ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΚΟΙΝΟΠΟΙΗΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ (DATA BREACH) – ΝΟΜΙΚΕΣ & ΤΕΧΝΟΛΟΓΙΚΕΣ ΔΙΑΣΤΑΣΕΙΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΒΑΪΑ ΠΑΖΑΡΑ - Α.Μ.: 3232019023

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: Ε.ΜΗΤΡΟΥ

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

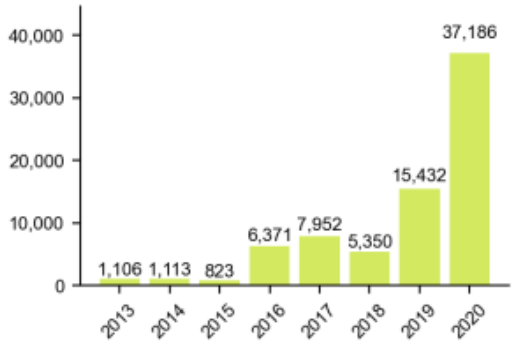
Το 2017, το Economist, βασιζόμενο σε μια φράση του Clive Humby, βρετανού μαθηματικού και αναλυτή δεδομένων το 2006, δημοσίευσε ένα άρθρο με τίτλο «Το πιο πολύτιμο αγαθό σήμερα δεν είναι το πετρέλαιο, αλλά τα δεδομένα», αντικατοπτρίζοντας έτσι τη μεταστροφή της παγκόσμιας οικονομίας στην οποία πλέον τα δεδομένα αποτελούν ακόμα και σήμερα σημαντικό ανταγωνιστικό πλεονέκτημα [1]. Με τον ίδιο τρόπο που το πετρέλαιο πριν από έναν αιώνα καθιερώνονταν ως ένας από τους πιο πολύτιμους φυσικούς πόρους, πρωταγωνιστώντας στην επερχόμενη βιομηχανική επανάσταση, τα δεδομένα σήμερα αποκτούν παρόμοια χαρακτηριστικά και πρωτοστατούν στη σύγχρονη τεχνολογική επανάσταση. Οι καινοτομίες στον τομέα των ΤΠΕ (Τεχνολογίες Πληροφοριών και Επικοινωνιών) διαμορφώνουν έναν νέο τρόπο ζωής στο πλαίσιο του οποίου οι κοινωνικές σχέσεις, οι επιχειρήσεις, οι ιδιωτικές και οι δημόσιες υπηρεσίες συνδέονται ψηφιακά δημιουργώντας με αυτόν το τρόπο ολοένα και μεγαλύτερο όγκο δεδομένων, εκ των οποίων τα περισσότερα είναι δεδομένα προσωπικού χαρακτήρα. Οι κυβερνήσεις, οι επιχειρήσεις και οι πολίτες δραστηριοποιούνται ολοένα και περισσότερο στο πλαίσιο μιας οικονομίας με γνώμονα τα δεδομένα, όπου τα ίδια τα δεδομένα έχουν πλέον αναχθεί σε πολύτιμους πόρους.

Η αυξανόμενη χρήση των ηλεκτρονικών συσκευών καθώς και η εντατικοποίηση της ψηφιοποίησης των προσωπικών και κοινωνικών δραστηριοτήτων, έχουν σαν αποτέλεσμα την παραγωγή, τη συλλογή και την επεξεργασία ολοένα και περισσότερων ψηφιακών δεδομένων. Τα δεδομένα μπορούν να συλλεχθούν από ανθρώπους μέσω διαδικτύου, συμπεριλαμβανόμενων και των κοινωνικών δικτύων, μέσω εμπορικών και οικονομικών συναλλαγών, μέσω αρχείων ηλεκτρονικής διακυβέρνησης ή μέσω συσκευών, όπως έξυπνων συσκευών, GPS κλπ. Η ανάλυση και η επεξεργασία των δεδομένων που συλλέγονται, προσφέρουν σημαντικά οφέλη σε διάφορους τομείς, όπως η ιατρική, η επιστήμη, οι επιχειρήσεις, οι κρατικές υπηρεσίες. Στον τομέα της ιατρικής, η γενετική, η χαρτογράφηση της γονιδιακής αλληλουχίας, η ανάπτυξη εξατομικευμένων αγωγών, είναι μερικές από τις καινοτομίες που στηρίζονται στη δύναμη των δεδομένων. Στον τομέα των επιχειρήσεων, η συλλογή και η επεξεργασία δεδομένων οδηγεί στην υιοθέτηση καλύτερων και αποδοτικότερων τεχνικών marketing και εξυπηρέτησης πελατών, μελετώντας τις τάσεις της κάθε εποχής. Μέσω κυρίως του διαδικτύου και των υπηρεσιών κοινωνικής δικτύωσης, οι άνθρωποι καταχωρούν δεδομένα προσωπικού χαρακτήρα, δημιουργώντας έτσι το προφίλ τους. Η διαδικασία αυτή περιλαμβάνει την αναζήτηση τάσεων, οι οποίες αντικατοπτρίζουν τα χαρακτηριστικά ενός τύπου καταναλωτή, βάσει για παράδειγμα προηγούμενων αγορών ή συγκεκριμένων αναζητήσεων στο διαδίκτυο. Η στοχευμένη διαφήμιση αποτελεί έναν σύγχρονο τρόπο για τις εταιρίες προσέγγισης των πελατών τους, προσφέροντας μια πιο εξατομικευμένη εξυπηρέτηση. Από την άλλη, επιχειρήσεις, όπως ασφαλιστικές εταιρίες, τράπεζες, αλλά και πολλοί εργοδότες ενδιαφέρονται ιδιαίτερα για τη γνώση προσωπικών και κυρίως ιατρικών δεδομένων των πολιτών, δεδομένων δηλαδή που μπορούν να επηρεάσουν την ικανότητα του ατόμου για εργασία, ασφάλιση, δανειοληψία κ.α.

[1] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Δεδομένης της αναγκαιότητάς τους αυτής τόσο σε οικονομικό, όσο και σε κοινωνικό επίπεδο, τα προσωπικά δεδομένα αποτελούν έναν ιδανικό στόχο για παράνομες δραστηριότητες, όπως η πώληση ή η επεξεργασία τους, για διαφορετικό σκοπό από τον οποίο έχουν αρχικά συλλεχθεί. Το διαδίκτυο αποτελεί έναν ιδανικό χώρο για κυβερνοεγκληματίες, να οργανώνουν επιθέσεις ενάντια σε άτομα, επιχειρήσεις, οργανισμούς και κυβερνήσεις, εκμεταλλευόμενοι την ευελιξία και την ανωνυμία που αυτό τους παρέχει. Προσωπικά δεδομένα υποκλέπτονται και χρησιμοποιούνται σε οικονομικές απάτες, εκβιασμούς, εταιρική ή και κρατική κατασκοπεία. Το 2020 αναφέρθηκαν 3932 τέτοιες παραβιάσεις, που οδήγησαν στην απώλεια 37,86 εκ. στοιχείων [2] (Εικ.1, Εικ.2). Ο μεγαλύτερος αριθμός αυτών των παραβιάσεων είχαν προκληθεί από Hackers (2528), ενώ οι περισσότερες παραβιάσεις έλαβαν χώρα μέσω διαδικτύου (35,066 εκ. records). Τα στοιχεία που συνήθως διαρρέουν είναι το ονοματεπώνυμο, το email, οι αριθμοί κοινωνικής ασφάλισης, οι κωδικοί ασφαλείας, οι αριθμοί πιστωτικών καρτών, τα ιατρικά στοιχεία, ενώ κύριοι στόχοι επιθέσεων για το 2020 αποτέλεσαν οι οργανισμοί υγείας, πληροφορικής, τα πιστωτικά ιδρύματα και οι ασφαλιστικές εταιρείες. Σύμφωνα με την ετήσια μελέτη της IBM σε συνεργασία με το Ινστιτούτο Ponemon σε ανάλυση 524 τέτοιων περιστατικών διαρροών δεδομένων, το κόστος για τις επιχειρήσεις και τους οργανισμούς των παραβιάσεων αυτών υπολογίστηκε σε 3,86 εκ. δολάρια ανά περιστατικό για το 2020, με πιο κοστοβόρες τις παραβιάσεις που σχετίζονται με υπηρεσίες υγείας[3] (Εικ.3). Τα προσωπικά δεδομένα ήταν ο στόχος των περισσότερων επιθέσεων για το 2020, ενώ το οικονομικό ήταν το βασικό κίνητρο των επιθέσεων αυτών.

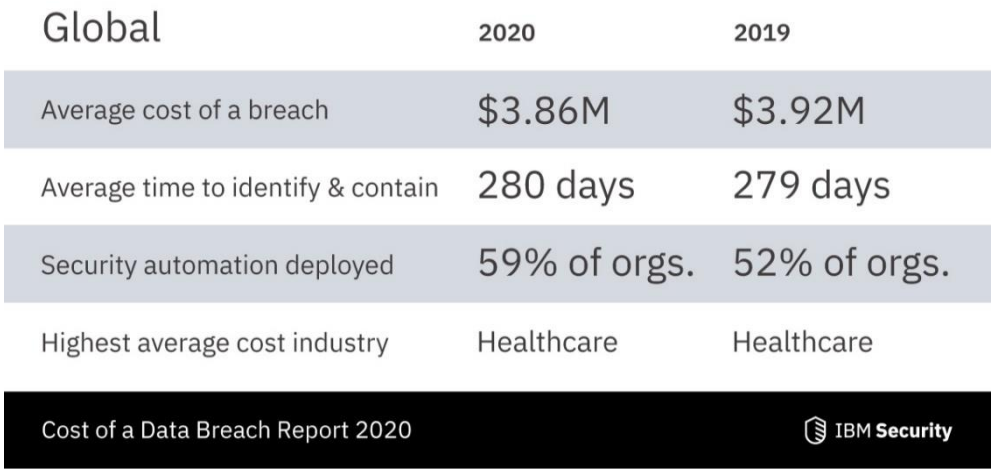
Εικόνα 1: Αριθμός περιστατικών διαρροών δεδομένων



Εικόνα 2: Αριθμός στοιχείων που διέρρευσαν (σε εκατομμύρια)

[2] Risk Based Security, 2020 Year End Report

[3] https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf



Εικόνα 3: Στοιχεία περιστατικών διαρροών δεδομένων

Το κόστος μιας παραβίασης δεδομένων, εκτός από οικονομικές απώλειές, αναφέρεται και σε απώλεια φήμης, διακοπή της επιχειρησιακής λειτουργίας, διακύβευση της εθνικής ασφάλειας.

Η σοβαρότητα του αντικτύπου μιας τέτοιας παραβίασης, έχει οδηγήσει τα κράτη και τις επιχειρήσεις στον καθορισμό μιας σειράς μέτρων (οδηγιών, κανόνων, νόμων, πολιτικών ασφάλειας), με σκοπό την προστασία των δεδομένων και τον περιορισμό των παραβιάσεών τους. Νόμοι και κανονισμοί όπως οι HIPPA(Health Insurance Portability and Accountability Act), CCPA(νόμος για την προστασία των καταναλωτών), PCI-DSS(πρότυπο ασφάλειας των καρτών πληρωμών), SHIEDACT (Stop Hacks and Improve Economic Data security ACT) στις Ηνωμένες Πολιτείες Αμερικής, ο GDPR (Γενικός Κανονισμός για την Προστασία των Δεδομένων) στην Ευρώπη, ο LGPD (νόμος για την προστασία των προσωπικών δεδομένων) στη Βραζιλία, έχουν εκδώσει οδηγίες για τη διαχείριση και την προστασία των προσωπικών δεδομένων και τον περιορισμό των διαρροών τους.

Οι διαρροές δεδομένων περιορίζονται υιοθετώντας κατάλληλα μέτρα πρόληψης από τη μία και περιορισμού των επιπτώσεων τους από την άλλη, μέσω των πολιτικών κοινοποίησης. Οι πολιτικές κοινοποίησης και οι σχετικοί νόμοι έχουν την απαίτηση από τους οργανισμούς και τις επιχειρήσεις να ενημερώνουν τους πελάτες τους, τα άτομα των οποίων τα δεδομένα παραβιάστηκαν, σχετικά με την παραβίαση αυτή. Είναι αξιοσημείωτο το γεγονός ότι μετά την εφαρμογή του ΓΚΠΔ, του νόμου που υποχρεώνει την κοινοποίηση, οι παραβιάσεις μειώθηκαν κατά 48% από το 2019, ενώ οι κοινοποιήσεις τέτοιων παραβιάσεων στα αρμόδια όργανα τετραπλασιάστηκαν από το προηγούμενο έτος [4,5].

