ενημερώνει τον υπεύθυνο επεξεργασίας και, όπου απαιτείται, τον εκτελούντα την επεξεργασία για την εν λόγω παράταση εντός ενός μηνός από την παραλαβή του αιτήματος διαβούλευσης, καθώς και για τους λόγους της καθυστέρησης. Οι εν λόγω προθεσμίες μπορούν να αναστέλλονται έως ότου η εποπτική αρχή λάβει τις πληροφορίες που ζήτησε για τους σκοπούς της διαβούλευσης.

3. Κατά τη διαβούλευση με την εποπτική αρχή δυνάμει της παραγράφου 1, ο υπεύθυνος επεξεργασίας παρέχει στην εποπτική αρχή:

α) κατά περίπτωση, τις αντίστοιχες αρμοδιότητες του υπευθύνου επεξεργασίας, των από κοινού υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία που συμμετέχουν στις εργασίες, ιδίως όσον αφορά επεξεργασία εντός ομίλου επιχειρήσεων,
β) τους σκοπούς και τα μέσα της σχεδιαζόμενης επεξεργασίας,

γ) τα μέτρα και τις εγγυήσεις για την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σύμφωνα με τον παρόντα κανονισμό,

δ) κατά περίπτωση, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, 4.5.2016 L 119/54 Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης EL

ε) την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων που προβλέπεται στο άρθρο 35, και στ) κάθε άλλη πληροφορία που ζητεί η εποπτική αρχή.

4. Τα κράτη μέλη ζητούν τη γνώμη της εποπτικής αρχής κατά την εκπόνηση προτάσεων νομοθετικών μέτρων προς θέσπιση από τα εθνικά κοινοβούλια ή κανονιστικών μέτρων που βασίζονται σε τέτοια νομοθετικά μέτρα, τα οποία αφορούν την επεξεργασία.

5. Κατά παρέκκλιση από την παράγραφο 1, το δίκαιο του κράτους μέλους μπορεί να απαιτεί από τους υπευθύνους επεξεργασίας να διαβουλεύονται και να λαμβάνουν προηγούμενη άδεια από την εποπτική αρχή σε σχέση με την επεξεργασία από υπεύθυνο επεξεργασίας για την εκτέλεση καθήκοντος που ασκείται από τον εν λόγω υπεύθυνο προς το δημόσιο συμφέρον, περιλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία.

Παράρτημα Β

The PIA Software

Το λογισμικό PIA είναι ένα εργαλείο που διανέμεται ελεύθερα από τη CNIL, προκειμένου να διευκολυνθεί η πραγματοποίηση αναλύσεων των επιπτώσεων αναφορικά με την προστασία των προσωπικών δεδομένων, σύμφωνα με τον Γενικό Κανονισμό. Στόχος του ανοικτού αυτού λογισμικού, είναι να βοηθήσει τους Υπεύθυνους Προστασίας Δεδομένων (DPO's) να δημιουργήσουν και να αποδείξουν τη συμμόρφωση του εκάστοτε φορέα με το GDPR.

- **Εφαρμογή front–end**

Πρόκειται για το "web front office" του ανοικτού λογισμικού PIA, για πρόσβαση μέσω ενός φυλομετρητή web και περαιτέρω παραμετροποίηση κατά την ανάπτυξή σε περιβάλλον server, το οποίο περιλαμβάνει τα εξής:

Developmet server

Εκτέλεση `ng serve` για dev server. Πλοηγηθείτε στο `http://localhost:4200/`
Η εφαρμογή θα επαναφορτωθεί αυτόματα αν αλλάξετε κάποιο από τα αρχεία προέλευσης.

Code scaffolding

Εκτελέστε `ng generate component component-name` για να δημιουργήσετε ένα νέο στοιχείο.
Μπορείτε επίσης να χρησιμοποιήσετε την εντολή:
`ng generate directive|pipe|service|class|module`.

Build

Πληκτρολογήστε `ng build` για να εκτελεστεί το project.
Τα αντικείμενα δημιουργίας θα αποθηκευτούν στον `dist/` κατάλογο.

Build for production

Πρώτα πρέπει να μετονομάσετε το αρχείο
`src/environments/environment.prod.ts.example` σε
`src/environments/environment.prod.ts`.
Στη συνέχεια, ορίστε τον αριθμό έκδοσης μέσα σε αυτό το αρχείο και χρησιμοποιήστε την εντολή
`ng build --prod --build-optimizer --sourcemaps` ή `yarn prod`
για την κατασκευή.

Running unit tests

Εκτελέστε `ng test` την εκτέλεση δοκιμών μέσω του Karma

Running end-to-end tests

Εκτελέστε `ng e2e`την εκτέλεση των δοκιμών από άκρο σε άκρο μέσω του Protractor και πριν εκτελέσετε τις δοκιμές, βεβαιωθείτε ότι χρησιμοποιείτε την εφαρμογή μέσω της εντολής `ng serve`.

