ΑΚΑΔΗΜΙΑ ΕΜΠΟΡΙΚΟΥ ΝΑΥΤΙΚΟΥ

Α.Ε.Ν ΜΑΚΕΔΟΝΙΑΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΥΑΚΙΝΘΟΣ ΧΑΡΑΛΑΜΠΟΣ

ΘΕΜΑ: GDPR - Ασφάλεια Προσωπικών Δεδομένων

ΤΟΥ ΣΠΟΥΔΑΣΤΗ: ΚΑΡΑΠΑΤΑΚΗ ΙΩΑΝΝΗ

Α.Γ.Μ: 4070

Ημερομηνία ανάληψης της εργασίας: 17/05/2019

Ημερομηνία παράδοσης της εργασίας:

Α/Α	Ονοματεπώνυμο	Ειδικότητα	Αξιολόγηση	Υπογραφή
1				
2				
3				
ΤΕΛΙΚΗ ΑΞΙΟΛΟΓΗΣΗ				

Ο ΔΙΕΥΘΥΝΤΗΣ ΣΧΟΛΗΣ: ΤΣΟΥΛΗΣ ΝΙΚΟΛΑΟΣ

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Η παρούσα εργασία αποτελεί μια αναφορά στον νέο κανονισμό προστασίας προσωπικών δεδομένων (Γενικός Κανονισμός για την Προστασία Δεδομένων-GDPR), τον τρόπο προστασίας τους και διασφάλισης τους. Στις μέρες μας η κοινωνία γίνεται συνεχώς πιο αυτοματοποιημένη με το διαδίκτυο ως ένα από τα μεγαλύτερα μέσα πληροφόρησης και επικοινωνίας, μέσω των ηλεκτρονικών υπολογιστών και των έξυπνων κινητών τηλεφώνων να μας παρέχουν το δικαίωμα της πρόσβασης στην πληροφορία και την επικοινωνία συμφώνως με το Άρθρο 5 & 5Α του Συντάγματος. Λόγω της απότομης εξέλιξης τις τεχνολογίας υπάρχει δυνατότητα αποθήκευσης τεράστιου όγκου δεδομένων σε μικρό χρονικό διάστημα και με μικρό κόστος, δυνατότητα επεξεργασίας των δεδομένων σε πολύ μικρό χρονικό διάστημα καθώς και συσχέτισης των δεδομένων με άλλες πήγες μέσω του διαδικτύου. Με αποτέλεσμα τα προσωπικά μας δεδομένα να είναι πιο ευάλωτα, δημιουργώντας ένα κενό στην ασφάλεια της ιδιωτικότητας του ανθρώπου. Το Ευρωπαϊκό Κοινοβούλιο και το συμβούλιο της 27ης Απριλίου το 2016 ψήφησε ένα νέο ενωσιακό νομοθέτημα, με αποτέλεσμα να αντικαταστήσει την οδηγία 95/46/ΕΚ που ήταν μέχρι τότε αρμόδια για την ασφάλεια των προσωπικών μας δεδομένων. Γνωρίζοντας για τον Γενικό Κανονισμό για την Προστασία Δεδομένων εν συντομία GDPR μπορούμε να καταλάβουμε πόσο σημαντικά είναι τα προσωπικά μας δεδομένα και να αρχίσουμε να αναρωτιόμαστε ποιοι και για ποιους λόγους τα συλλέγουν. Έτσι θα καταλάβουμε επίσης και πότε τα προσωπικά μας δεδομένα παραβιάζονται, τι συνέπειες μπορεί να υποστεί κάποιος που τα παραβιάζει αλλά το σημαντικότερο από όλα το πως θα τα προστατευσούμε από άλλους

ΚΕΦΑΛΑΙΟ 1

Γενικός Κανονισμός για την Προστασία Δεδομένων-GDPR

1.1 Επεξήγηση του όρου "Κανονισμός της Ευρωπαϊκής Ένωσης"

Μπορούμε πολύ εύκολα να παρατηρήσουμε ότι συχνά υπάρχει μια παρανόηση σε σχέση με το νέο νομοθετικό πλαίσιο, το οποίο πρόκειται για ένα Κανονισμό της Ευρωπαϊκής Ένωσης. Απλουστέρα, ο όρος "Κανονισμός" είναι δεσμευτική νομοθετική πράξη που εκδίδετε όχι σε εθνικό επίπεδο, αλλά σε επίπεδο Ευρωπαϊκής Ένωσης, με συνέπεια η εφαρμογή της να είναι υποχρεωτική σε όλες τις χώρες της ΕΕ.

Οι Κανονισμοί διαφέρουν από τις οδηγίες της Ευρωπαϊκής Ένωσης (για παράδειγμα η οδηγία 95/46/ΕΚ που αποτέλεσε τη βάση για τον νόμο 2472/1997), καθώς οι οδηγίες ορίζουν έναν στόχο τον οποίο όλες οι χώρες της ΕΕ σκοπεύουν να επιτύχουν, παρ' όλα αυτά εναπόκειται σε κάθε χώρα να θεσπίσει τους δικούς της νόμους για την επίτευξή του.

Ωστόσο, όπως συχνά επισημαίνεται, εκτός του αντικειμενικού στόχου της ενιαίας ρύθμισης και της εξάλειψης των αποκλίσεων μεταξύ των νομοθεσιών των κρατών-μελών, ο ΓΚΠΔ μοιάζει σε αρκετές περιπτώσεις με Οδηγία. Αυτό συμβαίνει διότι περιλαμβάνει αρκετές ρήτρες ευελιξίας μέσω των οποίων ο εθνικός νομοθέτης επιτρέπεται ή και επιβάλλεται να ρυθμίσει επιμέρους ζητήματα.

Για παράδειγμα, ο ΓΚΠΔ δίνει το περιθώριο στους εθνικούς νομοθέτες να ορίσουν την ηλικία στην οποία ένας ανήλικος μπορεί να παρέχει τη συγκατάθεσή του ώστε να επεξεργαστούν τα προσωπικά του δεδομένα, ανάμεσα στα 13 και τα 16 έτη. Στην Ελλάδα σε επίπεδο σχεδίου νόμου ο νομοθέτης έχει επιλέξει την ηλικία των 15 ετών.

Η επιλογή της Ευρωπαϊκής Ένωσης να ορίσει το νέο νομοθέτημα ως Κανονισμό απέφερε αρνητικές κριτικές, οι λόγοι για τους οποίους η ΕΕ αποφάσισε να ρυθμίσει το ζήτημα της προστασίας των Προσωπικών Δεδομένων ως Κανονισμό και οχι ως οδηγία, είναι εύκολα αντιληπτοί. Ενόψει των ταχύτατων τεχνολογικών εξελίξεων και της απότομης αύξησης των προσωπικών δεδομένων, του γεγονότος ότι τα δεδομένα αυτά είναι πλέον εύκολα διαθέσιμα στο διαδίκτυο και την τεράστιο οικονομικό και κοινωνικό αντίκτυπο που έχουν τα προσωπικά δεδομένα. Κρίθηκε η ανάγκη ανάπτυξης μίας νέας, ενιαίας και λεπτομερούς προσέγγισης, με κανόνες που θα ρυθμίζουν την προστασία των δεδομένων με τρόπο που δεν θα επιτρέπει την εκμετάλλευση προσωπικών δεδομένων για αθέμιτους σκοπούς εντός των ορίων της Ένωσης (αλλά και εκτός όπως θα δούμε παρακάτω), ενώ παράλληλα θα υποχρεώνει ολα τα κράτη της Ένωσης να επιβάλλουν κανόνες με κοινά μέσα ελεγχόμενης και εγγυημένης αποτελεσματικοτητας.

1.2 Ιστορική ανάδρομη.

Στις 24/10/1995 Εγκρίνεται η ευρωπαϊκή οδηγία για την προστασία των δεδομένων (οδηγία 95/46/ΕΚ) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών).

Το 2009, η Ευρωπαϊκή Επιτροπή άρχισε να επανεξετάζει το ισχύον νομικό πλαίσιο για την προστασία των δεδομένων, διοργανώνοντας αρχικά διάσκεψη υψηλού επιπέδου τον Μάιο του 2009 και στη συνέχεια δημόσια διαβούλευση που ολοκληρώθηκε στα τέλη του 2009. Καθ' όλη τη διάρκεια του έτους 2010 οργανώθηκαν διαβουλεύσεις με συγκεκριμένους ενδιαφερόμενους φορείς.

Στις 25/01/2012 η Ευρωπαϊκή Επιτροπή προτείνει μεταρρύθμιση για ενίσχυση των διαδικτυακών δικαιωμάτων απορρήτου και της ψηφιακής οικονομίας. Η Ευρωπαϊκή Επιτροπή προτείνει μια ολοκληρωμένη μεταρρύθμιση του τότε ισχύος κανονισμού προστασίας δεδομένων 95/46/ΕΚ για την ενίσχυση των διαδικτυακών δικαιωμάτων απορρήτου και την ενίσχυση της ψηφιακής οικονομίας της Ευρώπης.

Στις 12/03/2014 Το Ευρωπαϊκό κοινοβούλιο υιοθετεί το GDPR. Το Ευρωπαϊκό Κοινοβούλιο επιδεικνύει ισχυρή υποστήριξη για το GDPR ψηφίζοντας στην Ολομέλεια με 621 ψήφους υπέρ και 10 κατά.

Στις 16/05/2015 Το Συμβούλιο καταλήγει σε μια γενική μορφή για την υλοποίηση του GDPR.

Στις 27/07/2015 Ο ΕΕΠΔ καταθέτει συστάσεις σχετικά με το τελικό κείμενο του GDPR. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων δημοσιεύει τις συστάσεις του στους ευρωπαίους συννομοθέτες που διαπραγματεύονται το τελικό κείμενο του GDPR με τη μορφή σύνταξης προτάσεων. Επίσης, δημιουργεί μια εφαρμογή για έξυπνα κινητά τηλεφωνά που συγκρίνει την πρόταση της Ευρωπαϊκής Επιτροπής με τα τελευταία κείμενα του Ευρωπαϊκού Κοινοβουλίου και του Ευρωπαϊκού Συμβουλίου.

Στις 15/12/2015 Το Ευρωπαϊκό Κοινοβούλιο , το Ευρωπαϊκό Συμβούλιο και η Ευρωπαϊκή Επιτροπή καταλήγουν σε συμφωνία για τον GDPR.

Στις 27/04/2016 ψηφίστηκε ένα νέο ενωσιακό νομοθέτημα, με αποτέλεσμα να αντικαταστήσει την οδηγία 95/46/ΕΚ. Προκειται για τον Κανονισμό 2016/679 «Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων».

Στις 24/05/2016 Ο κανονισμός τίθεται σε ισχύ, 20 ημέρες μετά τη δημοσίευση στην Επίσημη Εφημερίδα της ΕΕ. Την ιδία ημερομηνία ο GDPR ενισχύει ένα ευρύ

φάσμα δικαιωμάτων και δημιουργεί κάποια νέα δικαιώματα για φυσικά πρόσωπα, όπως: το δικαίωμα διαγραφής (right to be forgotten) όπου ένα φυσικό πρόσωπο μπορεί να ζητήσει από έναν οργανισμό να διαγράψει τα προσωπικά σας δεδομένα, για παράδειγμα όταν τα δεδομένα ενός προσώπου δεν είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν ή για τους οποίους έχετε δώσει τη συγκατάθεσή σας.

Στις 10/01/2017 Η Ευρωπαϊκή Επιτροπή προτείνει δύο νέους κανονισμούς για την προστασία της ιδιωτικής ζωής και τις ηλεκτρονικές επικοινωνίες (ePrivacy) και για τους κανόνες προστασίας δεδομένων που ισχύουν για τα θεσμικά όργανα της ΕΕ (επί του παρόντος κανονισμού 45/2001).

Στις 06/05/2018 εφαρμόζετε οδηγία προστασίας δεδομένων για τους τομείς της αστυνομίας και της δικαιοσύνης στην εθνική νομοθεσία που εφαρμόζεται από σήμερα. Τα κράτη μέλη πρέπει να έχουν μεταφέρει τις διατάξεις για την προστασία δεδομένων στους τομείς της αστυνομίας και της δικαιοσύνης στην εθνική νομοθεσία.

Στις 25/05/2018 Διόρθωση στον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, καθώς και για την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός Προστασίας Δεδομένων). Επίσης Διόρθωση στην οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς πρόληψης, διερεύνησης, διαπίστωσης και δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων, καθώς και για την ελεύθερη κυκλοφορία των δεδομένων αυτών των δεδομένων. [1]

*Στις 25/05/2018 Ο Γενικός Κανονισμός Προστασίας Δεδομένων τίθεται σε εφαρμογή.