Σκοπός της παρούσας μελέτης είναι τόσο η διερεύνηση της αναγκαιότητας της κοινοποίησης μιας διαρροής δεδομένων όσο και της διαδικασίας της κοινοποίησης αυτής

[4] http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf,

[5] DLA Piper GDPR Data Breach Survey https://www.dlapiper.com/~/media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf

καθαυτής, τόσο από τη νομική, όσο και από την τεχνολογική σκοπιά. Ειδικότερα, στο πρώτο κομμάτι της εργασίας γίνεται μια συνοπτική ανασκόπηση της νομοθεσίας στην Ελλάδα και στην Ευρωπαϊκή Ένωση, σχετικής με τα δεδομένα και την προστασία τους και μια ειδική αναφορά στον ΓΚΠΔ, ο οποίος εισάγει την αναγκαιότητα της κοινοποίησης σε περιπτώσεις παραβίασης προσωπικών δεδομένων. Στο επόμενο κομμάτι, παρουσιάζεται αναλυτικότερα η έννοια της κοινοποίησης και αρχικά πως αυτή καλύπτεται από τα νομικά πλαίσια της Ευρώπης και της Αμερικής κατά τη διάρκεια των ετών. Αναλύονται οι πρακτικές λεπτομέρειες της εφαρμογής της κοινοποίησης, τόσο από την τεχνολογική, όσο και από τη νομική σκοπιά. Ποια είναι τα βασικά στοιχεία μιας κοινοποίησης, πότε γίνεται αυτή, με ποιους τρόπους, σε ποιους απευθύνεται και ποιες είναι οι συνέπειες της μη κοινοποίησης μιας παραβίασης. Περιγράφεται η σχέση της κοινοποίησης στην προστασία των προσωπικών δεδομένων και η θέση της στην πολιτική ασφάλειας μιας επιχείρησης. Καταλήγοντας, παρουσιάζονται ορισμένα ζητήματα που προκύπτουν από την παραπάνω ανάλυση και αναφέρονται οι «γκρίζες ζώνες» στη νομολογία της κοινοποίησης.

2. ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Για την πληρέστερη κατανόηση και παρακολούθηση της εργασίας είναι σημαντική η διάκριση και ο προσδιορισμός των βασικών εννοιών που χρησιμοποιούνται. Οι σχετικές ορολογίες προκύπτουν από τις νομοθεσίες για την προστασία των προσωπικών δεδομένων που εφαρμόζονται στα διάφορα κράτη.

- Προσωπικά Δεδομένα

Προσωπικά δεδομένα ή δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αναφέρονται σε και περιγράφουν ένα άτομο. Πληροφορίες που «αν συγκεντρωθούν μαζί μπορούν να οδηγήσουν άμεσα ή έμμεσα στην ταυτοποίηση ενός συγκεκριμένου ατόμου», όπως αναγνωριστικά στοιχεία ταυτότητας (αριθμός ταυτότητας, όνομα, επώνυμο), δεδομένα θέσης ή παράγοντες που προσδιορίζουν τη σωματική, γενετική, επαγγελματική ή ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του ατόμου [6].

Παραδείγματα τέτοιων στοιχείων, τα οποία περιγράφουν ένα πρόσωπο και μπορούν να το διακρίνουν από άλλα, είναι το όνομα, ο αριθμός τηλεφώνου, ο αριθμός κοινωνικής ασφάλισης, ο αριθμός κυκλοφορίας οχήματος, ο αριθμός τραπεζικού λογαριασμού, η ηλεκτρονική διεύθυνση, δεδομένα τοποθεσίας, διεύθυνση διαδικτυακού πρωτοκόλλου(IP), cookies, βιομετρικά δεδομένα. Ειδική κατηγορία προσωπικών δεδομένων αποτελούν τα ευαίσθητα προσωπικά δεδομένα, τα οποία απορρέουν από την προσωπική ζωή των ατόμων και απαιτούν αυξημένη προστασία. Τέτοια δεδομένα θεωρούνται τα δεδομένα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, δεδομένα που αποκαλύπτουν πολιτικά φρονήματα, θρησκευτικές ή άλλες πεποιθήσεις, δεδομένα που αποκαλύπτουν συνδικαλιστική δράση, γενετικά και βιομετρικά δεδομένα, δεδομένα που αφορούν την υγεία, τη σεξουαλική ζωή ή τον γενετικό προσανατολισμό και δεδομένα που αφορούν αδικήματα και ποινικές δίκες. Το φυσικό πρόσωπο στο οποίο αναφέρονται τα προσωπικά δεδομένα που περιγράφηκαν παραπάνω, αποτελεί το υποκείμενο των δεδομένων.

- Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

Η επεξεργασία των προσωπικών δεδομένων είναι κάθε εργασία , αυτοματοποιημένη ή όχι, που μπορεί να εφαρμοστεί στα προσωπικά δεδομένα[7]. Αναφέρεται στην

- συλλογή, αναζήτηση και συγκέντρωση των δεδομένων
- καταχώρηση, π.χ. την τοποθέτηση των δεδομένων σε μια βάση δεδομένων
- οργάνωση, δηλαδή την κατηγοριοποίηση των δεδομένων βάσει κριτηρίων
- διάρθρωση
- αποθήκευση, δηλαδή τη διατήρηση σε οποιοδήποτε μέσο (όπως σκληρός δίσκος)
- προσαρμογή ή στην μεταβολή των δεδομένων, π.χ. κρυπτογράφηση, ανωνυμοποίηση

[6] Κανονισμός ΕΕ 2016 1079, άρθρο 4 παρ.1
[7] Κανονισμός ΕΕ 2016 1079, άρθρο 4 παρ.2

- ανάκτηση, αναζήτηση των πληροφοριών
- χρήση
- κοινολόγηση με διαβίβαση, δηλαδή τη μετάδοση των δεδομένων σε κάθε κατεύθυνση-δημοσίευση, στο internet, στα ΜΜΕ
- διάδοση ή στην κάθε άλλης μορφής διάθεση
- συσχέτιση ή στον συνδυασμό, δηλαδή στον καθορισμό των σχέσεων ανάμεσα σε δύο ή περισσότερες πηγές με σκοπό την εξαγωγή συμπερασμάτων
- περιορισμό, δηλαδή τον αποκλεισμό κάθε επιπλέον επεξεργασίας
- διαγραφή ή καταστροφή

Παραδείγματα επεξεργασίας αποτελούν: η διαχείριση του προσωπικού και οι μισθοδοσίες μιας εταιρίας, η διαβίβαση των στοιχείων αυτών στις φορολογικές αρχές, η προσπέλαση ή αναζήτηση πληροφορίας σε βάση δεδομένων που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα, αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων, καταστροφή εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα, δημοσίευση/ανάρτηση φωτογραφιών ενός ατόμου σε ιστοσελίδες, μαγνητοσκόπηση, αποθήκευση διευθύνσεων IP, η διευθύνσεων MAC.

- Χρήστες Δεδομένων Προσωπικού Χαρακτήρα

Οι δύο βασικές κατηγορίες των χρηστών των δεδομένων προσωπικού χαρακτήρα, είναι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία. Ο υπεύθυνος επεξεργασίας ελέγχει τις διαδικασίες και τους σκοπούς της επεξεργασίας των προσωπικών δεδομένων όπως αυτοί καθορίζονται με νομοθετικές διατάξεις ή κανονιστικές εθνικού ή κοινοτικού δικαίου και κατά συνέπεια είναι υπεύθυνος για την προστασία των υποκειμένων. Είναι αυτός που καθορίζει πώς και γιατί τα δεδομένα που συλλέχθηκαν πρόκειται να χρησιμοποιηθούν. Ο εκτελών την επεξεργασία είναι το φυσικό ή νομικό πρόσωπο που επεξεργάζεται τα δεδομένα για λογαριασμό του υπεύθυνου της επεξεργασίας κάτω από τις σαφείς οδηγίες του τελευταίου και μπορεί να θεωρηθεί και ο ίδιος ως υπεύθυνος της επεξεργασίας εφόσον καθορίζει αυτός τους σκοπούς και τα μέσα της επεξεργασίας. Για παράδειγμα: Μια εταιρεία Α έχει αναθέσει την καταβολή των μισθών των εργαζομένων της σε μια εταιρεία πληρωμών Β. Η εταιρεία Α ενημερώνει την Β για το πότε γίνεται η καταβολή των μισθών, πότε ένας εργαζόμενος αποχωρεί, τα απαραίτητα στοιχεία του κάθε εργαζόμενου. Η εταιρεία Β παρέχει το σύστημα καταβολής των πληρωμών και αποθηκεύει τα δεδομένα των πελατών της. Η εταιρεία Α είναι είναι ο υπεύθυνος επεξεργασίας και η Β ο εκτελών[8].

- Παραβίαση δεδομένων.

Τα κριτήρια που καθορίζουν μια παραβίαση δεδομένων ποικίλλουν από χώρα σε χώρα. Σε κάποιες υιοθετείται ένας γενικός ορισμός, που αναφέρει την παραβίαση δεδομένων σαν μια μη εξουσιοδοτημένη πρόσβαση δεδομένων η οποία διακυβεύει την ασφάλεια, την ακεραιότητα ή/και την εμπιστευτικότητα των δεδομένων αυτών που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία[9] , ενώ σε άλλες υπογραμμίζονται συγκεκριμένα παραδείγματα,

[8] GDPR 2016/679, Άρθρο 4, παρ. 7, 8

[9] οδηγία 2002/58/ΕΚ παρ.85,
US Mandatory Data Breach Legislation,
Australian Privacy Act (https://www.cookielawinfo.com/the-privacy-act-1988-australia)

όπως: απώλεια τεχνολογικού εξοπλισμού, κοινοποίηση αλληλογραφίας σε λάθος παραλήπτες, έκθεση εγγράφων, hacking, τεχνικό λάθος, κλοπή, μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένη διακίνηση.

2.2 ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ - ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Η προστασία των προσωπικών δεδομένων και ο σεβασμός στην προσωπική και οικογενειακή ζωή ενός ατόμου αποτελούν θεμελιώδη δικαιώματα του, τα οποία προστατεύονται από αυθαιρεσίες των κρατών ή ιδιωτών. Ήδη από το 1890 γίνεται αναφορά στην έννοια της ιδιωτικότητας σε άρθρο των Samuel D. Warren και Louis Branders, με τίτλο «το δικαίωμα στην ιδιωτική ζωή»[10]. Το άρθρο γράφτηκε με αφορμή τις τότε καινοτόμες τεχνολογικές ανακαλύψεις και μεθόδους εργασίας, όπως οι φωτογραφίες και οι εφημερίδες και τον ρόλο αυτών στην οικογενειακή και ιδιωτική ζωή των πολιτών, υπογραμμίζοντας τους κινδύνους που αυτές ενέχουν, θέτοντας έτσι για πρώτη φορά την έννοια του δικαιώματος να μένεις μόνος (right to be left alone). Το δικαίωμα των ανθρώπων στην ιδιωτικότητα αναφέρεται ρητά στο άρθρο 12 της Οικουμενικής διακήρυξης των ανθρωπίνων δικαιωμάτων που διατυπώθηκε το 1948[11]. Δύο χρόνια αργότερα, η Ευρωπαϊκή επιτροπή αναγνωρίζει επίσης το δικαίωμα αυτό ως ένα από τα θεμελιώδη δικαιώματα των πολιτών της, συμπεριλαμβάνοντάς το στο άρθρο 8 της σύμβασης για τα δικαιώματα του ανθρώπου (Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής)[12]. Σύμφωνα με το Δικαστήριο των Ανθρωπίνων Δικαιωμάτων, το άρθρο 8 ερμηνεύτηκε έτσι ώστε τα προσωπικά δεδομένα να θεωρηθούν ειδικότερη έκφανση του γενικότερου δικαιώματος στην προστασία της ιδιωτικής ζωής. Η έννοια της προστασίας δεν αναφέρεται στα δεδομένα αυτά καθαυτά, αλλά στην προστασία του ατόμου από την επεξεργασία τους.

Η μεγάλη τεχνολογική ανάπτυξη κατά τις δεκαετίες 60-70 και η ολοένα αυξανόμενη χρήση των υπολογιστών στην επεξεργασία και τη διενέργεια συναλλαγών καθιστά ακόμα μεγαλύτερη την ανάγκη προστασίας των προσωπικών δεδομένων, οδηγώντας πολλές από τις χώρες της Ευρώπης στην υιοθέτηση αντίστοιχων εθνικών νόμων. Ειδικότερα, στην Γερμανία, το ομοσπονδιακό κρατίδιο της Έσσης, υιοθέτησε πρώτο νομοθεσία σχετική με την προστασία του ατόμου από την αυτόματη επεξεργασία των δεδομένων τους. Το συμβούλιο της Ευρώπης εκδίδει το 1973-1974 τις αρχές για την προστασία δεδομένων σε αυτοματοποιημένες βάσεις δεδομένων στον ιδιωτικό και δημόσιο τομέα αντίστοιχα, με στόχο οι αρχές αυτές να αποτελέσουν τις βάσεις για την ανάπτυξη ανάλογων νομοθετημάτων από τα κράτη μέλη του. Το παράδειγμα της Έσσης ακολούθησαν και άλλα κρατίδια της Γερμανίας, μαζί με άλλα ευρωπαϊκά κράτη, όπως η Σουηδία (1973), η Νορβηγία (1978), το Λουξεμβούργο, η Γαλλία και η Αυστρία.

---

[10] Samuel D. Warren, Louis D. Brandeis. BOSTON, December 1890

[11] ΟΙΚΟΥΜΕΝΙΚΗ ΔΙΑΚΗΡΥΞΗ ΓΙΑ ΤΑ ΑΝΘΡΩΠΙΝΑ ΔΙΚΑΙΩΜΑΤΑ, , 1948, ΑΡΘΡΟ 12: «Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.»