Run in production mode

Εκτελέστε τον κατάλογο `ng build --prod` και μετά `dist/` που δημιουργείται από το ng build στον `www/` κατάλογό σας (όπως το / var / www / html για προεπιλογή σε Apache server)

Generate a static documentation of PIA with Compodoc

Εκτελέστε την εντολή `npm run compodoc` ή την εντολή `yarn run compodoc` για να δημιουργήσετε μια τεκμηρίωση στο `documentation` κατάλογό.

Αναλυτικότερες οδηγίες στο
https://github.com/LINCnil/pia#build-for-production

- **Εφαρμογή back-end**

Η εφαρμογή PIA-BACK αναπτύσσεται με το πλαίσιο RubyOnRails, παρέχοντας ένα RESTful API δηλαδή ένα Application Program Interface που χρησιμοποιεί HTTP αιτήματα, για τα εργαλεία PIA , PIA-APP και περιλαμβάνει τα εξής:

Requirements

pia (front-end) application και / ή pia (stand-alone) application

Ruby 2.3.x

Rails 5.0.x

PostgreSQL 9.4+

System requirements

CPU: i5

Ram: 4GB

Disk space: 20GB

OS: κατά προτίμηση Linux

PostgreSQL installation

Βασική εγκατάσταση στο Debian μπορείτε να χρησιμοποιήσετε την ακόλουθη τεκμηρίωση: wiki.debian.org/PostgreSql στο Ubuntu που μπορείτε να χρησιμοποιήσετε: help.ubuntu.com/community/PostgreSQL

Επίσης, πρέπει να δημιουργήσετε έναν νέο χρήστη με κωδικό πρόσβασης.

Clone the repository

```
git clone https://github.com/atnos/pia-back.git
```

Go to the folder pia-back

```
cd pia-back
```

Create and fill the file database.yml

```
cp config/database.example.yml config/database.yml
```

Συμπληρώστε τα πεδία **username** και **password** για κάθε περιβάλλον με το όνομα χρήστη και τον κωδικό πρόσβασης PostgreSQL που δημιουργήσατε στο βήμα "PostgreSQL installation".

Install all dependencies

```
bundle install
```

Create and fill the file application.yml

```
cp config/application.example.yml config/application.yml
```

Δημιουργήστε το SECRET_KEY_BASE με: `bin/rake secret` και επικολλήστε το μυστικό κλειδί στο αρχείο.

Create database

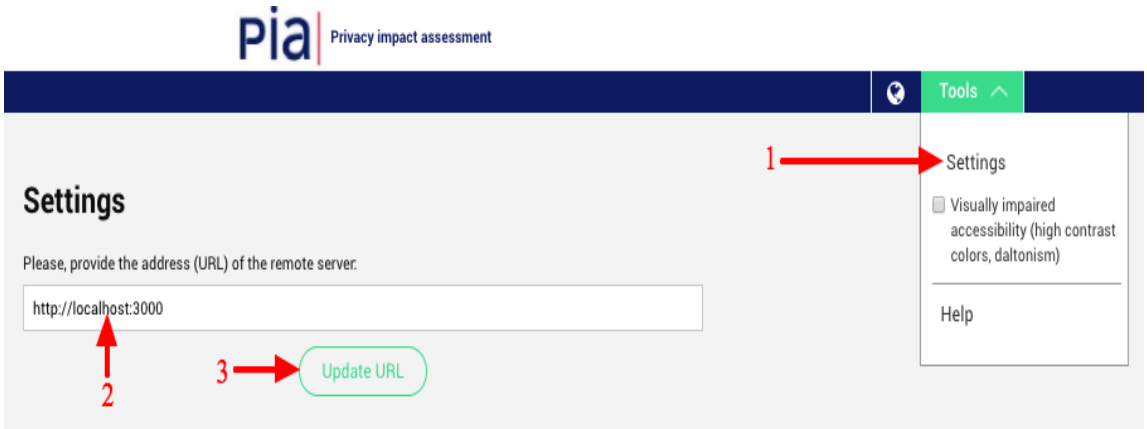
```
bin/rake db:create
```

Create tables

```
bin/rake db:migrate
```

Run the application

- `bin/rails s` ο διακομιστής σας θα είναι προσβάσιμος με τη διεύθυνση URL `localhost:3000`
- Μπορείτε να ορίσετε την επιλογή `-b` για να δεσμεύσετε μια δημόσια IP ή ένα όνομα τομέα και `-p` για να χρησιμοποιήσετε μια άλλη θύρα.
  Παράδειγμα: `bin/rails s -b 123.456.789.101 -p 8080` ο διακομιστής θα είναι προσβάσιμος με τη διεύθυνση URL `123.456.789.101:8080`
- Στην front-end εφαρμογή , χρησιμοποιήστε αυτήν τη διεύθυνση URL για να ενεργοποιήσετε τη λειτουργία διακομιστή.
- Συμπληρώστε το πεδίο στο "Tools"--> "Settings"



Run the application in production mode

- Συμπληρώστε την ενότητα `production` στο αρχείο `database.yml`
- Δημιουργία της βάσης δεδομένων: `RAILS_ENV = production bin/rake db:create`
- Δημιουργία των πινάκων: `RAILS_ENV = production bin/rake db:migrate`
- Εκτελέστε στο διακομιστή: `RAILS_ENV = production bin/rails s`

Update the application

Ενημέρωση του αποθετηρίου: `git pull`

Ενημέρωση της βάσης δεδομένων: `RAILS_ENV=production bin/rake db:migrate`

Run the test

`bin/rake`

Αναλυτικότερες οδηγίες στο

https://github.com/LINCnil/pia-back#le-logiciel-pia--the-pia-software

Αναφορές

Αρθρογραφία

1. Arockia Panimalar.S 1, Varnekha Shree.S2, Veneshia Kathrine.A3 , Sep-2017, "The 17 V's Of Big Data", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 09 | www.irjet.net p-ISSN: 2395-0072.