Έπειτα ο κανονισμός έχει υποστεί πολλές τροποποιήσεις

*Η διάθεση της διετούς μεταβατικής περιόδου (27/04/2016 - 25/05/2018) ορίστηκε προκειμένου να δοθεί η δυνατότητα σε όσους χειρίζονται προσωπικά δεδομένα, δηλαδή υπεύθυνους επεξεργασίας αλλά και στις αρμόδιες εποπτικές αρχές, που για την Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα να ενημερωθούν και να προετοιμαστούν για την εφαρμογή των νέων ρυθμίσεων. Μέχρι σήμερα ο κανονισμός έχει υποστεί τις παρακάτω τροποποιήσεις.

1.3 Γενικός Κανονισμός για την Προστασία Δεδομένων.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) είναι ένας ισχυρός **νόμος περί απορρήτου** που δημιουργήθηκε από την Ευρωπαϊκή Ένωση (ΕΕ) το 2016 και τέθηκε σε ισχύ το 2018. Σχεδιάστηκε για να αντικαταστήσει την οδηγία 95/46ΕΚ για την προστασία δεδομένων του 1995 από τις 25 Μαΐου 2018. Ο κανονισμός δίνει στους πολίτες της ΕΕ νέα δικαιώματα σε σχέση με τα προσωπικά τους δεδομένα, όπως, μεταξύ άλλων, το δικαίωμα να αποσύρουν τη συγκατάθεσή τους, καθώς και ευκολότερη πρόσβαση στα δεδομένα που τους ανήκουν. Αναγκάζει τις επιχειρήσεις να αναλάβουν μεγαλύτερη ευθύνη για τα δεδομένα χρηστών τα οποία συλλέγουν και να εξασφαλίσουν ότι κάνουν ότι καλύτερο μπορούν για την προστασία των δεδομένων αυτών.

Ο σκοπός του GDPR είναι να ενημερώσει την ψηφιακή ασφάλεια για τους πολίτες της ΕΕ, παρέχοντάς τους υψηλότερο επίπεδο ελέγχου στις προσωπικές πληροφορίες που μοιράζονται στο Διαδίκτυο, καθώς και να διασφαλίσει την ιδιωτικότητα και τα προσωπικά μας δεδομένα.

Αν και ο GDPR είναι ένας νόμος που προέρχεται από την ΕΕ, ισχύει για τις επιχειρήσεις σε όλο τον κόσμο. Εφόσον υπάρχει ακόμη και η παραμικρή πιθανότητα ένας ιστότοπός να συλλέξει τα προσωπικά στοιχεία κάποιου από ένα από τα κράτη μέλη της ΕΕ, τότε ο ισότοπος αυτός θα πρέπει να συμμορφωθεί με τον νέο κανονισμό.

Δύο από τους σημαντικότερους κανονισμούς του GDPR είναι οι ακόλουθοι:

1. Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας 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)

2. Οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, διαπίστωσης και δίωξης αξιόποινων αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, και για την ελεύθερη κυκλοφορία των δεδομένων αυτών [2]

1.4 Αντικείμενο και στόχοι του GDPR.

GDPR Άρθρο 1

1. Ο παρών κανονισμός θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα.

2. Ο παρών κανονισμός προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

3. Η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

1.5 Ουσιαστικό Πεδίο εφαρμογής.

GDPR Άρθρο 2

1. Ο παρών κανονισμός εφαρμόζεται στην, εν ολω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

2. Ο παρών κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα: α) στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης, β) από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ, γ) από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας, δ) από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

3. Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα θεσμικά όργανα, φορείς, υπηρεσίες και οργανισμούς της Ένωσης, εφαρμόζεται ο κανονισμός (ΕΚ) αριθ. 45/2001. Ο κανονισμός (ΕΚ) αριθ. 45/2001 και άλλες νομικές πράξεις της Ένωσης εφαρμοστέες σε μια τέτοια επεξεργασία δεδομένων προσωπικού χαρακτήρα προσαρμόζονται στις αρχές και τους κανόνες του παρόντος κανονισμού σύμφωνα με το άρθρο 98. [3]

4. Ο παρών κανονισμός δεν θίγει την εφαρμογή της οδηγίας 2000/31/ΕΚ, ιδίως των κανόνων για την ευθύνη των μεσαζόντων παροχής υπηρεσιών που προβλέπονται στα άρθρα 12 έως 15 της εν λόγω οδηγίας.[10]

1.6 Εδαφικό πεδίο εφαρμογής.

GDPR Άρθρο 3

1. Ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης.

2. Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με: α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.

3. Ο παρών κανονισμός εφαρμόζεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου. [4]

1.7 Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

GDPR Άρθρο 5

Βάση του άρθρου 5 του ΓΚΠΔ τα προσωπικά δεδομένα προσωπικού χαρακτήρα:

α) **Νομιμότητα, αντικειμενικότητα και διαφάνεια:** Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων

β) **Περιορισμός του σκοπού:** 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.

γ) **Ελαχιστοποίηση των δεδομένων:** είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

δ) **Ακρίβεια**: 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

ε) **Περιορισμός της περιόδου αποθήκευσης**: 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

στ) **Λογοδοσία:** «Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει την συμμόρφωση...». Συνοδεύεται από πληθώρα ρυθμιστικών διατάξεων, ικανών να εξασφαλίσουν την αποτελεσματική προστασία και ασφάλεια των δεδομένων, που διαχειρίζονται οι υπεύθυνοι, εντός του πλαισίου της πλέον ισχύουσας αρχής της αυτορρύθμισης. Μερικές από αυτές είναι η υποχρέωση εκπόνησης μελέτης αντικτύπου, η γνωστοποίηση των παραβιάσεων προσωπικών δεδομένων, που έχουν λάβει χώρα τόσο στην εποπτική αρχή όσο και στο υποκείμενο των δεδομένων, ο σχεδιασμός με γνώμονα την ιδιωτικότητα τόσο κατά τον σχεδιασμό όσο και εξ ορισμού (Privacy by Design/Privacy by Default) κ.λπ.

ζ) **Ακεραιότητα και εμπιστευτικότητα:** 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 [5]

1.8 Νομιμότητα της επεξεργασίας.

GDPR Άρθρο 6

Βάση του άρθρου 6 του ΓΚΠΔ η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

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

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

γ**) Έννομη Υποχρέωση του Υπεύθυνου Επεξεργασίας:** η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας

δ**) Διαφύλαξη Ζωτικού Συμφέροντος του Υποκειμένου:** η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου

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

στ**) Έννομο Συμφέρον για σκοπούς του Υπεύθυνου Επεξεργασίας:** η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί. [6]

1.9 Προϋποθέσεις για συγκατάθεση.

GDPR Άρθρο 7

Βάση του άρθρου 7 του ΓΚΠΔ η συγκατάθεση είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

1. Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα.

2. Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Κάθε τμήμα της δήλωσης αυτής το οποίο συνιστά παράβαση του παρόντος κανονισμού δεν είναι δεσμευτικό.

3. Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.

4. Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης. [7]

1.10 Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.

GDPR Άρθρο 9

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 δικαίου της 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. [8]

ΚΕΦΑΛΑΙΟ 2

Τα δικαιώματα μας συμφωνως του κανονισμού

2.1 Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων.

GDPR Άρθρο 15

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις ακόλουθες πληροφορίες:

α) τους σκοπούς της επεξεργασίας,

β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα,

γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,

δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

ε) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία,

στ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

ζ) όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους,

η) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που προβλέπεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

2. Όταν δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτη χώρα ή σε διεθνή οργανισμό, το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερώνεται για τις κατάλληλες εγγυήσεις σύμφωνα με το άρθρο 46 σχετικά με τη διαβίβαση.

3. Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Για επιπλέον αντίγραφα που ενδέχεται να ζητηθούν από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας μπορεί να επιβάλει την καταβολή εύλογου τέλους για διοικητικά έξοδα. Εάν το υποκείμενο των δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα και εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό, η ενημέρωση παρέχεται σε ηλεκτρονική μορφή που χρησιμοποιείται συνήθως.

4. Το δικαίωμα να λαμβάνεται αντίγραφο που αναφέρεται στην παράγραφο 3 δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων. [9]

2.2 Δικαίωμα διόρθωσης.

GDPR Άρθρο 16

Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

Συμφώνα με το προοίμιο του κανονισμού, για να διασφαλιστεί ότι τα δεδομένα προσωπικού χαρακτήρα δεν διατηρούνται περισσότερο από όσο είναι αναγκαίο, ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για τη διαγραφή τους ή για την περιοδική επανεξέτασή τους. Θα πρέπει να λαμβάνεται κάθε εύλογο μέτρο, ώστε να διασφαλίζεται ότι τα δεδομένα προσωπικού χαρακτήρα που δεν είναι ακριβή διορθώνονται ή διαγράφονται. [10]

2.3 Δικαίωμα διαγραφής (δικαίωμα στη λήθη).

GDPR Άρθρο 17

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

α) τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία

β) το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) και δεν υπάρχει άλλη νομική βάση για την επεξεργασία

γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 2

δ) τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,

ε) τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας

στ) τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών που αναφέρονται στο άρθρο 8 παράγραφος 1

2. Όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα και υποχρεούται σύμφωνα με την παράγραφο 1 να διαγράψει τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, λαμβάνει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς τους υπευθύνους

επεξεργασίας τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα.

3. Οι παράγραφοι 1 και 2 δεν εφαρμόζονται στον βαθμό που η επεξεργασία είναι απαραίτητη:

α) για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση

β) για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας,

γ) για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχεία η) και θ), καθώς και το άρθρο 9 παράγραφος 3

δ) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, εφόσον το δικαίωμα που αναφέρεται στην παράγραφο 1 είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της εν λόγω επεξεργασίας ή

ε) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων. [10]

2.4 Δικαίωμα περιορισμού της επεξεργασίας. GDPR Άρθρο 18

1. Το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα:

α) η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα

β) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους

γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,

δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

2. Όταν η επεξεργασία έχει περιοριστεί σύμφωνα με την παράγραφο 1, τα εν λόγω δεδομένα προσωπικού χαρακτήρα, εκτός της αποθήκευσης, υφίστανται επεξεργασία μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους.

3. Το υποκείμενο των δεδομένων το οποίο έχει εξασφαλίσει τον περιορισμό της επεξεργασίας σύμφωνα με την παράγραφο 1 ενημερώνεται από τον υπεύθυνο επεξεργασίας πριν από την άρση του περιορισμού επεξεργασίας. [11]

2.5 Δικαίωμα στη φορητότητα των δεδομένων
GDPR Άρθρο 20

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, όταν:

α) η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) ή σε σύμβαση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) και

β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

2. Κατά την άσκηση του δικαιώματος στη φορητότητα των δεδομένων σύμφωνα με την παράγραφο 1, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητά την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό.

3. Το δικαίωμα που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου ασκείται με την επιφύλαξη του άρθρου 17. Το εν λόγω δικαίωμα δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

4. Το δικαίωμα που αναφέρεται στην παράγραφο 1 δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων. [12]

2.6 Δικαίωμα εναντίωσης.
GDPR Άρθρο 21

1. Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η οποία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο ε) ή στ), περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

2. Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση.

3. Όταν τα υποκείμενα των δεδομένων αντιτίθενται στην επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονται πλέον σε επεξεργασία για τους σκοπούς αυτούς.

4. Το αργότερο κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων, το δικαίωμα που αναφέρεται στις παραγράφους 1 και 2 επισημαίνεται ρητώς στο υποκείμενο των δεδομένων και περιγράφεται με σαφήνεια και χωριστά από οποιαδήποτε άλλη πληροφορία.

5. Στο πλαίσιο της χρήσης υπηρεσιών της κοινωνίας των πληροφοριών και με την επιφύλαξη της οδηγίας 2002/58/ΕΚ, το υποκείμενο των δεδομένων μπορεί να ασκεί το δικαίωμά του να αντιταχθεί με αυτοματοποιημένα μέσα τα οποία χρησιμοποιούν τεχνικές προδιαγραφές.

6. Όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς κατά το άρθρο 89 παράγραφος 1, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί, για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εκτός εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που ασκείται για λόγους δημόσιου συμφέροντος. [12]

ΚΕΦΑΛΑΙΟ 3

Ασφάλεια προσωπικών δεδομένων.

3.1 Ορισμός προσωπικών δεδομένων.

Ο όρος «προσωπικά δεδομένα» είναι η βασική φράση «κλειδί» στην εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Καθώς μόνο εάν η επεξεργασία δεδομένων αφορά προσωπικά δεδομένα, ισχύει ο Γενικός Κανονισμός Προστασίας Δεδομένων. Ο όρος "Προσωπικά δεδομένα" ορίζεται στο Άρθρο 4 του ΓΚΠΔ* . Τα προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία που σχετίζεται με ένα φυσικό πρόσωπο που έχει ταυτοποιηθεί ή αναγνωριστεί.