[12] Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, 1950 Άρθρο 8

Το 1980, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) προτείνει με τη σειρά του ένα σύνολο κατευθυντήριων αρχών σχετικών με την προστασία της ιδιωτικότητας και της διασυνοριακής κυκλοφορίας προσωπικών δεδομένων, που μεταξύ άλλων περιλαμβάνουν την αρχή της περιορισμένης συγκέντρωσης και συλλογής δεδομένων, της ποιότητας των δεδομένων, του περιορισμού του σκοπού, της περιορισμένης χρήσης των προσωπικών δεδομένων, της διαφάνειας της ευθύνης[13]. Οι παραπάνω αρχές είχαν μη δεσμευτικό χαρακτήρα και αποτέλεσαν σύσταση προς τα κράτη μέλη, ώστε να προστατεύσουν τους πολίτες τους από την κατάχρηση των πληροφοριών.

Σε αντίθεση με τις μη δεσμευτικές συστάσεις του ΟΟΣΑ, το συμβούλιο της Ευρώπης υπέγραψε το 1981, τη σύμβαση 108 «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα». Η σύμβαση αυτή ήταν το πρώτο διεθνές νομικά δεσμευτικό κείμενο και αποτέλεσε ορόσημο στην προστασία προσωπικών δεδομένων. Στόχος της ήταν η συντονισμένη προσέγγιση των κρατών-μελών στην προστασία των δεδομένων καθιστώντας το δικαίωμα στην ιδιωτικότητα ως νομική υποχρέωση[14].

Συνέχεια των παραπάνω αποτέλεσε η οδηγία 95/46/ΕΚ του Ευρωπαϊκού κοινοβουλίου και του συμβουλίου, γνωστή και ως Data Protection Directive που τέθηκε σε ισχύ στα μέσα της δεκαετίας του 90. Η οδηγία αυτή θεσπίζει ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα ανά την ένωση[15]. Διατυπώνει τις αρχές που πρέπει να διέπουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, όπως την αρχή του περιορισμού του σκοπού της επεξεργασίας, τις αρχές της ποιότητας των δεδομένων, την αρχή της αναλογικότητας, την αρχή της διαφάνειας, οι οποίες αποτέλεσαν τη βάση για μετέπειτα κανονισμούς. Παρέχει σαφή διαχωρισμό των δεδομένων σε προσωπικά και ευαίσθητα προσωπικά δεδομένα και εισάγει την υποχρέωση της ενημέρωσης των υποκειμένων των δεδομένων από τον υπεύθυνο επεξεργασίας τους και τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της επεξεργασίας των δεδομένων. Επιπλέον, το κενό που υπήρχε στις προηγούμενες νομοθετικές πράξεις για τη διασφάλιση της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ήρθε να καλύψει η οδηγία 2002/58/ΕΚ – Directive of Privacy and Electronic Communication) η οποία περιείχε πιο εξειδικευμένες ρυθμίσεις για την επεξεργασία των προσωπικών δεδομένων στον χώρο των τηλεπικοινωνιών και του διαδικτύου[16]. Ωστόσο η οδηγία αυτή δεν κατάφερε να φέρει την ομοιομορφία στους τρόπους που το κάθε κράτος μέλος την υλοποιούσε ανάλογα με την ερμηνεία της. Οι ραγδαίες εξελίξεις της τεχνολογίας και η ανάγκη υιοθέτησης ενός ενιαίου νομοθετικού πλαισίου από όλα τα κράτη μέλη, σε αντίθεση με την Οδηγία που απαιτούσε τη θέσπιση μέτρων ενσωμάτωσης, οδήγησε στην αντικατάσταση της τελευταίας

[13] Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD, 1980 - PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

[14] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981

[15] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 24 October 1995

[16] Directive 2002/58/EC of the European Parliament and of the Council, 12 July 2002

από το νέο κανονισμό 2016/679 (GDPR- Γενικός Κανονισμός Προστασίας Δεδομένων)[17]. Σκοπός της εφαρμογής του κανονισμού είναι η άρση των νομικών και κανονιστικών ασαφειών που δημιουργούσε το προηγούμενο νομικό πλαίσιο, η ομοιομορφία του νομικού πλαισίου σε όλα τα κράτη-μέλη καθώς και η ενίσχυση των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων. Επιπλέον, καθώς η οδηγία είχε εκδοθεί πριν την επέλαση της 4ης τεχνολογικής επανάστασης κατά την οποία τεράστιος όγκος προσωπικών δεδομένων συλλέγεται, η ανάγκη για την υιοθέτηση ενός πιο σύγχρονου νόμου ήταν επιτακτική [12]. Οι βασικότερες αλλαγές που επιφέρει ο νέος κανονισμός σε σχέση με τους προηγούμενους, είναι:

- Τα αυξημένα δικαιώματα των υποκειμένων των δεδομένων, στα οποία περιλαμβάνονται το δικαίωμα στη λήθη, το δικαίωμα περιορισμού της επεξεργασίας, το δικαίωμα στη φορητότητα,
- η ενίσχυση της προστασίας ανηλίκων,
- η γνωστοποίηση παραβίασης προσωπικού χαρακτήρα,
- η προστασία των δεδομένων από τον σχεδιασμό και εξ ’ορισμού (data protection by default and by design),
- η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων,
- η τήρηση αρχείων δραστηριότητας επεξεργασίας,
- ο ορισμός του υπεύθυνου προστασίας δεδομένων

[17]General Data Protection Regulation (EU) 2016/679, 27 April 2016

3. ΚΟΙΝΟΠΟΙΗΣΗ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η πληροφόρηση του υποκειμένου της επεξεργασίας των δεδομένων, αποτελεί τον πυρήνα της προστασίας τους. Κάθε άτομο έχει δικαίωμα πληροφόρησης του σκοπού της επεξεργασίας, της τέλεσης της επεξεργασίας καθώς και το δικαίωμα στην άρνηση της επεξεργασίας των δεδομένων που το αφορούν[18] . Σύμφωνα με το ευρωπαϊκό δίκαιο, η αρχή της διαφάνειας απαιτεί κάθε επεξεργασία δεδομένων να είναι γενικά διαφανής για τα υποκείμενα της επεξεργασίας. Το άρθρο 12 του ΓΚΠΔ ορίζει ρητά ότι ο «υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση»[19]. Οι υπεύθυνοι επεξεργασίας υποχρεούνται να ενημερώνουν το υποκείμενο των δεδομένων κατά τη συλλογή τους και τον σκοπό της επεξεργασίας τους. Η υποχρέωση αυτή δεν εξαρτάται από αίτημα του υποκειμένου, αντιθέτως ο υπεύθυνος επεξεργασίας των δεδομένων θα πρέπει να δρα εκ των προτέρων, ανεξάρτητα αν το υποκείμενο εκφράζει το ενδιαφέρον για ενημέρωση. Προέκταση του παραπάνω δικαιώματος της πληροφόρησης του υποκειμένου αποτελεί και η ειδοποίηση της παραβίασης των δεδομένων που το αφορούν. Οι παραβιάσεις των δεδομένων επιφέρουν σημαντικό κόστος στα υποκείμενα καθώς στερεί το δικαίωμα της εμπιστευτικότητας, της ιδιωτικότητας και της ακεραιότητάς τους [18]. Μπορούν να οδηγήσουν σε υποκλοπή ταυτότητας, απάτη, δυσφήμιση. Έτσι, οι υπεύθυνοι επεξεργασίας των δεδομένων, πέρα από την εξασφάλιση της ορθής και ασφαλούς επεξεργασίας των δεδομένων, οφείλουν να εξασφαλίσουν ότι όταν λαμβάνει χώρα μια παραβίαση, είναι σε θέση να την αντιμετωπίσουν κατάλληλα και έγκαιρα. Τα υποκείμενα των δεδομένων καθώς και τις περισσότερες φορές οι ίδιες οι εποπτικές αρχές, δεν γνωρίζουν πάντα ότι έχει σημειωθεί μια παραβίαση δεδομένων. Αποτέλεσμα είναι να μην είναι σε θέση να προστατευθούν από τις αρνητικές συνέπειές της. Για τον λόγο αυτό η σχετική νομοθεσία επιβάλλει, σε ορισμένες περιπτώσεις στους υπεύθυνους επεξεργασίας την υποχρέωση γνωστοποίησης. Η απόκρυψη μιας παραβίασης είναι πιο επιζήμια από την ίδια την παραβίαση. Η κοινοποίησή της δίνει τη δυνατότητα στα άτομα που επηρεάστηκαν (οργανισμοί, υποκείμενα), να περιορίσουν τους κινδύνους της παραβίασης. Για παράδειγμα, σε περίπτωση υποκλοπής ή διαρροής των στοιχείων της πιστωτικής κάρτας ενός ατόμου, αμέσως μετά την κοινοποίησή της, το άτομο μπορεί να προβεί σε ενέργειες επανάκτησής τους (ακύρωση παλιάς κάρτας και επανέκδοση νέας). Το δίκαιο της ΕΕ, καθώς και οι νομοθεσίες κρατών όπως οι ΗΠΑ, η Αυστραλία κ.λπ. θεσπίζουν καθεστώς που ορίζει τον χρόνο, τον τρόπο και το περιεχόμενο των γνωστοποιήσεων.

[18] Ν2472/1997, Άρθρο 11
[19] GDPR 2016/679, Άρθρο 12

3.1 ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΚΟΙΝΟΠΟΙΗΣΗΣ – ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Η υποχρέωση της κοινοποίησης της παραβίασης δεδομένων εμφανίστηκε για πρώτη φορά το 2002 στην Καλιφόρνια, με νόμο που τέθηκε σε ισχύ το 2003 (Financial Services Modernization Act). Ο νόμος θεσπίστηκε για τη διασφάλιση της κλοπής προσωπικών δεδομένων και της απάτης. Απαιτεί κάθε οργανισμός, άτομο ή επιχείρηση που δραστηριοποιείται στην Καλιφόρνια και κατέχει ή επεξεργάζεται δεδομένα που συμπεριλαμβάνουν προσωπικά δεδομένα, να κοινοποιεί με συγκεκριμένους τρόπους κάθε διαρροή τέτοιων δεδομένων σε κάθε κάτοικο της Καλιφόρνιας, υποκείμενο των δεδομένων αυτών, τα οποία αποκτήθηκαν από μη εξουσιοδοτημένα άτομα. Επίσης απαιτεί κάθε οντότητα που έχει στην κατοχή της τέτοια δεδομένα να ενημερώνει τον κάτοχο ή το υποκείμενο των δεδομένων για κάθε είδους παραβίαση της ασφάλειας των δεδομένων αυτών. Μέχρι πρότινος, δεν υπάρχει κάποιος κοινός ομοσπονδιακός νόμος που να διασφαλίζει τα προσωπικά δεδομένα. Παρ'ολ'αυτά, υπάρχουν κάποιοι ομοσπονδιακοί νόμοι που προστατεύουν προσωπικά δεδομένα σε συγκεκριμένα πλαίσια και διαχειρίζονται διαρροές δεδομένων, όπως ο νόμος για την προστασία ιατρικών και άλλων δεδομένων υγείας HIPA (Health Insurance Portability & Accountability act), ο νόμος GLBA (Gramm-Leach-Bliley Act) που απαιτεί από οικονομικά ιδρύματα να προστατεύουν τα προσωπικά δεδομένα των πελατών τους, ο νόμος COPPA (Children's Online Privacy Protection Rule), που προστατεύει τα προσωπικά δεδομένα παιδιών κάτω των 13 ετών, εμπεριέχουν κανόνες που καθορίζουν τη διαρροή δεδομένων ορίζονται σε επίπεδο πολιτείας. Οι νόμοι στις περισσότερες πολιτείες βασίζονται στις βασικές αρχές του νόμου της Καλιφόρνια.

Τον Φεβρουάριο του 2018 τέθηκε σε ισχύ ο νόμος που καθιστά υποχρεωτική την κοινοποίηση διαρροής των δεδομένων και στην Αυστραλία. Ο νόμος αυτός ουσιαστικά τροποποιεί τον νόμο περί ιδιωτικότητας του 1988 (Privacy Act) ο οποίος είχε θέσει τις βάσεις για τον ορισμό ενός σχήματος ενημέρωσης σχετικά με διαρροές δεδομένων, συμπεριλαμβανομένων και προσωπικών δεδομένων, που ενδέχεται να οδηγήσουν σε ζημία. Στην Κίνα, ο νόμος που αναφέρεται στην πληροφόρηση παραβίασης δεδομένων και στις απαιτήσεις της, τέθηκε σε ισχύ στα μέσα του 2017, ενώ στην Ιαπωνία ο νόμος που προτρέπει τις επιχειρήσεις στο να αποκαλύπτουν παραβιάσεις δεδομένων, τροποποιήθηκε το 2015 και ήρθε σαν τροποποίηση του νόμου περί προστασίας προσωπικών δεδομένων (APPI- Act on the Protection of Personal Information). Στη Νέα Ζηλανδία, ο νόμος προστασίας της ιδιωτικότητας θεσπίστηκε το 2020, αντικαθιστώντας έναν παλαιότερο του 1993. Σύμφωνα με τον νόμο αυτό η κοινοποίηση παραβίασης των δεδομένων καθίσταται υποχρεωτική.