2. Carmen Vargas Pérez Department of Applied Economics IV, Complutense University of Madrid Juan Luis Peñaloza Figueroa Department of Statistics and Operations Research II, Complutense University of Madrid, 2017, "Big Data and the Demand for Court and Legal Services" European Journal of Interdisciplinary Studies Sep. Dec. 2017, [pdf].

3. Christos Stergiou, Student Member, IEEE, and Kostas E. Psannis, Member, IEEE, 2017, Algorithms for Big Data in Advanced Communication Systems and Cloud Computing.

4. Cornelia L. Hammer, Diane C. Kostroch, Gabriel Quirós, and STA Internal Group, 2017, "Big Data: Potential, Challenges, and Statistical Implications", IMF STAFF DISCUSSION NOTE.

5. David Basin1, Soren Debois2, and Thomas Hildebrandt2, 2018, "On Purpose and by Necessity: Compliance under the GDPR", 1 ETH Zurich basin@inf.ethz.ch, 2 IT University of Copenhagen fdebois,hildeg@itu.dk.

6. Elizabeth C. Wiggins, 2006, "The Courtroom of the Future is Here: Introduction to Emerging Technologies in the Legal System", 28 LAW & POLY, 182, 185.

7. Gustav Stigestadh Felix Moberg, sping semester 2018, "Big data, for better or worse: GDPR support for the individual", Lunds Universitet Ekonomihogskolan, Master thesis.

8. Inga Hofer, 2007, "THE RISE OF COURTROOM TECHNOLOGY AND ITS EFFECT ON THE FEDERAL RULES OF EVIDENCE & THE FEDERAL RULES OF CIVIL PROCEDURE", Submitted in partial fulfillment of the requirements of the King Scholar Program Michigan State University College of Law under the direction of Professor John Pirich Spring.

9. Kostas E. Psannis, Member IEEE, Christos Stergiou, Student Member IEEE, and B. B. Gupta, Member IEEE, 2018, Advanced Media-based Smart Big Data on Intelligent Cloud Systems.

10. Moyeda, Jessica, 2014, "Courtroom Technology", Cornell Law School Graduate Student Papers. Paper 30. http://scholarship.law.cornell.edu/lps_papers/30.

11. Robert McDougall, 2013, "THE USES AND ABUSES OF TECHNOLOGY IN THE COURTROOM", Keynote address prepared for the Society of Construction Law, Australia Conference of 2013.

12. Tal Z. Zarsky, 2017,"Incompatible: The GDPR in the Age of Big Data", SETON HALL LAW REVIEW.

13. TEAM FRANCE: Adrien Fauchier Delavigne, Ariane Gajzler, Anna Marin. 3-6 July 2017, "The Challenges facing Justice in the future: Judges confronted with the advent of Big Data Analytics". ejtn Semi-Final D Budapest, Hungary.

14. The Federal Judicial Center and the National Institute for Trial Advocacy, 2012, "Effective Use of Courtroom Technology: A Judge's Guide to Pretrial and Trial".

15. Yu-Che Chen, School of Public Administration, University of Nebraska at Omaha, Omaha, NE, USA, Tsui-Chuan Hsieh, Department of Information Management, National Development Council, Taiwan, January-March 2014, "Big Data for Digital Government: Opportunities, Challenges, and Strategies".

16. Zakir, Jasmine, 2015, "Big Data Analytics". Conference: International Association for Computer Information Systems, At http://www.iacis.org/iis/2015/2_iis_2015_81-90.pdf,Volume:16,https://www.researchgate.net/publication/301698587_Big_Data_Analytics.

Ιστοσελίδες

17. https://www.capterra.com/gdpr-compliance-software

18. https://www.cnil.fr/en/privacy-impact-assessment-pia

19. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

20. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

21. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

22. https://www.computing.co.uk/ctg/opinion/3014301/gdpr-and-big-data-friends-or-foes

23. http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/GDPR/FILES%20GDPR/WP253_EL.PDF

24. https://www.egress.com/: "The digital courtroom: Four key considerations for local authorities sharing court bundles electronically", INDUSTRY WHITE PAPER.

25. https://www.evidencer.com.au: EVIDENCER THE DIGITAL TRUTH "Revolutionize Judicial system and process"

26. https://www.forbes.com/sites/michaelkanellos/2016/03/11/the-five-different-types-of-big data

27. https://www.taxheaven.gr/news/news/view/id/43234#

28. https://www.thomsonreuters.com: "The future of the courts" A white paper THOMSON REUTERS.