Τα **υποκείμενα των δεδομένων** είναι αναγνωρίσιμα εάν μπορούν να ταυτοποιηθούν άμεσα ή έμμεσα, ειδικά με αναφορά σε ένα αναγνωριστικό όπως ένα όνομα, έναν αριθμό ταυτοποίησης, δεδομένα τοποθεσίας, ένα διαδικτυακό αναγνωριστικό ή ένα από τα πολλά ειδικά χαρακτηριστικά, τα οποία εκφράζουν τη φυσική, φυσιολογική, γενετική , ψυχική, εμπορική, πολιτιστική ή κοινωνική ταυτότητα αυτών των φυσικών προσώπων. Στην πράξη, αυτά περιλαμβάνουν επίσης όλα τα δεδομένα που είναι ή μπορούν να εκχωρηθούν σε ένα άτομο με οποιονδήποτε τρόπο. Για παράδειγμα, ο αριθμός τηλεφώνου, πιστωτικής/χρεωστικής κάρτας ή το αναγνωριστικό εργαζομένου ενός ατόμου, τα στοιχεία λογαριασμού, ο αριθμός πινακίδας αυτοκινήτου, η εξωτερική εμφάνιση (Συνήθως φωτογραφία προσώπου), ο αριθμός πελάτη ή η διεύθυνση είναι όλα προσωπικά δεδομένα.

Δεδομένου ότι ο ορισμός περιλαμβάνει «οποιαδήποτε πληροφορία», πρέπει κανείς να υποθέσει ότι ο όρος «προσωπικά δεδομένα» πρέπει να ερμηνεύεται όσο το δυνατόν ευρύτερα. Αυτό προτείνεται επίσης στη νομολογία του Ευρωπαϊκού Δικαστηρίου, το οποίο λαμβάνει επίσης υπόψη λιγότερο σαφείς πληροφορίες, όπως καταγραφές των ωρών εργασίας που περιλαμβάνουν πληροφορίες σχετικά με την ώρα έναρξης και λήξης της εργασίας του εργαζομένου, καθώς και διαλείμματα ή ώρες που δεν εμπίπτουν στο χρόνο εργασίας, ως προσωπικά δεδομένα. Επίσης, οι γραπτές απαντήσεις από έναν υποψήφιο κατά τη διάρκεια ενός τεστ και τυχόν παρατηρήσεις του εξεταστή σχετικά με αυτές τις απαντήσεις είναι «προσωπικά δεδομένα» εάν ο υποψήφιος μπορεί να αναγνωριστεί θεωρητικά. Το ίδιο ισχύει και για τις διευθύνσεις IP. Εάν ο υπεύθυνος επεξεργασίας έχει τη νομική επιλογή να υποχρεώσει τον πάροχο να παραδώσει πρόσθετες πληροφορίες που του επιτρέπουν να προσδιορίσει τον χρήστη πίσω από τη διεύθυνση IP, αυτά είναι επίσης προσωπικά δεδομένα. Επιπλέον,

πρέπει να σημειωθεί ότι τα προσωπικά δεδομένα δεν πρέπει να είναι αντικειμενικά. Οι υποκειμενικές πληροφορίες όπως απόψεις, κρίσεις ή εκτιμήσεις μπορεί να είναι προσωπικά δεδομένα. Έτσι, αυτό περιλαμβάνει μια αξιολόγηση της πιστοληπτικής ικανότητας ενός ατόμου/επιχείρησης ή μια εκτίμηση της εργασιακής απόδοσης από έναν εργοδότη και όχι μόνο.

Τέλος, ο κανονισμός ορίζει ότι οι πληροφορίες για τη συσχέτιση ενός εργαζομένου πρέπει να αναφέρονται σε ένα φυσικό πρόσωπο και μόνο. Με άλλα λόγια, η προστασία δεδομένων δεν ισχύει για πληροφορίες σχετικά με νομικά πρόσωπα όπως εταιρείες και ιδρύματα. Για τα φυσικά πρόσωπα, από την άλλη πλευρά, η προστασία έχει πλήρη νομική ισχύ. Απλουστέρα, ένα άτομο αποκτά το δικαίωμα της προστασίας των προσωπικών του δεδομένων με τη γέννησή του και το χάνει μετά το θάνατό του. Επομένως τα δεδομένα πρέπει να εκχωρηθούν σε αναγνωρισμένα ή αναγνωρίσιμα ζωντανά άτομα για να θεωρηθούν προσωπικά.

Εκτός από τα γενικά προσωπικά δεδομένα, πρέπει κανείς να εξετάσει πάνω απ 'όλα τις ειδικές κατηγορίες προσωπικών δεδομένων (επίσης γνωστά ως ευαίσθητα προσωπικά δεδομένα) που είναι ιδιαίτερα σχετικές επειδή υπόκεινται σε υψηλότερο επίπεδο προστασίας. Αυτά τα δεδομένα περιλαμβάνουν γενετικά, βιομετρικά και δεδομένα υγείας, καθώς και προσωπικά δεδομένα που αποκαλύπτουν φυλετική και εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή ιδεολογικές πεποιθήσεις ή συμμετοχή σε συνδικαλιστικές οργανώσεις. [13]

3.2 Παραβίαση προσωπικών δεδομένων.

Πρώτα από όλα, θα αναλύσουμε τι είναι η παραβίαση προσωπικών δεδομένων. Ο GDPR το ορίζει ως «παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται σε επεξεργασία με άλλο τρόπο». Οι οδηγίες της Ομάδας Εργασίας (ΟΕ) του άρθρου 29 (η ΟΕ του άρθρου 29 ήταν η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως τις 25 Μαΐου 2018) διακρίνουν μεταξύ **περιστατικών ασφαλείας** και **παραβιάσεων προσωπικών δεδομένων**. Μια παραβίαση προσωπικών δεδομένων θα είναι πάντα ένα περιστατικό ασφαλείας, αλλά δεν θα είναι όλα τα περιστατικά ασφαλείας παραβιάσεις προσωπικών δεδομένων. [14]

3.2.1 Κατηγορίες παραβίασης προσωπικών δεδομένων.

Η ΟΕ εξήγησε ότι οι παραβιάσεις μπορούν να κατηγοριοποιηθούν σύμφωνα με τις ακόλουθες αρχές :

(i) **Εμπιστευτικότητα (Confidentiality)** - μη εξουσιοδοτημένη ή τυχαία αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα.

- Εμπιστευτικότητα σημαίνει:

▪ Πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών.

▪ Πρόληψη μη εξουσιοδοτημένης ανάγνωσης (πρόσβασης σε προσωπικά δεδομένα.

• Privacy: προστασία των προσωπικών δεδομένων.

• Secrecy: προστασία των δεδομένων που ανήκουν σε έναν οργανισμό.

(ii) **Ακεραιότητα (Integrity)** - μια μη εξουσιοδοτημένη ή τυχαία αλλοίωση των προσωπικών δεδομένων.

• Πρόληψη μη εξουσιοδοτημένης (unauthorized) μεταβολής πληροφοριών.

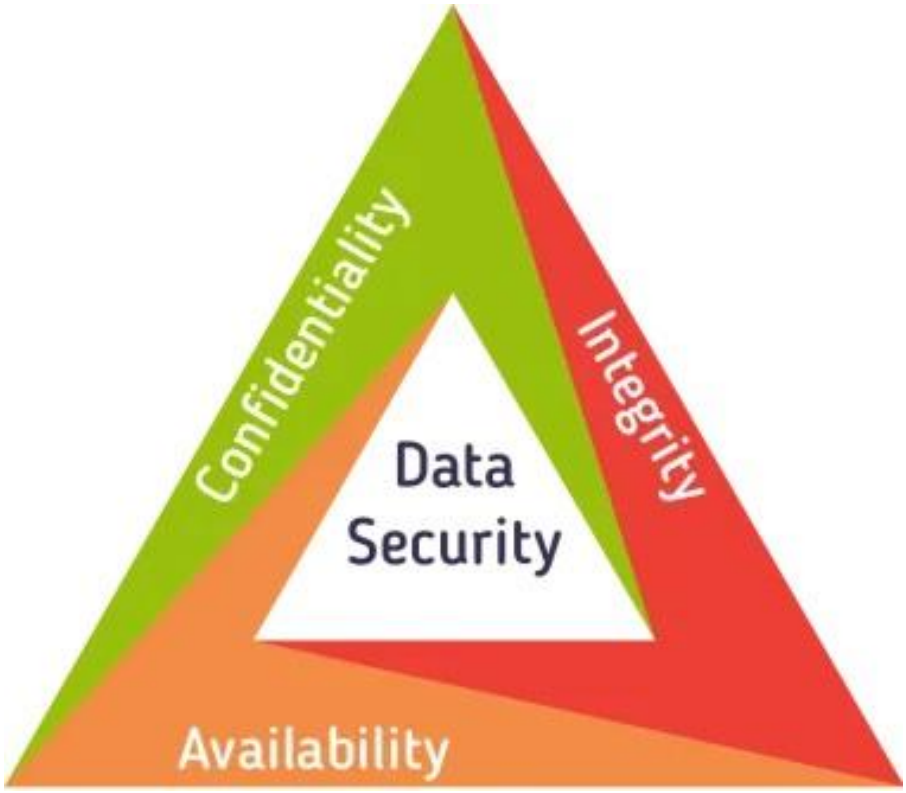
• Πρόληψη μη εξουσιοδοτημένης εγγραφής ή διαγραφής.

(iii) **Διαθεσιμότητα (Availability)** - μη εξουσιοδοτημένη ή τυχαία απώλεια πρόσβασης ή καταστροφή προσωπικών δεδομένων π.χ. διαγραφή δεδομένων κατά λάθος ή από μη εξουσιοδοτημένο άτομο, χαμένο κλειδί αποκρυπτογράφησης στην περίπτωση κρυπτογραφημένων δεδομένων ή μη διαθεσιμότητα λόγω διακοπής ρεύματος ή επίθεσης υπηρεσίας.

• Η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός ΠΣ όταν χρειάζονται από μια εξουσιοδοτημένη οντότητα.

• Άρνηση παροχής υπηρεσιών (Denial of Service (Γνωστό και ως DDoS): παρεμπόδιση εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή καθυστέρηση λειτουργιών κρίσιμων στο χρόνο (time-critical).

Είναι σημαντικό να σημειωθεί ότι μια παραβίαση διαθεσιμότητας μπορεί να συμβεί ακόμα και αν τα δεδομένα χάνονται προσωρινά ή δεν είναι διαθέσιμα, παρόλο που μια τέτοια παραβίαση ενδέχεται να μην χρειάζεται να ειδοποιηθεί, εκτός εάν είναι πιθανό να οδηγήσει σε κίνδυνο για τα δικαιώματα των ατόμων υπό τις συγκεκριμένες περιστάσεις. [15]



Εικόνα1 από:
https://www.checkmarx.com/2016/06/24/20160624the-importance-of-database-security-and-integrity

3.2.2 Παράδειγμα παραβίασης δεδομένων – Facebook.

Το παράδειγμα μας άφορα το σκάνδαλο προσωπικών δεδομένων Facebook-Cambridge Analytica όπου περιλαμβάνει τη συλλογή προσωπικών στοιχείων μέχρι και 87 εκατομμυρίων χρηστών του Facebook και σχεδόν σίγουρα πολύ μεγαλύτερο αριθμό που η Cambridge Analytica άρχισε να συλλέγει το 2014. Τα δεδομένα φέρονται να χρησιμοποιούνται για να επιχειρήσουν να επηρεάσουν τη γνώμη των ψηφοφόρων εξ ονόματος των πολιτικών που τους προσέλαβαν. Μετά την ανακάλυψη, το Facebook ζήτησε συγγνώμη εν μέσω δημόσιας κατακραυγής. Ο τρόπος με τον οποίο η Cambridge Analytica συγκέντρωσε τα δεδομένα αποκαλέστηκε "ακατάλληλος".

Τον Δεκέμβριο του 2015, η Guardian ανέφερε ότι ο γερουσιαστής των Ηνωμένων Πολιτειών Τεντ Κρουζ χρησιμοποίησε δεδομένα από αυτό το σκάνδαλο και ότι τα υποκείμενα των δεδομένων δεν γνώριζαν ότι οι εταιρείες πωλούσαν και οι πολιτικοί αγόραζαν τα προσωπικά τους στοιχεία.

Τον Μάρτιο του 2018, οι New York Times, το The Guardian και το Channel 4 News έκαναν πιο λεπτομερείς αναφορές στο σκάνδαλο των δεδομένων με νέες πληροφορίες από τον πρώην υπάλληλο της Cambridge Analytica, τον πληροφοριοδότη Christopher Wylie, ο οποίος παρείχε σαφέστερες πληροφορίες σχετικά με το μέγεθος της συλλογής δεδομένων, των προσωπικών πληροφοριών που έχουν κλαπεί και της επικοινωνίας μεταξύ Facebook, Cambridge Analytica και πολιτικών αντιπροσώπων που προσέλαβαν την Cambridge Analytica για να χρησιμοποιήσουν τα δεδομένα και για να επηρεάσουν τη γνώμη των ψηφοφόρων.