Στην ΕΕ, η υποχρέωση γνωστοποίησης σε περιπτώσεις παραβιάσεων ορίζεται αρχικά στην Οδηγία 2009/136/ΕΚ, η οποία τροποποιεί την Οδηγία 2002/58 (E-Privacy) και αναφέρεται σε οργανισμούς οι οποίοι παρέχουν υπηρεσίες ηλεκτρονικών επικοινωνιών. Ορισμένα κράτη της ΕΕ έχουν υιοθετήσει στη δική τους νομοθεσία την υποχρέωση γνωστοποίησης παραβιάσεων, η οποία περιλαμβάνει την υποχρέωση γνωστοποίησης παραβιάσεων που αφορούν υπεύθυνους επεξεργασίας που δεν σχετίζονται μόνο με εταιρείες παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών ή εφαρμόζουν τους δικούς τους κώδικες ορθής πρακτικής. Ειδικότερα, στη Γερμανία, η υποχρέωση να γίνονται γνωστοποιήσεις σε περιπτώσεις διαρροής δεδομένων τέθηκε σε εφαρμογή το 2009 σαν μέρος του Ομοσπονδιακού Νόμου Προστασίας Δεδομένων (Bundesdatenschutzgesetz-BDSG). Ο νόμος στηρίχθηκε στους αντίστοιχους νόμους που είχαν

τεθεί σε εφαρμογή στις ΗΠΑ και αφορά τραπεζικά δεδομένα -–στοιχεία πιστωτικών καρτών-, δεδομένα τηλεπικοινωνιών και δεδομένα που συλλέχθηκαν από το διαδίκτυο, δεδομένα που αφορούν εγκληματικές ενέργειες και άλλα ευαίσθητα δεδομένα. Στην Ισπανία, ο νόμος του 2007 (Royal Decree), ορίζει ανάμεσα σε άλλα, τους υπεύθυνους των δεδομένων να καταγράφουν σαν μέρος της πολιτικής ασφαλείας τις πρακτικές σχετιζόμενες με τη διαδικασία της γνωστοποίησης, της διαχείρισης και της αντιμετώπισης των κινδύνων. Εκεί καταγράφονται το είδος του περιστατικού ασφαλείας, η χρονική στιγμή που αυτό συνέβη ή έγινε αντιληπτό, το άτομο που έκανε τη γνωστοποίηση του περιστατικού, σε ποιόν έγινε αυτή, τα αποτελέσματα αυτής και τα μέτρα που λήφθηκαν. Στο Ηνωμένο Βασίλειο, το 2008, το Γραφείο του επιτρόπου (ICO - Information Commissioner ‘s Office) εξέδωσε οδηγία, σύμφωνα με την οποία πρέπει να ενημερώνεται σε περιπτώσεις σοβαρών διαρροών παρόλο που δεν υπάρχει κάποια τέτοια νομική υποχρέωση. Τέλος, στην Ιρλανδία ορίστηκε ο κώδικας ορθής πρακτικής, ο οποίος περιλαμβάνει ένα κομμάτι σχετικό με τις γνωστοποιήσεις σε περιπτώσεις παραβιάσεων προσωπικών δεδομένων. Παρόλο που αρκετές αρχές προστασίας δεδομένων στην ΕΕ ενθαρρύνουν τους υπεύθυνους επεξεργασίας να αναφέρουν παραβιάσεις, η οδηγία 95/46/ΕΚ για την προστασία των δεδομένων δεν περιέχει κάποια υποχρέωση γνωστοποίησης. Ωστόσο, ο ΓΚΠΔ, που τέθηκε σε εφαρμογή το 2018 και αντικατέστησε την οδηγία, καθιστά υποχρεωτική τη γνωστοποίηση για όλους τους υπεύθυνους επεξεργασίας, εκτός αν η παραβίαση δεν ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των προσώπων. Οι εκτελούντες την επεξεργασία διαδραματίζουν επίσης σημαντικό ρόλο και πρέπει να γνωστοποιούν οποιαδήποτε παραβίαση στον υπεύθυνο επεξεργασίας τους[20]

[20] GDPR,2016/679: Άρθρο 33, παρ. 2

3.2 ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΚΟΙΝΟΠΟΙΗΣΗΣ

Οι παραπάνω νόμοι και οδηγίες που θεσπίστηκαν και ορίστηκαν με σκοπό την παροχή πληροφόρησης σε περιπτώσεις παραβίασης δεδομένων, έχουν σαν στόχο να παρέχουν ενημέρωση στα ενδιαφερόμενα μέλη, είτε αυτά είναι οι υπεύθυνοι επεξεργασίας, είτε οι αρμόδιοι οργανισμοί, είτε τα ίδια τα άτομα στα οποία ανήκουν τα δεδομένα, σχετικά με τους κινδύνους που προκύπτουν από την παραβίαση αυτή και τις ενέργειες που θα πρέπει να κάνουν ώστε να προστατευθούν από τις πιθανές συνέπειες μιας παραβίασης. Σε κάθε νόμο ή οδηγία που αφορά στη γνωστοποίηση μιας παραβίασης, υπάρχουν διατάξεις σχετικές με το τι συνιστά παραβίαση δεδομένων, αν και πότε η παραβίαση αυτή θα πρέπει να γνωστοποιείται, ποιοι θα πρέπει να ενημερώνονται, με ποιόν τρόπο και ποιες πληροφορίες θα πρέπει να παρέχονται στο πλαίσιο της γνωστοποίησης αυτής.

Παρά την πληθώρα τους, οι αντίστοιχοι νόμοι και κανόνες που αναφέρονται στην κοινοποίηση παραβιάσεων δεδομένων, ακολουθούν μια κοινή γραμμή. Σε κάθε περίπτωση ορίζεται το σύνολο των δεδομένων που χρήζουν προστασίας. Καθορίζονται οι περιπτώσεις εκείνες που συνιστούν παραβίαση των δεδομένων αυτών και από τις περιπτώσεις αυτές καθορίζονται οι περιπτώσεις αυτές για τις οποίες θα υπάρξει κοινοποίηση. Τέλος, ορίζεται το σύνολο των ενεργειών που συνιστούν τη διαδικασία της κοινοποίησης της διαρροής, όπως ποιοι ενημερώνονται, πότε, τι πληροφορίες λαμβάνουν και με ποιον τρόπο και που λαμβάνονται από τα μέρη που έχουν υποστεί τη διαρροή καθώς και οι συνέπειες της μη συμμόρφωσης με τους κανόνες της κοινοποίησης. Στο κομμάτι αυτό μελετώνται και αναλύονται οι παραπάνω συνιστώσες των βασικών νομοθετημάτων κοινοποίησης διαρροών, του ΓΚΠΔ που ισχύει αυτή τη στιγμή στην ΕΕ και των αντίστοιχων νόμων των Ηνωμένων Πολιτειών, τόσο από νομοθετική, όσο και από τεχνολογική σκοπιά.

3.2.1 ΠΟΤΕ ΓΙΝΕΤΑΙ Η ΚΟΙΝΟΠΟΙΗΣΗ ΜΙΑΣ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΣΕ ΠΟΙΟΥΣ

Η γνωστοποίηση μιας παραβίασης δεδομένων ορίζεται από νόμους και κανονισμούς, όπως ο ΓΚΠΔ, ωστόσο δεν είναι πάντα υποχρεωτική για τα υποκείμενα των δεδομένων. Η κοινοποίηση μιας παραβίασης προσωπικών δεδομένων δεν είναι υποχρεωτική σε περίπτωση που ο υπεύθυνος επεξεργασίας έχει εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων αυτών πριν την παραβίαση, όπως είναι η ψευδοανωνυμοποίηση ή η κρυπτογράφηση και γενικά μέτρα που καθιστούν τα δεδομένα ακατάληπτα σε κάποιον που δεν έχει εξουσιοδοτημένη πρόσβαση σε αυτά[21]. Σε περίπτωση δηλαδή που η παραβίαση αφορά μόνο στο απόρρητο και τα δεδομένα έχουν κρυπτογραφηθεί με αλγόριθμο τελευταίας τεχνολογίας και το κλειδί για την αποκρυπτογράφησή τους δεν παραβιάστηκε και δεν μπορεί να εξακριβωθεί με τα διαθέσιμα τεχνολογικά μέσα[22]. Δεν είναι επίσης υποχρεωτική σε περιπτώσεις που ο υπεύθυνος επεξεργασίας αμέσως μετά την παραβίαση έχει λάβει μέτρα που διασφαλίζουν ότι δεν προκύπτει

[21] GDPR, 2016/679: Άρθρο 34, παρ. 3α
[22] Ομάδα Εργασίας 29

κίνδυνος για τα δικαιώματα και τις ελευθερίες των ατόμων[23]. Τέλος, η υποχρέωση κοινοποίησης δεν υφίσταται όταν η επικοινωνία με τα πρόσωπα συνεπάγεται δυσανάλογες προσπάθειες από πλευράς υπεύθυνων επεξεργασίας[24].

Από τη στιγμή που μια παραβίαση δεδομένων προσωπικού χαρακτήρα λαμβάνει χώρα και πρέπει να γνωστοποιηθεί, το πότε πραγματοποιείται καθώς και σε ποιους απευθύνεται ή γνωστοποιείται αυτή, καθορίζεται από τους σχετικούς νόμους. Η υποχρέωση της γνωστοποίησης τίθεται τόσο απέναντι στις αρμόδιες εποπτικές αρχές, όσο και στα υποκείμενα των δεδομένων. Οι αρμόδιες αρχές είναι ανεξάρτητες δημόσιες ή ιδιωτικές αρχές, οι οποίες έχουν την ευθύνη της υιοθέτησης και της σωστής εφαρμογής των αντίστοιχων νόμων περί προστασίας δεδομένων από τις διάφορες επιχειρήσεις ή οργανισμούς της δικαιοδοσίας τους. Στην Ελλάδα για παράδειγμα, τον ρόλο αυτό έχει η Αρχή Προστασίας Δεδομένων[25], μια ανεξάρτητη δημόσια αρχή, ενώ στην Καλιφόρνια, αντίστοιχο ρόλο έχει το γραφείο επιβολής και προστασίας της ιδιωτικότητας (Privacy Enforcement and Protection Unit[26]) ορισμένο από τον Γενικό Εισαγγελέα.

Σύμφωνα με τον ΓΚΠΔ, υπάρχουν δύο κατηγορίες παραβιάσεων που ακολουθούν διαφορετικούς δρόμους. Η πρώτη αφορά τις συνηθισμένες παραβιάσεις προσωπικών δεδομένων, οι οποίες θα πρέπει να γνωστοποιούνται στην αρμόδια αρχή 72 ώρες μετά την αποκάλυψή τους[27]. Η δεύτερη αφορά παραβιάσεις οι οποίες ενδέχεται να οδηγήσουν σε υψηλό κίνδυνο των δικαιωμάτων και των ελευθεριών των ανθρώπων, όπως αυτά ορίζονται από τον χάρτη των δικαιωμάτων των ανθρώπων και αφορούν κυρίως ευαίσθητα δεδομένα (EU Charter of Fundamental Rights). Αυτές θα πρέπει να κοινοποιούνται και στα υποκείμενα των δεδομένων αμελλητί – χωρίς καθυστέρηση[28] αμέσως μόλις ο υπεύθυνος επεξεργασίας γίνει γνώστης της παραβίασης. Τέτοιες παραβιάσεις αφορούν σε ευαίσθητα προσωπικά δεδομένα ή και σε δεδομένα που δεν είναι ευαίσθητα αλλά οι παραβιάσεις αυτές μπορούν να προκαλέσουν κακό στο υποκείμενο των δεδομένων.