Το σκάνδαλο ήταν σημαντικό για την υποκίνηση δημόσιας συζήτησης για τα δεοντολογικά πρότυπα για τις εταιρείες κοινωνικών μέσων ενημέρωσης, τις πολιτικές συμβουλευτικές οργανώσεις και τους πολιτικούς. Οι συνήγοροι καταναλωτών ζήτησαν μεγαλύτερη προστασία των καταναλωτών στα μέσα μαζικής ενημέρωσης και το δικαίωμα στην ιδιωτική ζωή, καθώς και περιορισμό της παραπληροφόρησης και της προπαγάνδας. [16]

Η Cambridge Analytica δημοσίευσε μια μη επαληθευμένη δήλωση λέγοντας ότι τα στοιχεία που ελήφθησαν από την Kogan δεν χρησιμοποιήθηκαν στις προεκλογικές εκστρατείες του Donald Trump του 2016 και του Ted Cruz.

Το Facebook έστειλε ένα μήνυμα σε αυτούς τους χρήστες που πιστεύεται ότι έχουν επηρεαστεί, λέγοντας ότι οι πληροφορίες πιθανόν περιλάμβαναν το "δημόσιο προφίλ, τις σελίδες που τους αρέσουν, τα γενέθλια και την τρέχουσα πόλη διαμονής". Μερικοί από τους χρήστες της εφαρμογής έδωσαν στην εφαρμογή την άδεια να αποκτήσει πρόσβαση στη ροή ειδήσεων, στο χρονοδιάγραμμά της και στα μηνύματά

της.
Τα δεδομένα ήταν αρκετά λεπτομερή ώστε η Cambridge Analytica να δημιουργήσει τα ψυχογραφικά προφίλ των υποκειμένων των δεδομένων. Τα δεδομένα περιλάμβαναν επίσης τις θέσεις κάθε ατόμου. Για μια δεδομένη πολιτική εκστρατεία, τα δεδομένα ήταν αρκετά λεπτομερή ώστε να δημιουργήσουν ένα προφίλ που πρότεινε τι είδους διαφήμιση θα ήταν πιο αποτελεσματική να πείσει ένα συγκεκριμένο άτομο σε μια συγκεκριμένη τοποθεσία για κάποιο πολιτικό γεγονός.

Οι New York Times και The Guardian ανέφεραν ότι από τις 17 Μαρτίου 2018 τα δεδομένα ήταν διαθέσιμα στο ανοιχτό Διαδίκτυο και ήταν διαθέσιμα σε γενική κυκλοφορία .

Το Facebook αναγκάστηκε να καταβάλει ένα πρόστιμο ύψους 5 δισεκατομμυρίων δολαρίων ($5.000.000.000) ως μέρος μιας διευθέτησης με την Ομοσπονδιακή Επιτροπή Εμπορίου, μακράν η μεγαλύτερη ποινή που έχει επιβληθεί ποτέ σε μια εταιρεία για παραβίαση των δικαιωμάτων απορρήτου των καταναλωτών.

Μετά από αυτήν την ποινή το Facebook συμφώνησε επίσης να υιοθετήσει νέες προστασίες για τα δεδομένα που μοιράζονται οι χρήστες στο κοινωνικό δίκτυο και σε μέτρα που περιορίζουν την εξουσία του Διευθύνοντος Συμβούλου Mark Zuckerberg. [16]

3.2.3 Αναφορά της παραβίασης στην εποπτική αρχή.

Ειδοποίηση της εποπτικής αρχής.

Δεν πρέπει να κοινοποιούνται όλες οι παραβιάσεις προσωπικών δεδομένων σε εποπτική αρχή. Οι υποχρεώσεις κοινοποίησης βάσει του GDPR ενεργοποιούνται μόνο όταν υπάρχει παραβίαση προσωπικών δεδομένων που ενδέχεται να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Οι αιτιολογικές σκέψεις του GDPR εξηγούν ότι ένας τέτοιος κίνδυνος υπάρχει όταν η παραβίαση μπορεί να οδηγήσει σε φυσική, υλική ή μη υλική ζημία για υποκείμενα δεδομένων όπως:

- Διάκριση
- Κλοπή ταυτότητας ή απάτη
- Οικονομική απώλεια ή
- Ζημιά στη φήμη.

Η ΟΕ δηλώνει ότι η αξιολόγηση του κινδύνου απαιτεί αντικειμενική εξέταση της πιθανότητας και της σοβαρότητας του κινδύνου στα δικαιώματα. Οι σχετικοί παράγοντες ως μέρος αυτής της αξιολόγησης είναι:

- Το είδος της παραβίασης
- Τη φύση, την ευαισθησία και τον όγκο των εν λόγω προσωπικών δεδομένων
- Την ευκολία αναγνώρισης των ατόμων
- Τη σοβαρότητα των συνεπειών για τα άτομα
- Τα ειδικά χαρακτηριστικά των ατόμων - π.χ. μια παραβίαση που επηρεάζει ευάλωτα άτομα μπορεί να τα θέσει σε μεγαλύτερο κίνδυνο βλάβης, τον αριθμό των ατόμων που έχουν πληγεί
- Τα ειδικά χαρακτηριστικά του υπευθύνου επεξεργασίας δεδομένων - υπάρχει μεγαλύτερη απειλή εάν, για παράδειγμα, παραβιαστεί ένας ιατρικός οργανισμός που επεξεργάζεται ευαίσθητα δεδομένα.

Το παράρτημα Β των κατευθυντήριων γραμμών της ΟΕ παρέχει παραδείγματα διαφορετικών τύπων παραβιάσεων που ενέχουν κίνδυνο.

Δεν απαιτείται κοινοποίηση προς μια εποπτική αρχή εάν δεν υπάρχει κίνδυνος για τα δικαιώματα και τις ελευθερίες των ατόμων. Η ΟΕ δίνει ένα **Παράδειγμα** : Χάνεται μια ασφαλής κρυπτογραφημένη κινητή συσκευή, αλλά ο οργανισμός διατηρεί το κλειδί κρυπτογράφησης και επαρκή αντίγραφα ασφαλείας των χαμένων δεδομένων σε αυτήν την περίπτωση δεν χεριάζετε η κοινοποίηση προς μια εποπτική αρχή διότι δεν υπάρχει κίνδυνος για τα δεδομένα των ατόμων καθώς αυτά είναι κρυπτογραφημένα, αλλά ούτε υπάρχει ο κίνδυνος της μη διαθεσιμότητας καθώς ο οργανισμός διατηρεί αντίγραφα ασφαλείας.

Αναφορά στην ανεξάρτητη εποπτική αρχή για ζητήματα που επηρεάζουν άτομα από διαφορές χώρες.

Όταν μια παραβίαση επηρεάζει άτομα σε περισσότερα από ένα κράτη μέλη, ο υπεύθυνος επεξεργασίας θα πρέπει να ειδοποιήσει την κύρια εποπτική του αρχή(Στην Ελλάδα η εποπτική αρχή είναι η Αρχή Προστασίας Προσωπικών Δεδομένων).

Μπορεί επίσης να αναφέρει ένα συμβάν σε μια εποπτική αρχή (η οποία δεν είναι η κύρια αρχή της) σε ένα κράτος μέλος όπου έχουν επηρεαστεί άτομα. Ωστόσο, αυτό φαίνεται να είναι προαιρετικό και όχι υποχρεωτικό και εάν ο υπεύθυνος επεξεργασίας επιλέξει να μην το πράξει, θα πρέπει να υποδείξει στην επικεφαλής εποπτική αρχή του στην οποία τα υποκείμενα των κρατών μελών ενδέχεται να έχουν επηρεαστεί. [17]

Το χρονικό διάστημα όπου πρέπει να κατοχυρωθεί μια ειδοποίηση.

Ο GDPR δηλώνει ότι η ειδοποίηση παραβίασης προσωπικών δεδομένων σε εποπτική αρχή πρέπει να πραγματοποιηθεί "όχι αργότερα από 72 ώρες αφότου [ο υπεύθυνος επεξεργασίας] το γνωρίζει". Λοιπόν, πότε θεωρείται ένας ελεγκτής «ενήμερος» για παραβίαση; Η ΟΕ υποδηλώνει ότι όταν ένας ελεγκτής έχει «εύλογο βαθμό βεβαιότητας» έχει συμβεί ένα συμβάν ασφαλείας το οποίο έχει φέρει σε κίνδυνο τα προσωπικά δεδομένα κάποιον ανθρώπων. Τα παραδείγματα στις οδηγίες υποδηλώνουν ότι επιτυγχάνεται ένας εύλογος βαθμός βεβαιότητας όταν παρουσιαστούν στον ελεγκτή σαφείς ενδείξεις παραβίασης, π.χ. Σε περίπτωση απώλειας ενός μη κρυπτογραφημένου CD, ο ελεγκτής θα γνωρίζει μόλις συνειδητοποιήσει ότι το CD είχε χαθεί, καθώς συχνά δεν είναι δυνατό να εξακριβωθεί εάν έχει επιτευχθεί μη εξουσιοδοτημένη πρόσβαση.

Σε ορισμένες περιπτώσεις, μπορεί να χρειαστεί χρόνος για να καθοριστεί το απαιτούμενο επίπεδο βεβαιότητας. οι οδηγίες επιτρέπουν μια σύντομη περίοδο έρευνας πριν από την κοινοποίηση. Μια τέτοια έρευνα θα πρέπει να είναι άμεση και ο στόχος της πρέπει να είναι αποκλειστικά για να προσδιοριστεί αν υπήρξε παραβίαση και οι πιθανές συνέπειες για τα άτομα. Μια πιο λεπτομερής έρευνα μπορεί να πραγματοποιηθεί μετά την ειδοποίηση.

Το περιεχόμενο μίας Ειδοποίησης.

Μία ειδοποίηση προς την αρμόδια εποπτική αρχή πρέπει να περιέχει τουλάχιστον τη φύση της παραβίασης (συμπεριλαμβανομένων, όπου είναι δυνατόν, των κατηγοριών και του κατά προσέγγιση αριθμού των υποκειμένων των δεδομένων και των σχετικών αρχείων προσωπικών δεδομένων), καθώς και στοιχεία επικοινωνίας, τις πιθανές

συνέπειες της παραβίασης και τα μέτρα που λαμβάνονται ή προτείνονται να ληφθούν από τον υπεύθυνο επεξεργασίας.

Σε περιπτώσεις όπου είναι σαφές ότι υπήρξε παραβίαση, αλλά ο ελεγκτής δεν έχει συγκεντρώσει όλες τις απαιτούμενες πληροφορίες για να κάνει μια ειδοποίηση, μπορεί να γίνει ειδοποίηση σε φάσεις και καθυστερημένες ειδοποιήσεις σε κατάλληλες εξαιρετικές περιστάσεις. Κατά την επιδίωξη μίας από αυτές τις επιλογές απαιτείται από τον ελεγκτή να εξηγήσει το πιθανό εύρος και αιτία της παραβίασης και το σχέδιό του να αντιμετωπίσει την παραβίαση. [17]

Ποια αρχεία πρέπει να διατηρούνται από τους οργανισμούς.

Ο ΓΚΠΔ απαιτεί από τους υπευθύνους επεξεργασίας να τηρούν αρχεία τυχόν παραβιάσεων προσωπικών δεδομένων, ανεξάρτητα από το εάν αυτές οι παραβιάσεις πρέπει να αναφερθούν ή όχι. Αυτά τα αρχεία πρέπει να περιέχουν λεπτομέρειες για την παραβίαση, τα αποτελέσματα και τις συνέπειές της, καθώς και τυχόν διορθωτικά μέτρα που έχουν ληφθεί. Η ΟΕ προτείνει επίσης να τεκμηριώνονται οι λόγοι για τις αποφάσεις που λαμβάνονται ως απάντηση σε παραβίαση, για παράδειγμα, αιτιολόγηση για μη αναφορά παραβίασης. [17]

3.2.4 Ποινικές κυρώσεις

GDPR Άρθρο 83

1. Όποιος με πρόθεση επεμβαίνει χωρίς δικαίωμα με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα και με την επέμβαση αυτή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων , ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τηρείται με φυλάκιση.

2. Εάν οι αξιόποινες πράξεις της παραγράφου 1 αφορούν ειδικές κατηγορίες δεδομένων ή δεδομένα που αναφέρονται σε ποινικές διώξεις, μέτρα ασφαλείας ή ποινικές καταδίκες τιμωρούνται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηστική ποινή από δέκα χιλιάδες ευρώ (10.000) έως εκατό χιλιάδες (100.000) ευρώ, εάν η πράξη δεν τιμωρείτε βαρύτερα από άλλες διατάξεις.

3. Αν ο υπαίτιος των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον ή να βλάψει άλλον, τιμωρείται με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή από εκατό χιλιάδες ευρώ (100.000) έως τριακόσιες χιλιάδες ευρώ (300.000), εάν η πράξη δεν τιμωρείτε βαρύτερα από άλλες διατάξεις.

4. Αν από τις πράξεις των παραγράφων 1 έως και 3 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή από εκατό χιλιάδες ευρώ (100.000) έως τριακόσιες χιλιάδες ευρώ (300.000).

5. Υπεύθυνος προστασίας δεδομένων που παραβιάζει την υποχρέωση εχεμύθειας που τον βαρύνει στο πλαίσιο του επαγγελματικού απορρήτου ανακοινώνοντας ή αποκαλύπτοντας σε άλλον γεγονότα ή πληροφορίες που περιήλθαν σε γνώση του από τη θέση του κατά την εκτέλεση των καθηκόντων του ή επ' ευκαιρία αυτών, με σκοπό να ωφεληθεί ο ίδιος ή τρίτος, ή για να βλάψει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ή το υποκείμενο των δεδομένων ή οποιονδήποτε τρίτο τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή από δέκα χιλιάδες (10.000) ευρώ έως εκατό χιλιάδες (100.000) ευρώ, εάν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

6. Οι πράξεις των παραγράφων 1,2,3 και 5 διώκονται ύστερα από έγκληση.

7. Τα κακουργήματα που προβλέπονται στο παρόν άρθρο υπάγονται στην αρμοδιότητα του Τριμελούς Εφετείου Κακουργημάτων. [18]

Γενικότερα οι λιγότερο σοβαρές παραβάσεις θα μπορούσαν να οδηγήσουν σε πρόστιμο έως και **10 εκατομμύρια ευρώ, ή στο 2% των παγκόσμιων ετήσιων εσόδων της εταιρείας** από το προηγούμενο οικονομικό έτος, όποιο ποσό είναι υψηλότερο.

Οι πιο σοβαρές παραβιάσεις, οι οποίες έρχονται σε αντίθεση με το δικαίωμα στην ιδιωτική ζωή και με το δικαίωμα της διαγραφής. Θα μπορούσαν να οδηγήσουν σε πρόστιμο έως και **20 εκατομμύρια ευρώ ή στο 4% των παγκόσμιων ετήσιων**

εσόδων της εταιρείας από το προηγούμενο οικονομικό έτος, όποιο ποσό είναι υψηλότερο. [19]

3.2.5 Ποινικές κυρώσεις για αποτυχία αναφοράς παραβίασης.

Το πρόστιμο για την αποτυχία αναφοράς παραβίασης μπορεί να φτάσει το υψηλότερο του 2% του παγκόσμιου κύκλου εργασιών ή των 10 εκατομμυρίων ευρώ. Ωστόσο, η ΟΕ τονίζει ότι μια αποτυχία ειδοποίησης μπορεί να εμφανίζει συστηματικές αστοχίες ασφαλείας. Αυτό θα αποτελούσε χωριστή παραβίαση του GDPR και θα προσελκύσει ξεχωριστό πρόστιμο στο ίδιο επίπεδο.

Ενώ τα μέγιστα πρόστιμα στο πλαίσιο του GDPR είναι μεγάλα, η Επίτροπος Πληροφοριών του Ηνωμένου Βασιλείου δήλωσε πρόσφατα σε ένα από τα ιστολόγια της «εξιχνίαση του μύθου» ότι τα πρόστιμα θα είναι αναλογικά και δεν θα εκδίδονται σε περίπτωση κάθε παράβασης. Ο GDPR περιέχει μια λίστα παραγόντων που πρέπει να εξετάσει η εποπτική αρχή κατά τον καθορισμό του εάν θα επιβάλει πρόστιμο και το ποσό τυχόν προστίμου. Αυτό περιλαμβάνει τον βαθμό συνεργασίας του υπευθύνου επεξεργασίας με την εποπτική αρχή για την αποκατάσταση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεων της παράβασης. [19]

3.3 Κίνδυνοι παραβίασης προσωπικών δεδομένων

(i) Cyber attacks: Επιθέσεις στον κυβερνοχώρο – Σε αυτές τις επιθέσεις οι γνωστοί σε όλους μας «χάκερ» χρησιμοποιούν κακόβουλο λογισμικό, **«phishing»** ηλεκτρονικό ψάρεμα, skimming, Ransomware και συναφείς τεχνικές για να αποκτήσουν πρόσβαση σε προστατευμένες πληροφορίες. (θα αναλύσουμε τι είναι το Phishing και το Ransomware παρακάτω και το πώς μπορούμε να προστατευτούμε.

(ii) Κλοπή ή απώλεια συσκευών - Φορητοί υπολογιστές, συσκευές κινητών τηλεφώνων, σκληροί δίσκοι και άλλα μέσα αποθήκευσης δεδομένων μπορεί να χαθούν, να κλαπούν ή να απορριφθούν ακατάλληλα. Εάν αυτές οι συσκευές περιέχουν προστατευμένες πληροφορίες και καταλήξουν σε λάθος χέρια, τότε πρόκειται για παραβίαση δεδομένων.

(iii) Κλοπή δεδομένων από εργαζόμενους ή διαρροή δεδομένων - Οι εργαζόμενοι, ειδικά εκείνοι που αναχωρούν σύντομα, ενδέχεται σκόπιμα να αποκτήσουν πρόσβαση σε προστατευμένες πληροφορίες χωρίς εξουσιοδότηση με κακόβουλη πρόθεση.

(**iv) Ανθρώπινα λάθη**. Λάθη συμβαίνουν συχνά και οι άνθρωποι είναι αμελείς. Οι εργαζόμενοι αποστέλλουν κατά λάθος προσωπικά δεδομένα σε λάθος άτομο, τα ανεβάζουν δημόσια σε μέσα κοινωνικής δικτύωσης ή αφήνουν κενά ασφαλείας στον προγραμματισμό των servers που είναι αποθηκευμένα τα προσωπικά δεδομένα ώστε να είναι εμφανή σε λάθος άτομα. [20]

3.3.1 Ηλεκτρονικό ψάρεμα – Phishing

Οι εγκληματίες στον κυβερνοχώρο, γνωστοί και ως «χάκερς» είναι απίστευτα προσαρμόσιμοι. Μαθαίνουν γρήγορα νέα μέτρα ασφαλείας και βρίσκουν νέους τρόπους για να κλέψουν ευαίσθητες πληροφορίες - συχνά ατόμων που δεν είναι εξοικειωμένα με το διαδίκτυο, τους υπολογιστές και τα κινητά τηλεφωνά.

Μία από τις πιο κοινές τεχνικές που χρησιμοποιούνται για την εκμετάλλευση χρηστών του διαδικτύου είναι η απάτη ηλεκτρονικού ψαρέματος (Phishing). Η πρακτική του Phishing «ηλεκτρονικό ψάρεμα» χρησιμοποιεί τα emails/sms αλλά και πολλές φορές και μηνύματα σε Μέσα Κοινωνικής Δικτύωσης ως μέσα για την υποκλοπή προσωπικών στοιχείων του παραλήπτη (συνήθως οικονομικού χαρακτήρα), προβάλλοντας ως «δόλωμα» κάποιο ψεύτικο πρόσχημα. Τα μηνύματα αυτά λαμβάνονται συνήθως κατά την πλοήγηση στο Internet και περιέχουν παραπλανητικό περιεχόμενο.

Οι αποστολείς των μηνυμάτων Phishing υποδύονται την ταυτότητα ενός νόμιμου οργανισμού/εταιρίας ή μιας νόμιμης ιστοσελίδας, χρησιμοποιώντας μια πλαστή διεύθυνση e-mail ή/και ιστοσελίδες με στόχο να εξαπατήσουν ανυποψίαστους χρήστες και να τους πείσουν να μοιραστούν απόρρητα προσωπικά και οικονομικά δεδομένα όπως όνομα χρήστη, κωδικούς πρόσβασης, τυχόν άλλα προσωπικά ή/και οικονομικά στοιχεία (π.χ. στοιχεία πιστωτικών καρτών). Στη συνέχεια τα στοιχεία αυτά μπορούν να χρησιμοποιηθούν για την πραγματοποίηση μη εξουσιοδοτημένων / παράνομων οικονομικών συναλλαγών ή για απάτη σε βάρος των χρηστών.

Συνήθως ζητείται ο παραλήπτης να επισκεφθεί κάποια συγκεκριμένη ιστοσελίδα, μέσα από έναν υπερσύνδεσμο (link) που περιλαμβάνεται στο κείμενο, η οποία προσομοιάζει ή/και αντιγράφει ακριβώς τις οικείες ιστοσελίδες των πραγματικών εταιρειών με τις οποίες ο παραλήπτης μπορεί να έχει συνάψει συναλλακτική σχέση. [21]

Πως να εντοπίσετε κακόβουλο (Phishing) email/sms/μήνυμα?

1. Ελέγξτε ποιος είναι ο αποστολέας.

Ελέγξτε ποιος σας στέλνει το μήνυμα. Εάν ανοίγετε το email μήνυμα από τον υπολογιστή σας, μετακινείστε τον κέρσορα (ποντίκι) επάνω στο όνομα του

αποστολέα. Εάν ανοίγετε το email μήνυμα από το κινητό σας, κάντε κλικ επάνω στο όνομα του αποστολέα για να αποκαλυφθεί πλήρως η διεύθυνση email. Επίσης μετακινήστε τον κέρσορα (ποντίκι) πάνω από το link που περιέχει το μήνυμα και ελέγξτε εάν το link είναι αυτό που θα έπρεπε να είναι

Ελέγξτε εάν τα στοιχεία του αποστολέα εμφανίζονται με την συνήθη σειρά (πχ. Όνομα, επίθετο@gmail, Hotmail, yahoo.com).

2. Ελέγξτε το περιεχόμενο του μηνύματος.

● Δείτε τον τρόπο που έχει γραφτεί και υπογραφεί το μήνυμα. Ταιριάζει στον ύφος και στον τρόπο γραφής που συνηθίζει να χρησιμοποιεί ο νόμιμος αποστολέας;

● Στα email/sms Phishing συνήθως η διατύπωση δεν φαίνεται να εκπροσωπεί τη δομή του αιτήματος μιας νόμιμης εταιρείας, έχει κακή γραμματική / ορθογραφία, καθώς και πιθανές παραλλαγές στο branding (χρώμα, λογότυπο κτλ).

3. Συχνά στοιχειά ενός ύποπτου μηνύματος

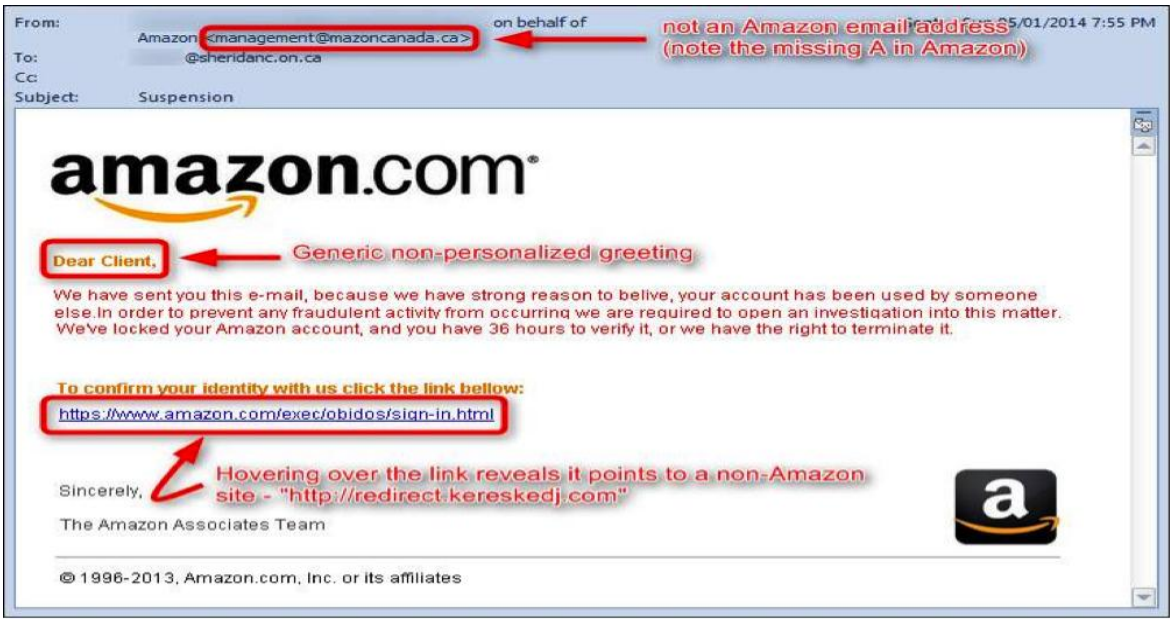
● **Ορθογραφικά και γραμματικά λάθη:** Αυτός είναι ο πιο συνηθισμένος τρόπος για να διαπιστώσετε εάν έχετε λάβει ένα δόλιο μήνυμα. Ιδρύματα ή εταιρείες, ειδικά τράπεζες, σπάνια θα σας στείλουν ένα κακό γραπτό email με ορθογραφικά ή γραμματικά λάθη.