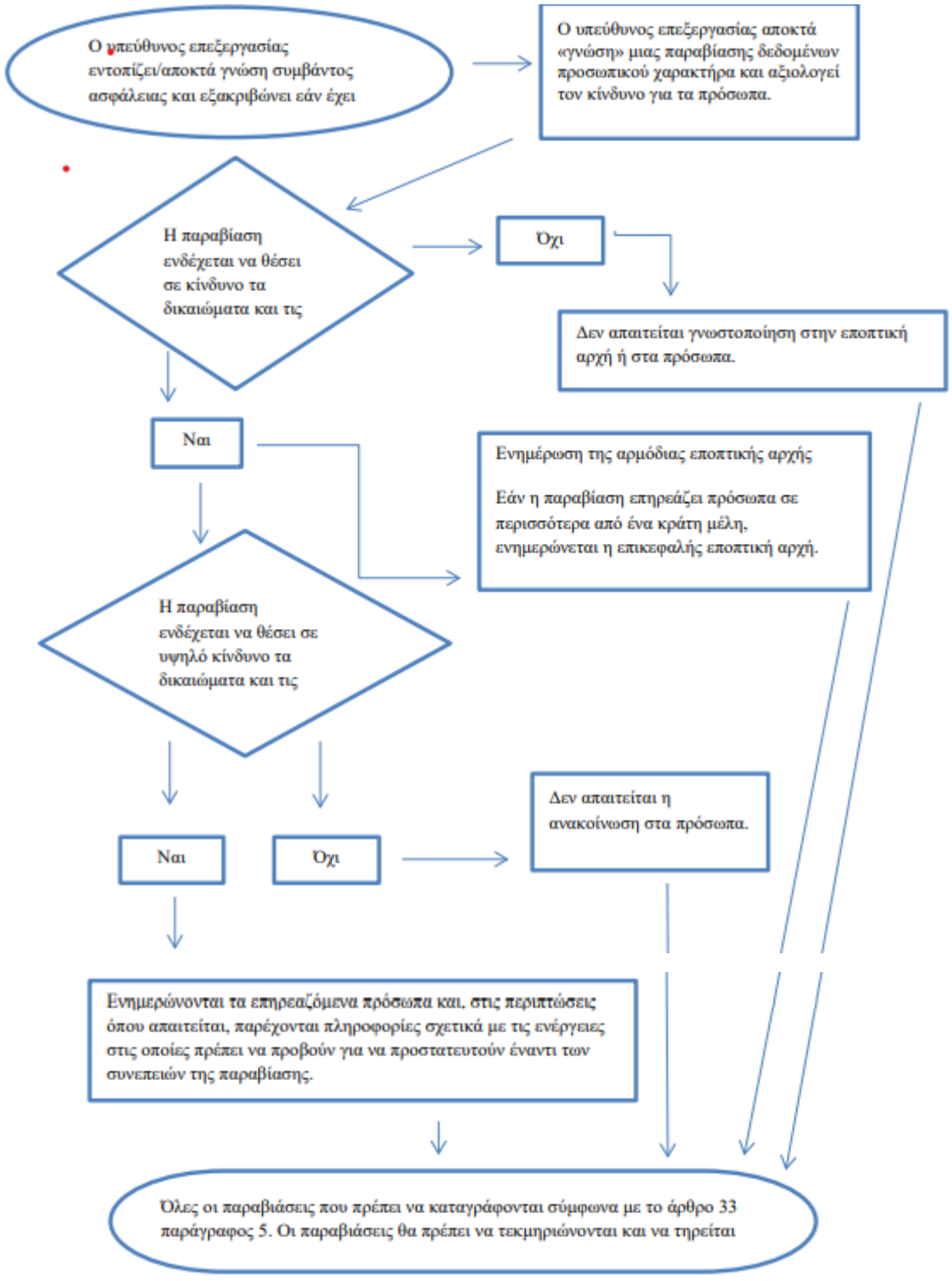
Στις ΗΠΑ οι διάφοροι πολιτειακοί νόμοι προτείνουν και διαφορετικούς χρόνους απόκρισης και στόχους ενημέρωσης. Οι περισσότεροι ορίζουν η κοινοποίηση να γίνεται απευθείας στα άτομα-υποκείμενα των δεδομένων χωρίς καθυστέρηση. Ωστόσο άλλοι υποδεικνύουν η κοινοποίηση να γίνεται και στον Γενικό Εισαγγελέα της πολιτείας μέσα σε 30 μέρες από τη στιγμή που αυτή γίνει γνωστή και αν αυτή έχει επηρεάσει το λιγότερο 500 άτομα. Συγκεκριμένα στην Καλιφόρνια, σε περίπτωση παραβίασης δεδομένων υγείας, θα πρέπει να ενημερώνεται και το υπουργείο υγείας (Department of Health Services) μέσα σε 15 ημέρες [19]. Σημαντικό ρόλο στην υποχρέωση κοινοποίησης και στους αποδέκτες της έχει και το μέγεθος και η φύση της παραβίασης. Αν από την παραβίαση επηρεάζεται μεγάλος αριθμός ατόμων, ανεξάρτητα αν τα δεδομένα που παραβιάζονται είναι ευαίσθητα ή όχι, τότε η κοινοποίηση θα πρέπει να γίνεται εκτός από τις εποπτικές αρχές και στα άτομα. Αν οι πληροφορίες που παραβιάζονται αφορούν μια ευαίσθητη ομάδα όπως είναι τα παιδιά, τότε ο κίνδυνος θεωρείται μεγάλος και η κοινοποίησή της παραβίασης γίνεται και στα άτομα που τα αφορούν.

[23] GDPR, 2016/679: Άρθρο 34, παρ. 3β
[24] GDPR, 2016/679: Άρθρο 34, παρ. 3γ
[25] https://www.dpa.gr/el
[26] https://www.oag.ca.gov/privacy
[27] GDPR, 2016/679: Άρθρο 33, παρ.1
[28] GDPR, 2016/679: Άρθρο 34, παρ.1

Κοινό χαρακτηριστικό όλων των παραπάνω και αφετηρία της διαδικασίας κοινοποίησης μιας παραβίασης αποτελεί η χρονική στιγμή που ο υπεύθυνος επεξεργασίας λάβει γνώση της παραβίασης αυτής. Το ακριβές χρονικό σημείο όπου ο υπεύθυνος επεξεργασίας θεωρείται, ότι αποκτά γνώση μιας παραβίασης εξαρτάται από τις περιστάσεις της συγκεκριμένης παραβίασης. Σε κάποιες περιπτώσεις το σημείο αυτό είναι αρκετά σαφές από την αρχή, ενώ σε άλλες χρειάζεται περισσότερος χρόνος για να διαπιστωθεί[29]. Αυτό εξαρτάται από τα τεχνικά και οργανωτικά μέτρα που εφαρμόζονται για τον άμεσο εντοπισμό κάθε παραβίασης. Σε κάθε περίπτωση όμως σημαντικό είναι η έγκαιρη ανάληψη δράσης για τη διερεύνηση του περιστατικού από τον υπεύθυνο επεξεργασίας. Το πόσο σοβαρή μπορεί να είναι μια παραβίαση προσωπικών δεδομένων αξιολογείται από τους υπεύθυνους επεξεργασίας. Αυτό, μπορεί να προκύψει βάσει μιας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, που έχει πραγματοποιηθεί πριν από τη διενέργεια της επεξεργασίας τους. Η εκτίμηση αντικτύπου είναι μέρος της πολιτικής ασφάλειας της επιχείρησης, του γενικού σχεδίου ασφάλειας των πληροφοριών που έχει εκπονηθεί (βλ. παρακάτω παράγραφος 4). Με την εκτίμηση αντικτύπου μελετάται ο κίνδυνος που μπορεί να προκύψει από ένα συμβάν παραβίασης δεδομένων και αξιολογείται η σοβαρότητά του. Ανάλογα με αυτή, η παραβίαση γνωστοποιείται είτε στην αρμόδια εποπτική αρχή ή/και στα υποκείμενα. Ο κίνδυνος λοιπόν, αποτελεί ουσιαστικά τον παράγοντα ενεργοποίησης της υποχρέωσης γνωστοποίησης.

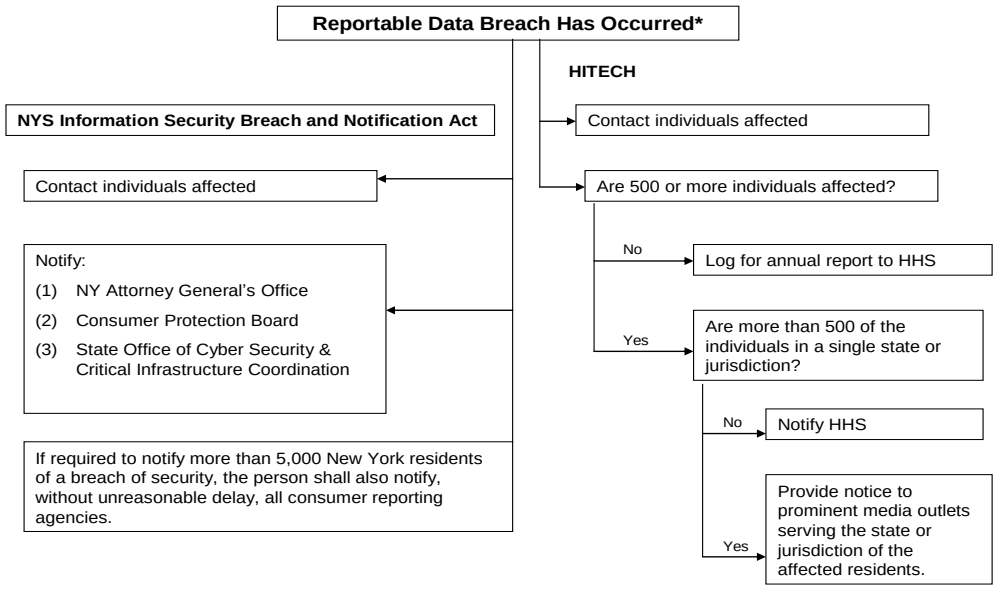
Οι απαιτήσεις της γνωστοποίησης μιας παραβίασης προσωπικών δεδομένων κατά τον ΓΚΠΔ, παρουσιάζονται διαγραμματικά στην παρακάτω εικόνα:

[29] Ομάδα Εργασίας 29, ΙΙ, Άρθρο 33, Γ.2



Εικόνα 4: Διάγραμμα ροής που απεικονίζει τις απαιτήσεις γνωστοποίησης

Αντίστοιχη διαγραμματική απεικόνιση παρέχεται για τις απαιτήσεις γνωστοποίησης βάσει των νόμων για κοινοποίηση δεδομένων της πολιτείας της Νέας Υόρκης (NYS Information Security Breach & Notification Act) και το νόμου προστασίας των δεδομένων υγείας (Health Information Technology for Economic and Clinical Health (HITECH) Act).

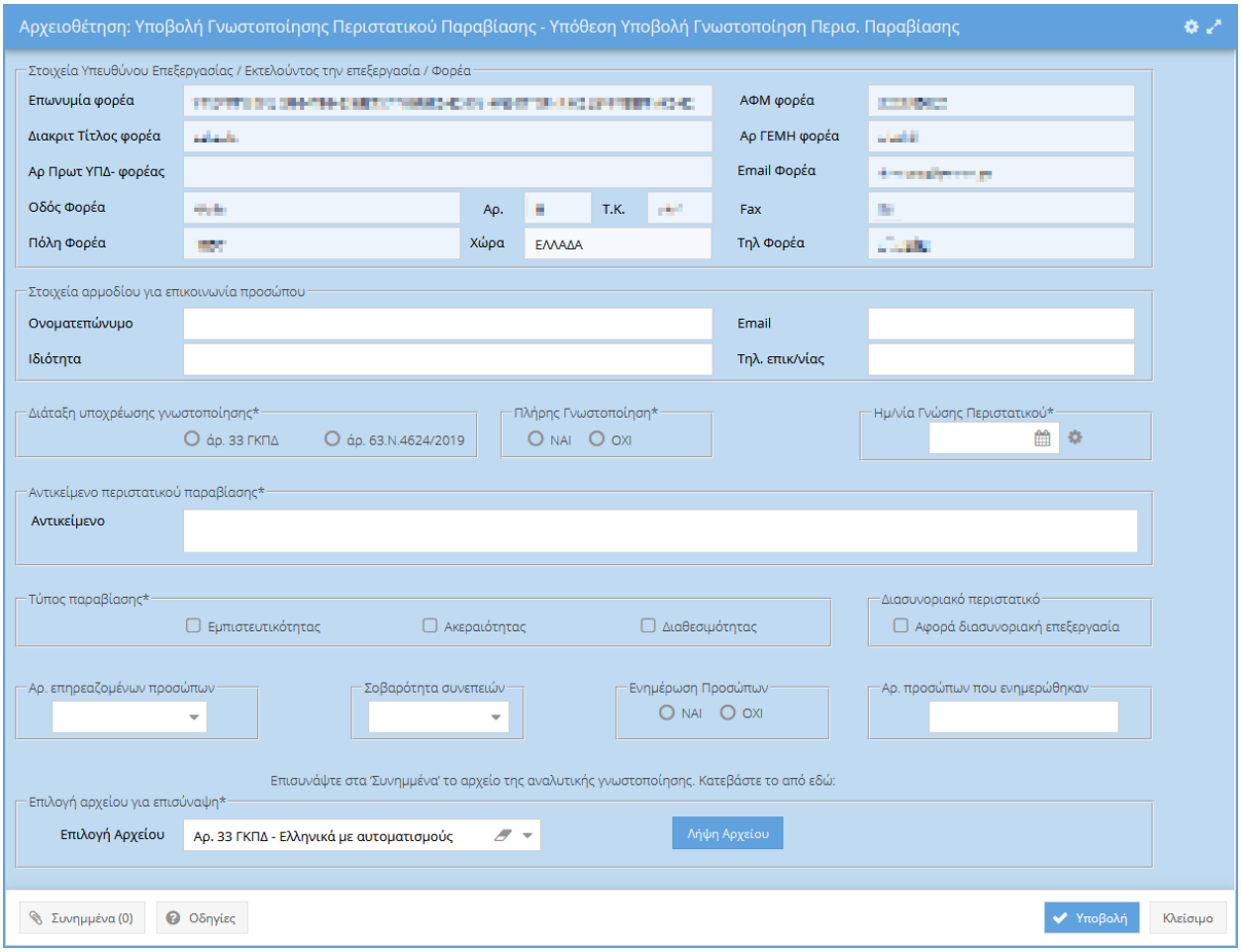


Εικόνα 5: Διάγραμμα ροής με τις απαιτήσεις γνωστοποίησης (ΗΠΑ)