● Ο αποστολέας ζητάει προσωπικά στοιχειά όπως **Όνομα χρηστή** και **κωδικό**: Οποιοδήποτε email ζητά διαπιστευτήρια σύνδεσης ή προσωπικά αναγνωρίσιμα στοιχεία θα πρέπει να επαληθεύεται απευθείας με τον οργανισμό.

● **Απίστευτες προσφορές**: Τα μηνύματα ηλεκτρονικού ταχυδρομείου που ισχυρίζονται ότι έχετε κερδίσει κάτι πολύ ακριβό ή ότι σας επιστρέφονται χρήματα για μια αγορά που δεν πραγματοποιήσατε ποτέ είναι κακές ειδήσεις.

● **Ύποπτη διεύθυνση E-mail του αποστολέα:** Μικρές παραλλαγές στη διεύθυνση ηλεκτρονικού ταχυδρομείου που προσπαθούν να φανούν σαν την αφεντική, αλλά δεν είναι. Για παράδειγμα, μπορείτε να κάνετε τραπεζικές συναλλαγές με ένα τραπεζικό ίδρυμα που συνήθως σας στέλνει μέσω ηλεκτρονικού ταχυδρομείου από τη διεύθυνση "name@examplebank.com", αλλά λαμβάνετε ένα μη αναμενόμενο μήνυμα ηλεκτρονικού ταχυδρομείου από τη διεύθυνση "name@accounts.examplebank.com". Μπορούν επίσης να προσπαθήσουν να αλλάξουν ένα γράμμα ή χαρακτήρα στη διεύθυνση ηλεκτρονικού ταχυδρομείου με την ελπίδα ότι ο στόχος δεν θα παρατηρήσει.

● **Ύποπτο μήνυμα με συνημμένο αρχείο:** Εάν λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από έναν άγνωστο αποστολέα που συνοδεύεται από ένα συνημμένο που δεν περιμένατε, μην κάνετε κλικ ή λήψη του. Υπάρχει πιθανότητα ότι κάποιος «χάκερ» σας έστειλε κακόβουλο λογισμικό ή ένα μήνυμα Ransomware: για να κλέψει τα στοιχεία σας ή να έχει πρόσβαση στον υπολογιστή σας.



Εικόνα 2 από:
https://www.identityiq.com/scams-and-fraud/what-is-phishing-prevent-attacks-with-common-examples/

Στην φωτογραφία βλέπουμε ότι ο αποστολέας έχει:

1^{ον} Διαφορετική διεύθυνση E-mail από την κανονική διεύθυνση του Amazon

2^{ον} Χρησιμοποίει απρόσωπο χαιρετισμό “Dear client”

3^{ον} Χρησιμοποίει τα λογότυπα της εταιρίας για να δείξει ότι το μήνυμα είναι αφεντικό και να ξεγελάσει τον παραλήπτη

4^{ον} Εάν μετακινήσουμε τον κέρσορα επάνω στο link θα δούμε ότι το link δεν θα μας παραπέμψει στην σελίδα του Amazon αλλά θα μας παραπέμψει σε μια ιστοσελίδα που σίγουρα θα βλάψει τον υπολογιστή μας ή τα προσωπικά μας δεδομένα.

Τρόποι αντιμετώπισης

- Αγνόηση του μηνύματος.
- Σε καμιά περίπτωση, απάντηση του μηνύματος ή προώθηση του.
- Σε καμία περίπτωση δεν δίνουμε τα προσωπικά σας στοιχεία.
- Άμεση διαγραφή τέτοιου είδους παραπλανητικών μηνυμάτων (emails/sms).
- Ενημέρωση του Ιδρύματος/Εταιρίας για το περιστατικό. [21]

3.3.2 Επίθεση κακόβουλου λογισμικού τύπου Ransomware.

Ransomware ορισμός

Το Ransomware είναι κακόβουλο λογισμικό που μπορεί να κλειδώσει μια συσκευή ή να κρυπτογραφήσει τα περιεχόμενά της, προκειμένου να ζητήσει χρήματα ως λύτρα από τον ιδιοκτήτη της. Σε αντάλλαγμα, οι δημιουργοί του κακόβουλου κώδικα υπόσχονται - φυσικά, χωρίς καμία εγγύηση - να αποκαταστήσουν την πρόσβαση στο μολυσμένο μηχάνημα ή τα δεδομένα.

Το συγκεκριμένο είδος κακόβουλου λογισμικού χρησιμοποιείται για εκβιασμούς. Όταν επιτίθεται σε μια συσκευή με επιτυχία, το κακόβουλο λογισμικό "κλειδώνει" την οθόνη ή κρυπτογραφεί τα δεδομένα που είναι αποθηκευμένα στο δίσκο. Στη συνέχεια, εμφανίζει μια απαίτηση καταβολής λύτρων με αναλυτικές λεπτομέρειες πληρωμής.

Οι επιτήδειοι «χάκερς» απαιτούν λύτρα, συχνά ζητώντας η πληρωμή να γίνει σε bitcoin ή κάποιο άλλο ψηφιακό νόμισμα, καθιστώντας έτσι αδύνατο τον εντοπισμό της συναλλαγής. Σε αντάλλαγμα, οι επιτιθέμενοι υπόσχονται να αποκρυπτογραφήσουν τα δεδομένα ή να αποκαταστήσουν την πρόσβαση στη μολυσμένη συσκευή.

Πρέπει να τονίσουμε ότι δεν υπάρχει καμία εγγύηση ότι οι κυβερνοεγκληματίες θα τηρήσουν τη δική τους πλευρά της συμφωνίας (μάλιστα, μερικές φορές δεν είναι καν σε θέση να το πράξουν, είτε εκ προθέσεως είτε εξαιτίας κακού προγραμματισμού). Ως εκ τούτου ειδικοί συνιστούν να μην καταβάλετε το απαιτούμενο ποσό των λύτρων - τουλάχιστον μέχρι να επικοινωνήσετε με την δίωξη ηλεκτρονικού εγκλήματος για να εξεταστεί, τι δυνατότητες υπάρχουν για την αποκρυπτογράφηση των αρχείων σας.

Συχνοί στόχοι των «χάκερς» μέσω του Ransomware

Υπάρχουν διάφοροι τρόποι με τους οποίους οι εισβολείς επιλέγουν τους οργανισμούς

που στοχεύουν με ransomware. Μερικές φορές είναι θέμα ευκαιρίας: για παράδειγμα, οι επιτιθέμενοι ενδέχεται να στοχεύουν πανεπιστήμια επειδή τείνουν να έχουν μικρότερες ομάδες ασφαλείας και μια διαφορετική βάση χρηστών που κάνει πολλή κοινή χρήση αρχείων, καθιστώντας ευκολότερη τη διείσδυση στην άμυνα τους.

Από την άλλη πλευρά, ορισμένοι οργανισμοί είναι δελεαστικοί στόχοι, επειδή φαίνεται να είναι πιο πιθανό να πληρώσουν γρήγορα λύτρα. Για παράδειγμα, κυβερνητικές υπηρεσίες ή ιατρικές εγκαταστάσεις συχνά χρειάζονται άμεση πρόσβαση στα αρχεία τους. Οι δικηγορικές εταιρείες και άλλοι οργανισμοί με ευαίσθητα δεδομένα ενδέχεται να είναι διατεθειμένοι να πληρώσουν όσο το δυνατόν πιο γρήγορα ώστε να μην δημιουργηθεί πρόβλημα με τους πελάτες τους και την φήμη της εταιρίας τους. Οπότε αυτοί οι οργανισμοί είναι μοναδικά ευαίσθητοι σε επιθέσεις με κακόβουλο λογισμικό τέτοιου είδους.

Αλλά δεν πρέπει να αισθανόμαστε ασφαλείς εάν επειδή δεν ανήκουμε σε αυτές τις κατηγορίες. Καθώς ορισμένα ransomware εξαπλώνονται αυτόματα και αδιάκριτα στο Διαδίκτυο.

Παράδειγμα Ransomware (WannaCry)

Το WannaCry είναι ένα worm (σκουλήκι) ransomware που εξαπλώθηκε γρήγορα σε διάφορα δίκτυα υπολογιστών τον Μάιο του 2017. Αφού μολύνει υπολογιστές με Windows, κρυπτογραφεί αρχεία στον σκληρό δίσκο του υπολογιστή, καθιστώντας τα αδύνατα για πρόσβαση στους χρήστες και, στη συνέχεια, απαιτεί πληρωμή λύτρων σε bitcoin. για να τις αποκρυπτογραφήσουμε.

Η ενημέρωση που απαιτείται για την πρόληψη των μολύνσεων της WannaCry ήταν διαθέσιμη πριν από την έναρξη της επίθεσης: Η Microsoft στις 14 Μαρτίου 2017, ενημέρωσε την εφαρμογή των Windows για το πρωτόκολλο SMB για να αποτρέψει τη μόλυνση μέσω του EternalBlue. Ωστόσο, παρά το γεγονός ότι η Microsoft είχε επισημάνει την ενημέρωση λογισμικού ως **κρίσιμη ενημέρωση**, πολλά συστήματα δεν είχαν εγκαταστήσει την ενημέρωση μέχρι τον Μάιο του 2017 όπου η WannaCry ξεκίνησε την ταχεία εξάπλωσή της.

Για εκείνα τα μη ενημερωμένα συστήματα που έχουν μολυνθεί, η μονή λύση είναι η επαναφορά αρχείων από ένα ασφαλές αντίγραφο ασφαλείας «backup» (εάν υπήρχε) - οπότε ας γίνει μάθημα σε όλους μας μάθημα ότι πρέπει πάντα να δημιουργούμε αντίγραφα ασφαλείας των αρχείων σας, καθώς και ότι πρέπει να ενημερώνουμε το λογισμικό των συσκευών μας. [22]

3.3.3 Μέτρα ασφαλείας από κακόβουλο λογισμικό.

● Διατηρήστε το λειτουργικό σας σύστημα ενημερωμένο για να διασφαλίσετε ότι έχετε λιγότερες ευπάθειες για εκμετάλλευση.

● Μην ευκατάστατε λογισμικό (εφαρμογές κλπ) και μην του δίνετε δικαιώματα διαχειριστή, εκτός εάν γνωρίζετε ακριβώς περί τίνος πρόκειται

● Εγκαταστήστε λογισμικό προστασίας από ιούς **(Antivirus),** το οποίο εντοπίζει κακόβουλα προγράμματα όπως ransomware κατά την άφιξή τους και λογισμικό επιτρεπόμενων, το οποίο εμποδίζει την εκτέλεση μη εξουσιοδοτημένων εφαρμογών.

● Δημιουργία αντίγραφων ασφαλείας αρχείων και δεδομένων **(Backup)** Όσο συχνότερα γίνετε και αν είναι εφικτό και αυτόματα! Αυτό δεν θα σταματήσει μια επίθεση κακόβουλου λογισμικού, αλλά μπορεί να κάνει τη ζημιά που θα προκληθεί πολύ μικρότερη, καθώς τα αρχεία σας θα είναι ασφαλή και δεν θα έχουν χαθεί.

● Δημιουργία **σύνθετων κωδικών πρόσβασης**. Η δημιουργία ισχυρών, μοναδικών κωδικών πρόσβασης για όλους τους κρίσιμους λογαριασμούς σας είναι πραγματικά ο καλύτερος τρόπος για να διατηρήσετε τα προσωπικά και οικονομικά στοιχεία σας ασφαλή.

● **Μην** χρησιμοποιείτε τον **ίδιο κωδικό πρόσβασης** για πολλούς λογαριασμούς, ένας εισβολέας μπορεί να πάρει τα δεδομένα που έχουν διαρρεύσει από μία επίθεση και να τα χρησιμοποιήσει για να συνδεθεί στους άλλους λογαριασμούς σας. Η καλύτερη λύση είναι να χρησιμοποιούμε έναν Ισχυρό κωδικό πρόσβασης ο οποίος να περιέχει Κεφαλαία και πεζά γράμματα καθώς και σύμβολα.

● Ελέγξτε αν οι διαδικτυακοί λογαριασμοί σας προσφέρουν έλεγχο ταυτότητας πολλών παραγόντων (**Two Factor Authentication (2FA)**). Αυτό συμβαίνει όταν απαιτούνται πολλά στοιχεία για την επαλήθευση της ταυτότητάς σας. Έτσι, για να συνδεθείτε σε έναν λογαριασμό, χρειάζεται να εισαγάγετε έναν κωδικό που αποστέλλεται στο τηλέφωνό σας, καθώς και τον κωδικό πρόσβασης και τη φράση πρόσβασης. Με αυτόν τον τρόπο αποτρέπουμε τους «χάκερς» να εισβάλουν στους λογαριασμούς μας καθώς δεν αρκεί το να μάθουν τον κωδικό μας για να εισέρθουν. [23]

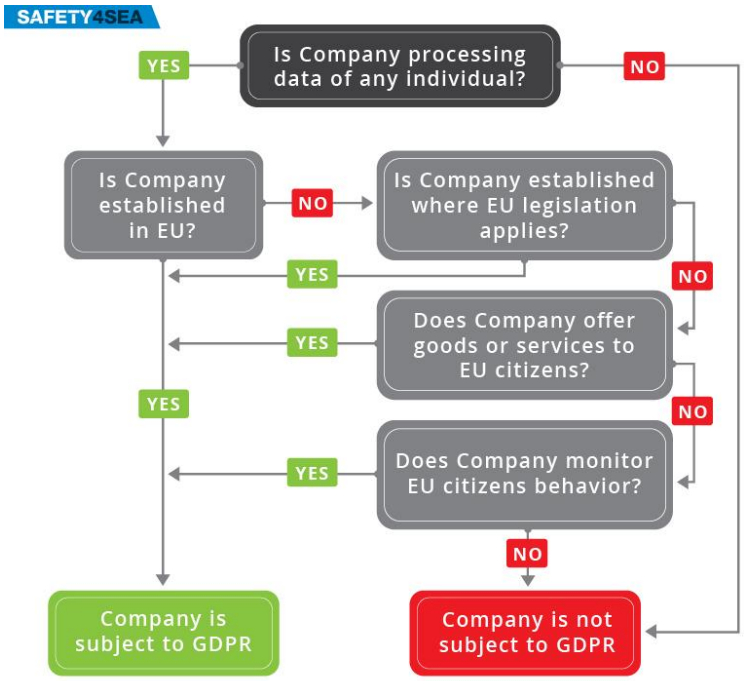
ΚΕΦΑΛΑΙΟ 4

Ο ΓΚΠΔ στον ναυτιλιακό κλάδο

4.1 Συμμόρφωση με τον κώδικα

Οι ναυτιλιακές εταιρείες αποθηκεύουν και διαχειρίζονται μεγάλο αριθμό προσωπικών δεδομένων, για παράδειγμα πληροφορίες επιβατών, στοιχεία μέλους πληρώματος, ταξιδιωτικά έγγραφα, εκπαιδευτικά αρχεία, τραπεζικά στοιχεία και άλλες πληροφορίες που συλλέγονται κατά τη συνήθη πορεία της επιχείρησης. Γι αυτό τον λόγο δεν μπορούν να εξαιρεθούν από τον κανονισμό, όλα τα ιδρύματα που επεξεργάζονται η έχουν στην κατοχή τους προσωπικά δεδομένα, πρέπει να ακλουθούν τις οδηγίες του κανονισμού. Επιπλέον, οι ναυτιλιακές εταιρείες είναι πολύ πιθανό να κοινοποιήσουν αυτές τις πληροφορίες σε τρίτους, όπως λιμενικούς πράκτορες και συλλόγους P&I.

Στον ΓΚΠΔ δεν υπόκεινται μόνο οι ναυτιλιακές εταιρίες αλλά και άλλοι στον ναυτιλιακό χώρο όπως: Ναύλο-Μεσίτες, επιθεωρητές, ναυτικοί πράκτορες, εξωτερικοί συνεργάτες παροχής ναυτιλιακών υπηρεσιών, οι οποίοι ασχολούνται πολύ συχνά με προσωπικά δεδομένα, μερικές φορές και ευαίσθητα. Για παράδειγμα, μία αναφορά τραυματισμού ενός ναυτικού. Στην περίπτωση αυτή, ο ενάγων, δηλαδή το υποκείμενο των δεδομένων - θα έχει όλα τα δικαιώματα που παρέχει ο ΓΚΠΔ. Επίσης θα πρέπει να γνωρίζουμε ότι τα εμπορικά δεδομένα ναυτιλιακών εταιριών όπως το έγγραφο φορτώσεως (Bill of Lading) ή άλλα έγγραφα όπως το Έγγραφο των στοιχείων του πλοίου (Ship’s Particulars) δεν υπόκεινται στον ΓΚΠΔ εκτός εάν τα εμπορικά δεδομένα περιλαμβάνουν προσωπικά δεδομένα. [24]



Πότε πρέπει να γίνετε συμμόρφωση με τον ΓΚΠΔ
Εικονα3 από:
https://safety4sea.com/cyber-security-eu-gdpr-framework/

4.1.1 Συμμόρφωση μίας ναυτιλιακής εταιρίας με τον ΓΚΠΔ

Προκειμένου να συμμορφωθεί με τον GDPR, μία ναυτιλιακή εταιρία πρέπει να ακολουθήσει αυτά τα 8 πρακτικά και ουσιαστικά βήματα:

Ενημέρωση (Awareness): να γνωρίζει ότι ο νόμος αλλάζει στον GDPR. Όλοι οι άνθρωποι ενός οργανισμού πρέπει να κατανοήσουν τον αντίκτυπο αυτής της νέας νομοθεσίας.

Έλεγχος πληροφοριών (Information audit) : Η εταιρία θα πρέπει να αξιολογεί ποια προσωπικά δεδομένα διατηρεί, από πού προέρχονται και σε ποιους κοινοποιούνται. Ο έλεγχος διεξάγεται συνήθως από την νομική ομάδα της εταιρίας ή επαγγελματικές εταιρείες με εμπειρία σε θέματα απορρήτου.

Σχέδιο ειδοποίησης απορρήτου (Draft privacy notice): μετά την ολοκλήρωση του ελέγχου, είναι δυνατό να καταρτιστεί μια προσαρμοσμένη πολιτική απορρήτου σύμφωνα με τους τύπους προσωπικών δεδομένων που επεξεργάζεται ο οργανισμός. Συνιστάται σε ορισμένους οργανισμούς να καταρτίσουν διάφορες πολιτικές απορρήτου, για παράδειγμα, μια που περιέχει συγκεκριμένη διατύπωση όπου

συλλέγονται δεδομένα ειδικής κατηγορίας, μία άλλη για εμπορική χρήση και μία άλλη για σκοπούς HR.

DPO: όπου απαιτείται, οι εταιρίες θα πρέπει να προσλάβουν έναν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer). Ένας οργανισμός υποχρεούται να διορίσει έναν ΥΠΔ - δηλαδή κάποιον που θα αναλάβει την ευθύνη για τη συμμόρφωση με την προστασία δεδομένων - όπου πραγματοποιεί την τακτική και συστηματική παρακολούθηση των ατόμων σε μεγάλη κλίμακα ή, πραγματοποιεί την ευρεία επεξεργασία ειδικών κατηγοριών δεδομένων όπως: αποτελέσματα εξετάσεων υγείας ή πληροφορίες σχετικά με ποινικό μητρώο του κάθε εργαζομένου. Ένας αρμόδιος υπεύθυνος προστασίας δεδομένων μπορεί να φέρει τεχνική εμπειρία και η βοήθεια του να αποφέρει τεράστια εξοικονόμηση χρόνου.

Συγκατάθεση (Consent): έλεγχος στον τρόπο με τον οποίο η εταιρία λαμβάνει, καταγράφει και διαχειρίζεται τη συγκατάθεση. Η συγκατάθεση πρέπει να είναι συγκεκριμένη, σαφής, εμφανής, κατάλληλα τεκμηριωμένη και να αποσύρεται με την ίδια ευκολία με την οποία δίνετε.

Δικαιώματα εργαζομένων: έλεγχος στη διαδικασία παροχής των δικαιωμάτων και βεβαίωση ότι καλύπτονται όλα τα δικαιώματα που έχουν οι εργαζόμενοι της εταιρίας. Σύμφωνα με τον GDPR, οι εργαζόμενοι έχουν τα εξής δικαιώματα: ενημέρωσης, πρόσβασης, διόρθωσης, διαγραφής, κ.ο.κ όπως είδαμε και στο Κεφάλαιο 2. Επομένως, μία εταιρία, θα πρέπει να είναι έτοιμη να αντιδράσει εάν κάποιος ζητήσει να διαγραφούν ή να τροποποιηθούν τα προσωπικά του δεδομένα.

Παραβιάσεις δεδομένων (Data Breaches): βεβαιωθείτε ότι υπάρχουν οι κατάλληλες διαδικασίες για τον εντοπισμό, την αναφορά και τη διερεύνηση παραβίασης προσωπικών δεδομένων, το λεγόμενο Σχέδιο Αναφοράς Περιστατικών (Incident Report Plan). Οι αρχές πρέπει να ενημερώνονται για τυχόν παραβίαση των κανονισμών εντός 72 ωρών από την εκδήλωση, όπως αναφέραμε και στο Κεφάλαιο 3.

Εκπαίδευση: βεβαιωθείτε ότι το προσωπικό της εταιρίας είναι εκπαιδευμένο σχετικά με τη συμμόρφωση με τον GDPR. Ένα σεμινάριο ενημέρωσης σχετικά με τον ΓΚΠΔ μαζί με μία καλή περιοδική εκπαίδευση θα ήταν κατάλληλο σε ορισμένες περιπτώσεις. [24]

4.2 Ενέργειες που πρέπει να ληφθούν από τους εργαζόμενους.

Σε σχέση με τη διαχείριση του πληρώματος, οι εργαζόμενοι οι οποίοι επεξεργάζονται η έχουν στην κατοχή τους προσωπικά δεδομένα θα πρέπει να λάβουν υπόψη τις ακόλουθες βασικές ενέργειες ως μέρος του ευρύτερου προγράμματος συμμόρφωσης GDPR:

● **Έλεγχος των πληροφοριών** του πληρώματος που διαχειρίζεται κάθε εργαζόμενος για να διαπιστώσει εάν λειτούργει σαν «επεξεργαστής δεδομένων – (Data Processor)» ή σαν «ελεγκτής δεδομένων – (Data Controller)» των προσωπικών δεδομένων του πληρώματος.

Ο ελεγκτής δεδομένων αποφασίζει τους σκοπούς και τα μέσα επεξεργασίας των προσωπικών δεδομένων.

Ο επεξεργαστής δεδομένων είναι υπεύθυνος για την επεξεργασία προσωπικών δεδομένων υπό την επίβλεψη του ελεγκτή δεδομένων. Επίσης στον επεξεργαστή των δεδομένων, ο GDPR επιβάλλει συγκεκριμένες νομικές υποχρεώσεις για τη διατήρηση αρχείων προσωπικών δεδομένων και δραστηριοτήτων επεξεργασίας που σχετίζονται με αυτό.

Ωστόσο, ο GDPR επιβάλλει πρόσθετες υποχρεώσεις στους ελεγκτές δεδομένων, για να διασφαλίσει ότι τα δεδομένα παραμένουν σωστά ελεγχόμενα / ασφαλή εάν αυτά μεταβιβάζονται σε τρίτους.

● **Προσδιορισμός του νομικό πλαισίου** για την επεξεργασία προσωπικών δεδομένων που σχετίζονται με το πλήρωμα - ο υπεύθυνος επεξεργασίας δεδομένων, θα πρέπει να καθορίσει ένα έγκυρο νομικό πλαίσιο για την επεξεργασία προσωπικών δεδομένων του πληρώματος στην εταιρία.

● **Συμπλήρωση του «αρχείου επεξεργασίας»** - οι υπεύθυνοι επεξεργασίας δεδομένων και οι υπεύθυνοι επεξεργασίας δεδομένων είναι υπεύθυνοι για τη διατήρηση ενός «αρχείου επεξεργασίας» που καταγράφει τις δραστηριότητες επεξεργασίας των προσωπικών δεδομένων. Τα μέλη πρέπει να διασφαλίζουν ότι τα αρχεία επεξεργασίας δεδομένων αναφέρουν λεπτομερώς τις δραστηριότητες επεξεργασίας δεδομένων που αναλαμβάνονται σε σχέση με το πλήρωμά τους.

● **Σημειώσεις απορρήτου (Privacy Notices)** – Σε αυτές τις σημειώσεις αναγράφετε ο τρόπος συλλογής και επεξεργασίας των δεδομένων από την εταιρία. Ο ΓΚΠΔ καθορίζει τις πληροφορίες που πρέπει να παρέχετε στους ιδιοκτήτες των δεδομένων κατά τη συλλογή και την επεξεργασία προσωπικών δεδομένων.