3.2.2 ΠΩΣ ΓΙΝΕΤΑΙ Η ΚΟΙΝΟΠΟΙΗΣΗ

Η κοινοποίηση μιας παραβίασης δεδομένων στα υποκείμενα των δεδομένων, μπορεί να τελεσθεί με διάφορους τρόπους, όπως μέσω έντυπης ή ηλεκτρονικής αλληλογραφίας, SMS ή μέσω δημόσιας ανακοίνωσης. Βάσει της φύσης της παραβίασης καθώς και του αριθμού των ατόμων που επηρεάστηκαν, η κοινοποίηση γίνεται μέσω αλληλογραφίας απ' ευθείας σε αυτά. Σύμφωνα με τον ΓΚΠΔ, αν ο αριθμός των ατόμων των οποίων τα προσωπικά δεδομένα παραβιάστηκαν είναι μεγάλος ή τα στοιχεία για την απευθείας επικοινωνία μαζί τους είναι δύσκολο να βρεθούν ή η απευθείας ενημέρωση των υποκειμένων προϋποθέτει δυσανάλογες προσπάθειες, η κοινοποίηση γίνεται είτε μέσω δημόσιας ανακοίνωσης σε περίοπτη θέση στην ιστοσελίδα της επιχείρησης ή του οργανισμού που είχε την ευθύνη της προστασίας των δεδομένων, είτε μέσω ανακοίνωσης στα μέσα μαζική ενημέρωσης. Η κοινοποίηση σε κάθε περίπτωση γίνεται με τρόπο σαφή και διαφανή. Για παράδειγμα τα μηνύματα SMS ή τα email είναι συγκεκριμένα και δεν πρέπει να συγχέονται

με άλλες πληροφορίες όπως τακτικές ενημερώσεις, τυποποιημένα μηνύματα, ενημερωτικά δελτία. Ένα δελτίο τύπου ή αποκλειστική ανακοίνωση της παραβίασης στον ιστότοπο της εταιρίας δεν συνιστά αποτελεσματικό τρόπο ανακοίνωσης[30]. Αντίστοιχα, βάσει νόμων στις ΗΠΑ, σε κάποιες πολιτείες, η κοινοποίηση συνιστάται να γίνεται γραπτώς, σε ηλεκτρονική ή έντυπη μορφή, ενώ σε άλλες τηλεφωνικά. Σε πολλές πολιτείες ορίζονται εναλλακτικοί τρόποι ενημέρωσης, σε περίπτωση που το κόστος των παραπάνω καθίσταται δυσανάλογο ή ο αριθμός των ατόμων που επηρεάστηκαν ήταν μεγάλος ή δεν υπάρχουν αρκετά στοιχεία επικοινωνίας, όπως μέσω ηλεκτρονικής αλληλογραφίας, ανακοίνωση στον ιστότοπο της εταιρείας ή στα Μέσα Μαζικής Ενημέρωσης. Σε περίπτωση κοινοποίησης μιας παραβίασης προσωπικών δεδομένων στους αρμόδιου φορείς , αυτή γίνεται μέσω ειδικών εντύπων που διατίθενται και συμπληρώνονται και διαδικτυακά στις ιστοσελίδες της εκάστοτε εποπτικής αρχής, όπως στο παρακάτω[31]:



Εικόνα 6: Πρότυπο υποβολής γνωστοποίησης περιστατικού παραβίασης στην εποπτική αρχή βάσει του ΓΚΠΔ

[30] Ομάδα Εργασίας 29: III, Άρθρο 34, Θ

[31] https://www.dpa.gr/el/syndesi/foreis/gnostopoiisi_peristatikou_paraviasis

Στις περισσότερες περιπτώσεις παρέχεται ένα έντυπο σε στυλ ερωτηματολογίου, μέσω του οποίου παρέχονται οι βασικές λεπτομέρειες της παραβίασης.

3.2.3 ΤΙ ΠΕΡΙΛΑΜΒΑΝΕΙ ΜΙΑ ΚΟΙΝΟΠΟΙΗΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Μόλις γίνει αντιληπτή μια παραβίαση προσωπικών δεδομένων από τον υπεύθυνο επεξεργασίας της επιχείρησης ή τον οργανισμό που διαχειρίζεται τα δεδομένα αυτά, αυτή θα πρέπει να κοινοποιηθεί στις εποπτικές αρχές ή και στα υποκείμενα των δεδομένων, ανάλογα με τις προϋποθέσεις που αναφέρθηκαν πιο πάνω. Το περιεχόμενο κάθε κοινοποίησης ορίζεται από τους εκάστοτε νόμους περί προστασίας των προσωπικών δεδομένων, ώστε αυτό να ικανοποιεί το δικαίωμα των υποκειμένων στην ενημέρωση της παραβίασης των προσωπικών τους δεδομένων και να παρέχει στους οργανισμούς κίνητρα για την ανάληψη επιπλέον μέτρων προστασίας των δεδομένων που διαχειρίζονται.

- Κοινοποίηση στις εποπτικές αρχές.

Σύμφωνα με την αιτιολογική σκέψη 85, ένας από τους σκοπούς της γνωστοποίησης είναι ο περιορισμός της ζημιάς για τα υποκείμενα των δεδομένων. Συνεπώς, η κοινοποίηση μιας παραβίασης που είχε σαν αποτέλεσμα συγκεκριμένη ζημιά για τα υποκείμενα, θα πρέπει κατ' ελάχιστο να περιλαμβάνει:

- Περιγραφή της φύσης της παραβίασης. Πληροφορίες που σχετίζονται με τον τρόπο και τον χρόνο στον οποίον ο υπεύθυνος επεξεργασίας έλαβε γνώση της παραβίασης, πληροφορίες που αφορούν στην κατηγορία και τον αριθμό των ατόμων που την αφορούν καθώς και πληροφορίες σχετικές με το είδος και τον αριθμό των δεδομένων που παραβιάστηκαν.
- Το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας των δεδομένων ή οποιουδήποτε συνέταξε την κοινοποίηση και θα μπορούσε να παρέχει περισσότερες πληροφορίες σχετικές με την παραβίαση.
- Περιγραφή των πιθανών συνεπειών, οικονομικών, ηθικών ή άλλων της παραβίασης.
- Περιγραφή των μέτρων που είχαν ληφθεί ή προτείνονται να ληφθούν από τον υπεύθυνο επεξεργασίας και σχετίζονται με την παραβίαση. Τέτοιες πληροφορίες περιλαμβάνουν τις ενέργειες που έγιναν κατά την ανακάλυψη της παραβίασης, αν η παραβίαση αυτή έχει αναφερθεί στις αρχές επιβολής του νόμου, αν τα δεδομένα που παραβιάστηκαν έχουν χρησιμοποιηθεί για εγκληματικούς σκοπούς ή ποια μέτρα έχουν ληφθεί, ώστε να εξασφαλιστεί η αποτροπή μελλοντικής παραβίασης[32].

[32] GDPR, 2019/679: Άρθρο 33, παρ. 3

SAMPLE LETTER TO ATTORNEY GENERAL

Date

Attorney General Maura Healey
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Dear Attorney General Healey:

Pursuant to M.G.L. c. 93H, we are writing to notify you of data security incident involving [number] Massachusetts resident[s]. [*If applicable*: This notice provides updated information relating to an incident previously reported to your Office on [date].]

IDENTIFICATION OF PARTIES

[This paragraph should identify all parties involved in the incident and the reporting of the incident. If the party reporting this incident is different from the entity that experienced it, provide the name and address of that entity that experienced the incident, and describe your relationship to it and the nature of your entity's goods or services (e.g. law firm, service provider). If known, also identity the person responsible for the incident].

NATURE OF THE DATA SECURITY INCIDENT

[This paragraph should provide the date of the incident, a description of the nature of the incident, a description of the categories of personal information and/or other data involved in the incident, and disclose whether the personal information and/or other data that was the subject of the incident was in electronic or paper form, and if in electronic form, whether it or the media on which it was stored was encrypted. Finally, indicate whether you are aware of any resulting identity theft, fraud, or financial losses to consumers].

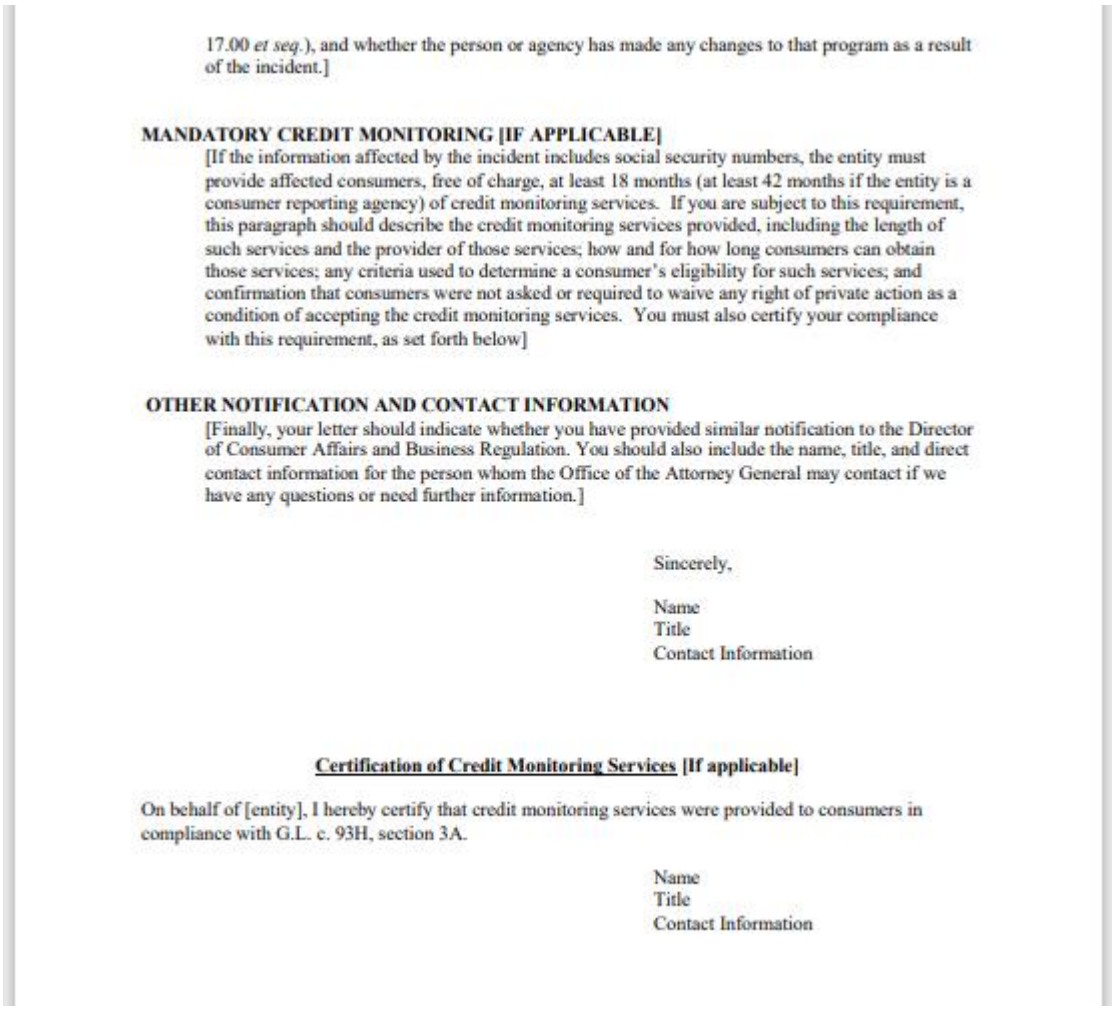
NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED

[This paragraph should specify the number of affected individuals residing in Massachusetts whose personal information was the subject of the incident, as known at the time of this notification. This paragraph should also indicate that these Massachusetts residents have received or will shortly receive notice pursuant to M.G.L. c. 93H, s. 3(b) and should specify the manner in which Massachusetts residents have or will receive such notice. You must also include a copy of the notice to affected Massachusetts residents along with your notification to the Attorney General].

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

[This paragraph should outline all the steps you have taken or plan to take relating to the incident including, without limitation, what you did when you discovered the incident; whether you have reported the incident to law enforcement; whether you have any evidence that the personal information has been used for fraudulent purposes; whether you intend to offer credit morning services to consumers; and what measures you have taken to ensure that similar incidents do not occur in the future.

This paragraph should further indicate whether the person or agency affected by the incident maintained, at the time of the incident, a written information security program (*see* 201 CMR



17.00 *et seq.*), and whether the person or agency has made any changes to that program as a result of the incident.]

MANDATORY CREDIT MONITORING [IF APPLICABLE]

[If the information affected by the incident includes social security numbers, the entity must provide affected consumers, free of charge, at least 18 months (at least 42 months if the entity is a consumer reporting agency) of credit monitoring services. If you are subject to this requirement, this paragraph should describe the credit monitoring services provided, including the length of such services and the provider of those services; how and for how long consumers can obtain those services; any criteria used to determine a consumer's eligibility for such services; and confirmation that consumers were not asked or required to waive any right of private action as a condition of accepting the credit monitoring services. You must also certify your compliance with this requirement, as set forth below]

OTHER NOTIFICATION AND CONTACT INFORMATION

[Finally, your letter should indicate whether you have provided similar notification to the Director of Consumer Affairs and Business Regulation. You should also include the name, title, and direct contact information for the person whom the Office of the Attorney General may contact if we have any questions or need further information.]

Sincerely,

Name
Title
Contact Information

Certification of Credit Monitoring Services [If applicable]

On behalf of [entity], I hereby certify that credit monitoring services were provided to consumers in compliance with G.L. c. 93H, section 3A.

Name
Title
Contact Information

Εικόνα 7: Οδηγίες για την ενημέρωση του Γενικού Εισαγγελέα Μασσαχουσσέτης για παραβίαση προσωπικών δεδομένων

Οι παραπάνω πληροφορίες παρέχονται κατ' ελάχιστο από τον υπεύθυνο επεξεργασίας. Ωστόσο, βάσει της κάθε παραβίασης, ενδέχεται να απαιτείται η παροχή περαιτέρω πληροφοριών για την πλήρη επεξήγηση των περιστάσεων κάθε περίπτωσης[33]. Η κάθε εποπτική αρχή μπορεί επίσης να απαιτήσει από τον υπεύθυνο επεξεργασίας περαιτέρω λεπτομέρειες για την παραβίαση.