● Συμβάσεις - επανεξέταση τυχόν συμβάσεων τρίτων που σχετίζονται με την επεξεργασία προσωπικών δεδομένων και βεβαίωση ότι πληρούν τις απαιτήσεις του ΓΚΠΔ. Οι εργαζόμενοι ενδέχεται να χρειαστεί να αναζητήσουν συγκεκριμένες νομικές συμβουλές σε αυτόν τον τομέα, προκειμένου να διασφαλιστεί ότι οι ρυθμίσεις επεξεργασίας δεδομένων συμμορφώνονται με το GDPR.

● **Εξέταση των τοπικών κανονισμών** - Εάν βρισκόμαστε εκτός Ευρώπης, θα πρέπει να συμμορφωθούμε με τους τοπικούς κανονισμούς σχετικά με θέματα προστασίας δεδομένων και απορρήτου. Ο ΓΚΠΔ ισχύει επίσης εάν οι υπηρεσίες που παρέχει η εταιρία άφορα άτομα της Ε.Ε ή εάν επεξεργάζεστε προσωπικά δεδομένα που σχετίζονται με άτομα που βρίσκονται στην Ευρωπαϊκή Ένωση.

● Απαγόρευση μεταφοράς δεδομένων προσωπικού χαρακτήρα εκτός του Ευρωπαϊκού Οικονομικού Χώρου σε χώρα η οποία, κατά την άποψη της Ευρωπαϊκής Επιτροπής βάση ΓΚΠΔ, δεν διαθέτει επαρκή προστασία δεδομένων, εκτός εάν υπάρχουν πρόσθετες διασφαλίσεις.

● Όλοι οι εργαζόμενοι θα πρέπει να γνωρίζουν εάν διατηρούν ή επεξεργάζονται δεδομένα ειδικής κατηγορίας (δεδομένα που αποτελούνται από φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα σχετικά με την υγεία ή δεδομένα σχετικά με τη σεξουαλική ζωή ενός φυσικού ατόμου) καθώς και να γνωρίζουν:

▪ Το νομικό πλαίσιο για την επεξεργασία αυτών των πληροφοριών

▪ Τους λόγους για την επεξεργασία δεδομένων ειδικής κατηγορίας και τον τρόπο συγκατάθεσης των υποκειμένων. Όπως αυτοί αναφέρονται λεπτομερώς στο άρθρο 9 του ΓΚΠΔ [25]

4.3 Κίνδυνοι παραβίασης προσωπικών δεδομένων για την εταιρία.

Οι απειλές στον κυβερνοχώρο έχουν γίνει μέρος της καθημερινής ναυτιλιακής εταιρίας, ειδικά στις μέρες μας που όλο και περισσότερες επιχειρήσεις γίνονται ψηφιακά εξαρτώμενες. Εσωτερικές - Εξωτερικές επικοινωνίες, κάθε είδους λειτουργίες φορτίου, πλοήγηση, λειτουργίες έρματος, συμβάσεις, ναύλωση κ.λπ.

Ενώ πολλοί μπορεί να υποστηρίξουν ότι κανένας από τους παραπάνω τύπους λειτουργίας δεν περιλαμβάνει προσωπικά δεδομένα - και αυτό είναι εν μέρει αλήθεια - στην πραγματικότητα, τα δεδομένα των ναυτικών ή του προσωπικού στο γραφείου, όπως ονόματα, εθνικότητες, πληροφορίες επαφών κ.λπ., περιλαμβάνονται στην πραγματικότητα σε πολλά έγγραφα ως ανά αίτημα σε καθημερινές δραστηριότητες. Επομένως, απαιτείται μια προληπτική προσέγγιση για την προστασία από παραβιάσεις όλων των δεδομένων που εμφανίζονται στα αρχεία.

Οι 5 κίνδυνοι για την εταιρία

Είναι συναρπαστικό το γεγονός ότι το 93% των επιτυχημένων παραβιάσεων δεδομένων συμβαίνουν σε λιγότερο από ένα λεπτό. Ωστόσο, το 80% των επιχειρήσεων χρειάζονται εβδομάδες για να συνειδητοποιήσουν μια παραβίαση.

Υπάρχουν πολλές δαπανηρές συνέπειες των παραβιασμένων δεδομένων. Αυτός είναι ο λόγος για τον οποίο το 86% των στελεχών επιχειρήσεων πιστεύουν ότι απειλές για την ασφάλεια στον κυβερνοχώρο, όπως η αδύναμη ασφάλεια δεδομένων, είναι ανησυχητικές.

1. Απώλεια εσόδων

Η σημαντική απώλεια εσόδων ως αποτέλεσμα παραβίασης της ασφάλειας είναι κοινή. Μελέτες δείχνουν ότι το 29% των επιχειρήσεων που αντιμετωπίζουν παραβίαση δεδομένων καταλήγουν να χάνουν έσοδα. Από αυτούς που έχασαν έσοδα, το 38% παρουσίασε απώλεια 20% ή περισσότερο.

Ένας μη λειτουργικός ιστότοπος, για παράδειγμα, μπορεί να αναγκάσει τους πιθανούς

πελάτες να εξερευνήσουν άλλες επιλογές. Ωστόσο, οποιαδήποτε διακοπή του συστήματος πληροφορικής μπορεί να οδηγήσει σε διακοπές της εργασίας.

2. Ζημιά στη φήμη της εταιρίας

Μια παραβίαση ασφαλείας μπορεί να επηρεάσει πολύ περισσότερο τα βραχυπρόθεσμα έσοδά της εταιρίας από ότι περιμένει κανείς. Διακινδυνεύει επίσης η μακροπρόθεσμη φήμη της επωνυμίας της εταιρίας.

Είναι σίγουρο, ότι καμία εταιρία δεν θέλει να διαρρεύσουν τα email της. Στις περισσότερες περιπτώσεις, αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει να διασφαλίζετε ότι θα παραμείνουν απόρρητα
Ωστόσο, οι πελάτες εκτιμούν επίσης το απόρρητό που τους διασφαλίζει η κάθε εταιρία - και οι παραβιάσεις περιλαμβάνουν συχνά πληροφορίες πληρωμής πελατών.

Οι δυνητικοί πελάτες θα διστάσουν να εμπιστευτούν μια επιχείρηση με ιστορικό κακής ασφάλειας δεδομένων.

3. Απώλεια πνευματικής ιδιοκτησίας

Η απώλεια εσόδων και η ζημιά της φήμης μπορεί να είναι άκρως καταστροφικές. Ωστόσο, σε ορισμένες περιπτώσεις, οι γνωστοί «χάκερ» θα στοχεύσουν επίσης σε σχέδια, στρατηγικές και σχεδιαγράμματα πολύτιμης αξίας για κάθε εταιρία.

Οι επιχειρήσεις στη μεταποιητική και κατασκευαστική βιομηχανία (Ναυπηγικές βιομηχανίες ή και εταιρίες παροχής ναυτικών ηλεκτρονικών οργάνων) είναι πιο επιρρεπείς σε αυτήν την απειλή. Οι μικρότερες επιχειρήσεις τείνουν να πιστεύουν ότι δεν θα χτυπηθούν. Αλλά το 60% των γνωστών «χακερς» στοχεύουν μικρές επιχειρήσεις. Αυτό συμβαίνει επειδή είναι πιο εύκολο να τις επιτεθούν.

Η απώλεια πνευματικής ιδιοκτησίας μπορεί να επηρεάσει την ανταγωνιστικότητα της επιχείρησής. Ορισμένοι αντίπαλοι δεν θα δίσταζαν να εκμεταλλευτούν τις κλεμμένες πληροφορίες.

4. Κρυφές δαπάνες

Οι επιφανειακές δαπάνες είναι μόνο η αρχή. Υπάρχουν επίσης πολλές κρυφές δαπάνες που σχετίζονται με παραβιάσεις δεδομένων.

Για παράδειγμα, οι νομικές αμοιβές ενδέχεται να τεθούν σε εφαρμογή. Επίσης, ενδέχεται μία εταιρία να χρειαστεί να ξοδέψει περισσότερα για τις δημόσιες σχέσεις και τις έρευνες, καθώς είναι σίγουρο για τις αυξήσεις των ασφαλίστρων.

Τα κανονιστικά πρόστιμα είναι μια άλλη πραγματικότητα που πολλές επιχειρήσεις αγνοούν. Το 2015, για παράδειγμα, η FCC χτύπησε την AT&T με πρόστιμο 25 εκατομμυρίων δολαρίων. Αυτό ήταν αποτέλεσμα παραβίασης που οδήγησε στην αποκάλυψη πληροφοριών που σχετίζονται με χιλιάδες λογαριασμούς. Αξίζει να σημειωθεί ότι η κάλυψη για πρόστιμα GDPR απαιτεί πράγματι να έχουν ληφθεί όλα τα εύλογα μέτρα για την αποφυγή της παραβίασης ώστε να αποζημιωθεί μια εταιρία από τα P&I clubs.

5. Διαδικτυακός βανδαλισμός

Μερικοί «χάκερ» χρησιμοποιούν αυτήν την μέθοδο μόνο για την προσωπική τους ικανοποίηση στο γεγονός ότι κατάφεραν να εισέρθουν στο σύστημα. Σε αυτές τις περιπτώσεις, μια παραβίαση ασφαλείας μπορεί να οδηγήσει μόνο σε λίγες αλλαγές λέξεων στον ιστότοπό σας.

Ενώ αυτό φαίνεται σχετικά αβλαβές, στην πραγματικότητα μπορεί να προκαλέσει μεγάλη ζημιά. Οι λεπτές αλλαγές είναι πιο δύσκολο να παρατηρηθούν.

Για παράδειγμα, ένας εισβολέας ενδέχεται να αλλάξει μερικά γράμματα ή αριθμούς στη σελίδα επαφών σας. Μπορούν επίσης να προσθέσουν χυδαίο περιεχόμενο σε ορισμένες από τις ιστοσελίδες σας. [26]

Βιβλιογραφία

[1] Ιστορικό της ψήφισης του ΓΚΠΔ
https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[2] Τι είναι ο ΓΚΠΔ, ποιος είναι ο σκοπός του,
https://gdpr.eu/what-is-gdpr/

[3] ΓΚΠΔ Άρθρο 1 & Άρθρο 2 Αντικείμενο και στόχοι & Ουσιασ. Πεδ. Εφ.
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e1383-1-1

[4] Εδαφικό πεδίο εφαρμογής Άρθρο 3
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e1454-1-1

[5] Αρχές που διέπουν την επεξεργασία δεδομένων Άρθρο 5
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e1796-1-1

[6] Νομιμότητα της επεξεργασίας Άρθρο 6
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e1887-1-1

[7] Προϋποθέσεις για συγκατάθεση Άρθρο 7
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e2000-1-1

[8] Επεξεργασία ειδικών κατηγοριών δεδομένων Άρθρο 9
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e2047-1-1

[9] Δικαίωμα πρόσβασης Άρθρο 15
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e2509-1-1

[10] Δικαίωμα Διόρθωσης Άρθρο 16 & Δικαίωμα Διαγραφής Άρθρο 17
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e2585-1-1

[11] Δικαίωμα περιορισμού της επεξεργασίας Άρθρο 18
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e2696-1-1

[12] Δικαίωμα στην φορητότητα των δεδομένων & Δικαίωμα εναντίωσης Άρθρο 20 & 21
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e2696-1-1

[13] Προσωπικά δεδομένα
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el

[14] Παραβίαση προσωπικών δεδομένων
https://www.lexology.com/library/detail.aspx?g=03e8a988-7c9e-4576-94ea-5ab13f2cb240

[15] Κατηγορίες παραβίασης προσωπικών δεδομένων
https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[16] Παράδειγμα παραβίασης δεδομένων Facebook
https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

[17] Αναφορά παραβίασης προσωπικών δεδομένων
https://www.lexology.com/library/detail.aspx?g=03e8a988-7c9e-4576-94ea-5ab13f2cb240

[18] Ποινικές κυρώσεις Άρθρο 83
www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf#page=84

[19] Ποινικές κυρώσεις
http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf

[20] Κίνδυνοι παραβίασης προσωπικών δεδομένων
https://blog.netwrix.com/2018/11/29/what-to-know-about-a-data-breach-definition-types-risk-factors-and-prevention-measures/

[21] Ηλεκτρονικό ψάρεμα Phishing
https://www.identityiq.com/scams-and-fraud/what-is-phishing-prevent-attacks-with-common-examples/

[22] Κακόβουλο λογισμικό τύπου Ransomware
https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

[23] Μέτρα ασφαλείας από κακόβουλο λογισμικό.
https://www2.deloitte.com/lu/en/pages/risk/articles/phishing-ransomware-how-to-prevent-threats.html

[24] Συμμόρφωση με τον κώδικα
https://www.macchimaggesi.co.uk/en/general-data-protection-regulation-in-the-shipping-industry/

[25] Ενέργειες που πρέπει να ληφθούν από τους εργαζόμενους.
https://www.hellenicshippingnews.com/gdpr-and-crew-management/

[26] Κίνδυνοι παραβίασης προσωπικών δεδομένων για την εταιρία.
https://www.theamegroup.com/security-breach/