Όπως αναφέρθηκε προηγούμενα, αν ο υπεύθυνος επεξεργασίας δεν καταφέρει να ενημερώσει την αντίστοιχη εποπτική αρχή μέσα στους χρόνους που προβλέπεται από το αντίστοιχο νομικό πλαίσιο, τότε θα πρέπει να παρέχει τους λόγους της καθυστέρησης αυτής και η κοινοποίηση μπορεί να γίνει τμηματικά[34].

[33] Ομάδα Εργασίας 29, Δ.5
[34] GDPR, 2016/679: Άρθρο 33, παρ.1

- Κοινοποίηση στα υποκείμενα των δεδομένων

Οι υπεύθυνοι επεξεργασίας, όπως αναφέρθηκε προηγούμενα, υποχρεούνται υπό ορισμένες προϋποθέσεις να κοινοποιούν την παραβίαση των δεδομένων και στα υποκείμενα των δεδομένων. Η υποχρέωση αυτή γίνεται παράλληλα με την υποχρέωση κοινοποίησης της παραβίασης προσωπικών δεδομένων στην εκάστοτε εποπτική αρχή. Σκοπός της είναι να παρέχει στα υποκείμενα των δεδομένων επαρκή ενημέρωση, ώστε να λάβουν τα απαραίτητα μέτρα για να μετριάσουν τις συνέπειες της παραβίασης[35].

Το περιεχόμενο της κοινοποίησης στα υποκείμενα των δεδομένων δεν είναι πολύ διαφορετικό από αυτό της κοινοποίησης στις εποπτικές αρχές. Περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται πληροφορίες που αφορούν τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας των δεδομένων, τις συνέπειες της παραβίασης καθώς και τα μέτρα που ελήφθησαν ή προτείνεται να ληφθούν από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης και τον περιορισμό των συνεπειών της[36] [20]. Για παράδειγμα, ο υπεύθυνος επεξεργασίας μπορεί να αναφέρει στα υποκείμενα ότι έχει ενημερώσει τις εποπτικές αρχές και έχει λάβει τις κατάλληλες οδηγίες ή να παρέχει συμβουλές στα υποκείμενα για την προστασία τους, όπως επαναφορά κωδικού πρόσβασης, ακύρωση πιστωτικών καρτών κ.α..

Η ανακοίνωση της παραβίασης στα άτομα των οποίων τα δεδομένα παραβιάστηκαν, πρέπει να είναι προσβάσιμη σε κατάλληλους εναλλακτικούς μορφότυπους και στις σχετικές γλώσσες, ώστε να διασφαλίζεται ότι είναι κατανοητή και να επιτυγχάνεται ο στόχος της[37]. Κατά τη σύνταξη της κοινοποίησης μιας παραβίασης προσωπικών δεδομένων που απευθύνεται στα υποκείμενα των δεδομένων λοιπόν, σημαντικό ρόλο έχει το στυλ της. Σύμφωνα με τον Bisogni [19], τα 4 βασικά στοιχεία μιας κοινοποίησης είναι: η σαφήνεια στην περιγραφή του περιστατικού, το ύφος στην περιγραφή των πιθανών συνεπειών δεδομένης της αντίδρασης του υπευθύνου επεξεργασίας, οι ενέργειες που πρέπει να ληφθούν από τα υποκείμενα και η αλληλεπίδραση με τα υποκείμενα των δεδομένων που παραβιάστηκαν. Η σαφήνεια στην περιγραφή των περιστατικών και των προσωπικών δεδομένων που παραβιάστηκαν δίνουν στους αποδέκτες της κοινοποίησης τη δυνατότητα να αξιολογήσουν τη σοβαρότητα της παραβίασης. Η αποφυγή του καθησυχαστικού ύφους στην περιγραφή των πιθανών συνεπειών της παραβίασης δίνει στους ίδιους τη δυνατότητα για γρήγορη και ουσιαστική αντίδραση. Η λεπτομερής και σαφής περιγραφή των μέτρων που προτείνεται να λάβουν είναι ουσιαστική για τον μετριασμό των συνεπειών της παραβίασης. Τέλος, η αλληλεπίδραση που προτείνεται στα υποκείμενα με τις εταιρείες διαχείρισης των δεδομένων τους, τους παρέχει την απαραίτητη διαφάνεια και υποστήριξη.

Στο παρακάτω παράδειγμα διακρίνονται τα χαρακτηριστικά της κοινοποίησης που αναφέρει ο Bisogni. Η γλώσσα που χρησιμοποιείται είναι απλή και κατανοητή. Το ύφος της ειδοποίησης είναι ειλικρινές και απολογητικό, δηλώνοντας το ενδιαφέρον της εταιρείας. Στην πρώτη παράγραφο, περιγράφεται το είδος της παραβίασης ακολουθούμενη από μια παράγραφο, στην οποία αναφέρονται τα δεδομένα που παραβιάστηκαν. Στη συνέχεια, περιγράφονται τα μέτρα που πάρθηκαν από την εταιρεία καθώς και μέτρα που μπορούν να ληφθούν από τους χρήστες με σκοπό την προστασία τους από μελλοντική εσφαλμένη χρήση των προσωπικών δεδομένων τους.

[35] Αιτιολογική σκέψη 86
[36] GDPR, 2016/679: Άρθρο 34, παρ.2
[37] Ομάδα Εργασίας 29, Θ

Τέλος, παρέχονται στοιχεία επικοινωνίας με την εταιρεία, καθώς και ένα σύνολο ερωταπαντήσεων προς ενημέρωση των χρηστών.

Notice of Data Breach: May 2016

You may have heard reports recently about a security issue involving LinkedIn. We would like to make sure you have the facts about what happened, what information was involved, and the steps we are taking to help protect you.

What Happened?

On May 17, 2016, we became aware that data stolen from LinkedIn in 2012 was being made available online. This was not a new security breach or hack. We took immediate steps to invalidate the passwords of all LinkedIn accounts that we believed might be at risk. These were accounts created prior to the 2012 breach that had not reset their passwords since that breach.

What Information Was Involved?

Member email addresses, hashed passwords, and LinkedIn member IDs (an internal identifier LinkedIn assigns to each member profile) from 2012.

What We Are Doing?

We invalidated passwords of all LinkedIn accounts created prior to the 2012 breach that had not reset their passwords since that breach In addition, we are using automated tools to attempt to identify and block any suspicious activity that might occur on LinkedIn accounts. We are also actively engaging with law enforcement authorities.

Also, since the data was stolen in 2012, LinkedIn has taken significant steps to strengthen account security. For example, we now use salted hashes to store passwords and enable additional account security by offering our members the option to use two-step verification.

What You Can Do.

We have several dedicated teams working diligently to ensure that the information members entrust to LinkedIn remains secure. While we do all we can, we always suggest that our members visit our Safety Center to learn about enabling two-step verification, and implementing strong passwords in order to keep their accounts as safe as possible.

We recommend that you regularly change your LinkedIn password and if you use the same or similar passwords on other online services, we recommend you set new passwords on those accounts as well.

For More Information.

If you have any questions, please feel free to contact our Trust & Safety team at **safety@linkedin.com**. To learn more visit our official blog.

Εικόνα 8: Παράδειγμα κοινοποίησης περιστατικού παραβίασης δεδομένων (LinkedIn 2016)

3.2.4 ΣΥΝΕΠΕΙΕΣ ΜΗ ΚΟΙΝΟΠΟΙΗΣΗΣ ΜΙΑΣ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Δεδομένης της αναγκαιότητας και της υποχρεωτικότητας της κοινοποίησης μιας παραβίασης προσωπικών δεδομένων, όπως αυτή ορίζεται από τους εκάστοτε νόμους και κανόνες κάθε κράτους, η μη τήρηση αυτής οδηγεί σε κυρώσεις. Όπως αναφέρθηκε παραπάνω, η κοινοποίηση μιας παραβίασης δεδομένων καθίσταται υποχρεωτική προς τους υπεύθυνους επεξεργασίας των δεδομένων ή των αντίστοιχων αρχών ή και προς τα υποκείμενα των δεδομένων, αν πληρούνται ορισμένες προϋποθέσεις. Η παραβίαση της υποχρέωσης αυτής συνίσταται είτε στην απουσία της κοινοποίησης, είτε στην αργοπορημένη κοινοποίησή της. Στις περιπτώσεις αυτές οι υπεύθυνοι επεξεργασίας των δεδομένων είτε απέτυχαν να εκτιμήσουν σωστά το ρίσκο και τις συνέπειες της παραβίασης θεωρώντας τα χαμηλά, είτε θεώρησαν την κοινοποίηση επιβλαβή για την φήμη και την αξιοπιστία τους οργανισμού/επιχείρησής τους και κατά συνέπεια δεν επικοινώνησαν την παραβίαση αυτή στα αρμόδια μέρη (εποπτικές αρχές ή υποκείμενα των δεδομένων),είτε απέτυχαν να αιτιολογήσουν την αργοπορημένη κοινοποίηση στα μέρη αυτά. Σημειώνεται ότι σύμφωνα με την πλειοψηφία των αντίστοιχων νομοθεσιών, η κοινοποίηση μιας παραβίασης δεδομένων πρέπει να γίνεται χωρίς καθυστέρηση από τη στιγμή που αυτή θα γίνει αντιληπτή και τυχόν καθυστέρηση αυτής θα πρέπει να συνοδεύεται από κατάλληλη αιτιολόγηση.

Βασικότερες συνέπειες της παραβίασης της υποχρέωσης κοινοποίησης είναι οι οικονομικές. Αυτές μεταφράζονται σε διοικητικά πρόστιμα που ορίζονται από τους ισχύοντες νόμους και τα οποία ποικίλλουν ανάλογα με το είδος και τις συνθήκες της παραβίασης. Η μη συμμόρφωση προς την υποχρέωση έγκαιρης κοινοποίησης μιας παραβίασης προσωπικών δεδομένων μπορεί να επισύρει σύμφωνα με τον GDPR, διοικητικά πρόστιμα έως 10.000.000 Ευρώ ή σε περίπτωση επιχείρησης έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο[38]. Αντίστοιχες ποινές προβλέπονται και από νόμους σε πολιτείες της Αμερικής. Σε κάποιες επιβάλλεται ένα όριο στις χρηματικές ποινές που μπορούν να επιβληθούν. Το όριο ορίζεται είτε σαν ένα ποσό ανά περιστατικό, είτε ένα ποσό ανά record δεδομένων που διέρρευσαν. Κάποιες άλλες πολιτείες επιτρέπουν επίσης στα υποκείμενα των δεδομένων να κινηθούν νομικά ενάντια στα άτομα ή τις επιχειρήσεις που παραβίασαν την υποχρέωση αυτή [21]. Σε κάθε περίπτωση, η επιβαλλόμενες ποινές οφείλουν να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές[39].

Το 2016, διέρρευσαν λογαριασμοί 57 εκ. χρηστών και 600.000 οδηγών της εταιρείας UBER. Η εταιρεία δεν κοινοποίησε την παραβίαση αυτή και επέλεξε να υποκύψει στις απαιτήσεις των εγκληματιών, πληρώνοντάς τους 100.000$ για να την κρατήσουν κρυφή. Όταν όμως αυτή ήρθε στο φως το 2018, η εταιρεία αναγκάστηκε να καταβάλλει πρόστιμο ύψους 148 εκ. δολαρίων για παραβίαση της νομοθεσίας περί κοινοποίησης παραβίασης δεδομένων. Το πρόστιμο αυτό είναι μέχρι και σήμερα το μεγαλύτερο που έχει επιβληθεί για τον σκοπό αυτό[40]. Αντίστοιχο παράδειγμα παραβίασης της υποχρέωσης κοινοποίησης είναι και αυτό της εταιρείας Booking.com. Στην εταιρεία επιβλήθηκε πρόστιμο ύψους 475.000 Ευρώ από την αρχή προστασίας δεδομένων της Δανίας, όχι γιατί απέκρυψε παραβίαση προσωπικών δεδομένων, αλλά γιατί καθυστέρησε να επικοινωνήσει την παραβίαση αυτή στην αρχή, αλλά και στα υποκείμενα των δεδομένων.

[38] GDPR, Άρθρο 83, παρ.4

[39] GDPR, Άρθρο 83, παρ.1

[40] https://ag.ny.gov/press-release/2018/ag-underwood-announces-record-148-million-settlement-uber-over-2016-data-breach

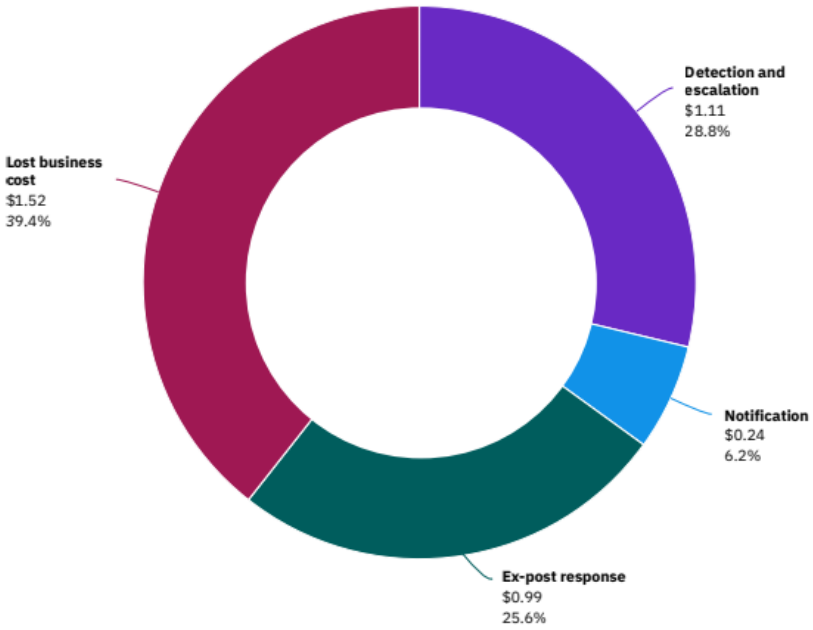
Σύμφωνα με την αναφορά της αρχής, η διαρροή των δεδομένων πραγματοποιήθηκε τον Δεκέμβρη του 2018, κατά την οποία διέρρευσαν δεδομένα 4109 πελατών, όπως ονόματα, διευθύνσεις, τηλέφωνα και αριθμοί πιστωτικών καρτών. Η εταιρεία έγινε ενήμερη για την διαρροή στις 13 Ιανουαρίου του 2019, ωστόσο ενημέρωσε τους πελάτες της στις 4 Φεβρουαρίου του 2019 και την αρχή προστασίας δεδομένων στις 7 Φεβρουαρίου του 2019. Σύμφωνα με τον ισχύοντα κανονισμό, η εταιρεία θα έπρεπε να ειδοποιήσει την αρχή μέχρι τις 16 Ιανουαρίου, δηλαδή 22 μέρες νωρίτερα από ότι το έκανε[41].

Αντίστοιχης βαρύτητας συνέπειες με τις οικονομικές και νομικές που μπορεί να αντιμετωπίσουν οι οργανισμοί ή οι επιχειρήσεις, είναι και οι συνέπειες στη φήμη και την αξιοπιστία τους. Όταν μια επιχείρηση κοινοποιεί ένα τέτοιο συμβάν και τις ενέργειες που έχει λάβει ώστε να μετριάσει τις συνέπειές του, δείχνει ότι έχει τον έλεγχο της κατάστασης και ενδιαφέρεται για τα υποκείμενα των δεδομένων και τους νόμους. Από την άλλη, όταν μια επιχείρηση επιλέγει να αποκρύψει ένα τέτοιο συμβάν αντιμετωπίζει τον κίνδυνο της απώλειας των πελατών της και της εμπιστοσύνης τους. Σε μια παραβίαση προσωπικών δεδομένων, εκτός από την εταιρεία που μπορεί να αποδείξει αυτό το συμβάν, αυτοί που έχουν γνώση του γεγονότος είναι αυτοί που το έχουν διαπράξει. Υποκύπτοντας η εταιρεία στον εκβιασμό τους (όπως έγινε στην περίπτωση της UBER που περιγράφεται παραπάνω), δείχνει ότι δεν φοβάται τόσο τις ποινικές συνέπειες, όσο τις συνέπειες στη φήμη και την αξιοπιστία της [22]. Η αδυναμία προστασίας των προσωπικών δεδομένων των πελατών αποτελεί μεγάλο πλήγμα για πολλές εταιρείες παροχής ηλεκτρονικών υπηρεσιών, εμπορίου, ιατρικών υπηρεσιών κλπ.

Στην έκθεση της IBM και του ινστιτούτου Ponemon για το κόστος των παραβιάσεων δεδομένων, οι ενέργειες που αφορούν στην επικοινωνία των εταιρειών με τα θύματα των παραβιάσεων, αλλά και οι σχετικές με τη συμμόρφωση προς τους κανονισμούς, αποτελούν βασικές συνιστώσες για τον υπολογισμό του κόστους μιας παραβίασης δεδομένων[42]. Ειδικότερα, οι συνέπειες μιας παραβίασης, στις οποίες περιλαμβάνονται οι ενέργειες της κοινοποίησης της παραβίασης, αλλά και της συμμόρφωσης με τους κανονισμούς, καθώς και οι απώλειες στη φήμη και την αξιοπιστία των εταιρειών, αποτελούν το μεγαλύτερο κομμάτι του συνολικού κόστους (Εικ.5)

[41] https://autoriteitpersoonsgegevens.nl/en/news/bookingcom-fined-delay-reporting-data-breach

[42]https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf (Ex-post response: Activities to help victims of a breach communicate with the company and redress activities to victims and regulators)



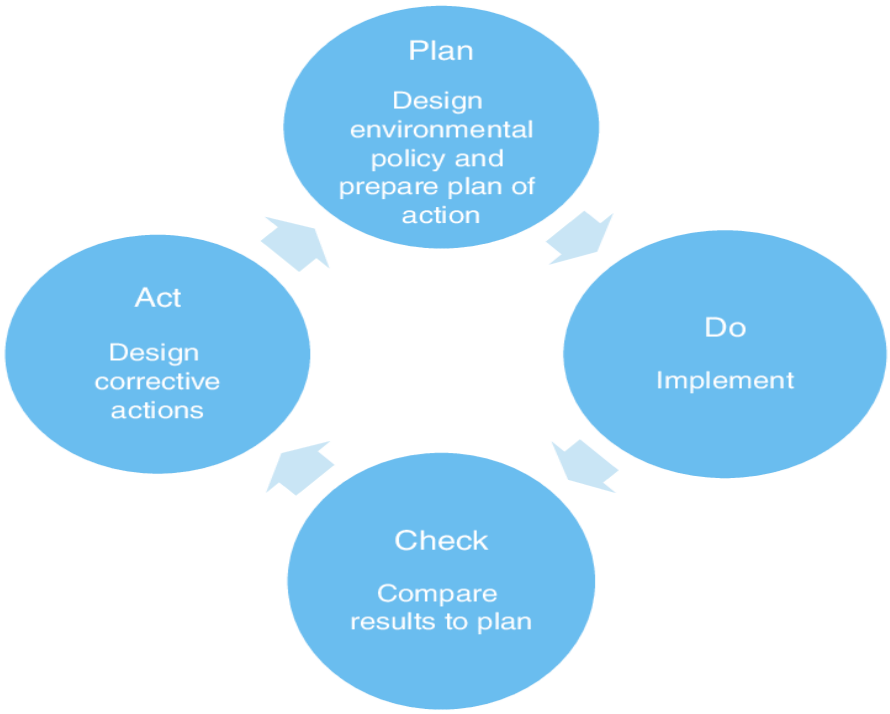
Εικόνα 9: Κόστος παραβίασης δεδομένων για το 2020, σύμφωνα με την έκθεση της IBM

4. ΚΟΙΝΟΠΟΙΗΣΗ ΣΑΝ ΜΕΡΟΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΜΙΑΣ ΕΠΙΧΕΙΡΗΣΗΣ

Το ζήτημα της διαχείρισης της ασφάλειας πληροφοριών (information security management) είναι πολύ σημαντικό για τη λειτουργία κάθε οργανισμού ή επιχείρησης. Η πληροφορία αποτελεί βασικό περιουσιακό στοιχείο για την εύρυθμη λειτουργία, την κερδοφορία και την απόδοση των επιχειρήσεων[9]. Εξαιτίας της σπουδαιότητας αυτής της πληροφορίας, χρειάζεται να προστατευθεί και να διασφαλιστεί η αξιοπιστία της ώστε να αποκλειστούν οι κίνδυνοι μη εξουσιοδοτημένης πρόσβασης ή αποκάλυψης, αλλοίωσης ή/και καταστροφής της. Η έννοια της ασφάλειας της πληροφορίας, προσδιορίζεται από τις παρακάτω συνιστώσες: την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα. Η πληροφορία θα πρέπει να παραμείνει κρυφή σε μη εξουσιοδοτημένους χρήστες, να παραμένει πλήρης, ακριβής και έγκυρη και να είναι πάντα διαθέσιμη προς χρήση. Εξαιτίας της ολοένα αυξανόμενης σπουδαιότητας της πληροφορίας στα σύγχρονα πληροφοριακά συστήματα, στις παραπάνω συνιστώσες έρχονται να προστεθούν και οι έννοιες της λογοδοσίας, η έμπρακτη απόδοση ευθυνών αναφορικά με την προστασία της πληροφορίας, η αξιοπιστία, η διαφάνεια, η μη αποποίηση και η προστασία από κακόβουλες ενέργειες. Η ασφάλεια των πληροφοριών είναι μια συνεχής και επαναλαμβανόμενη διαδικασία διαχείρισης των σχετικών κινδύνων και διασφάλισης των παραπάνω συνιστωσών. Αποτελεί έναν στρατηγικό στόχο κάθε οργανισμού και μια συνεχή διαδικασία σχεδιασμού, διαχείρισης, ελέγχου και συντονισμού, με σκοπό τη διασφάλιση επαρκούς επιπέδου ασφάλειας για τις εταιρείες και τους οργανισμούς[10]. Είναι μια διαδικασία που αφορά μια επιχείρηση στην ολότητά της και όχι μόνο σε τεχνικό επίπεδο. Είναι λάθος και ανέφικτο να θεωρούνται επαρκείς μέθοδοι ασφαλείας οι μεμονωμένες τεχνολογικές λύσεις, όπως η χρήση αναχωμάτων προστασίας (firewalls), αντιϊκά προγράμματα, ψηφιακές υπογραφές κ.λπ., καθώς αυτές προσφέρουν μεν λύση στο πρόβλημα της ασφάλειας, αλλά μόνο στο πεδίο που εφαρμόζονται [11]. Είναι μια επιχειρησιακή διεργασία και όχι ένα αμιγώς τεχνικό θέμα. Συμπεριλαμβάνει παραμέτρους από διάφορους χώρους, όπως οικονομία, διοίκηση, κοινωνία κ.λπ., οι στόχοι των οποίων και οι διαδικασίες τους θα πρέπει να είναι σαφώς ορισμένες και ελεγμένες προκειμένου να επιτευχθεί ένας αποδοτικός συντονισμός τους. Για το λόγο αυτό, αρκετοί οργανισμοί έχουν αναπτύξει μεθοδολογίες που καλύπτουν τις ανάγκες των επιχειρήσεων για ασφάλεια των πληροφοριών. Τα πρότυπα αυτά παρέχουν μια συστηματική προσέγγιση για την υιοθέτηση των βέλτιστων πρακτικών ελέγχου, ποσοτικοποίησης του ρίσκου και εφαρμογής κατάλληλων μέτρων προστασίας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Κάποιες από τις μεθοδολογίες που έχουν αναπτυχθεί και που χρησιμοποιούν ή στηρίζονται σε κάποιο από τα γνωστά πρότυπα είναι οι παρακάτω[9]:

- OCTAVE, το οποίο έχει αναπτυχθεί από τον οργανισμό CERT
- BS 7799, το οποίο έχει αναπτυχθεί από το British Standard Institute
- COBIT, το οποίο έχει αναπτυχθεί από τον οργανισμό ISACA (International Information Technology Association)
- NIST SP 800-14, το οποίο έχει αναπτυχθεί από το National Institute of Standards & Technology
- ISO 27001, το οποίο εκδόθηκε το 2005 και εστιάζει κυρίως στην προσέγγιση της εκτίμησης των κινδύνων και θεωρείται το πιο ευρέως χρησιμοποιήσιμο πρότυπο.

Σύμφωνα με το πρότυπο ISO27001, η ανάπτυξη ενός συστήματος διαχείρισης της ασφάλειας πληροφοριών, βασίζεται σε τέσσερα στάδια (μέθοδος Plan-Do-Check-Act): στον Σχεδιασμό, την Υλοποίηση, τον Έλεγχο και τη Δράση. Κατά τη φάση του σχεδιασμού γίνεται ανάλυση και εκτίμηση της επικινδυνότητας για την ασφάλεια των πληροφοριών. Αυτό γίνεται λαμβάνοντας υπόψη, ανάμεσα σε άλλα, τις πιθανές απειλές που αντιμετωπίζει η επιχείρηση, μέσω ενός σχεδίου αποτίμησης επικινδυνότητας, το νομικό και κανονιστικό πλαίσιο λειτουργίας της επιχείρησης και το σύνολο των στόχων και των αρχών της επιχείρησης [12]. Κατά τη φάση της υλοποίησης, με βάση τα παραπάνω αποτελέσματα της αποτίμησης, γίνεται η επιλογή και η υλοποίηση κατάλληλων μέτρων προστασίας, όπως σχέδιο διαχείρισης επικινδυνότητας, υλοποίηση μέτρων ασφάλειας, ενημέρωση και κατάρτιση προσωπικού, υλοποίηση διαδικασιών έγκαιρης και έγκυρης ανίχνευσης και αντιμετώπισης περιστατικών ασφαλείας. Κατά τον έλεγχο, γίνεται αξιολόγηση των αποτελεσμάτων των παραπάνω δράσεων σε σχέση με τους αρχικούς στόχους της επιχείρησης. Η διαδικασία αυτή είναι περιοδικά επαναλαμβανόμενη. Τέλος, κατά τη φάση της δράσης, πραγματοποιούνται όλες εκείνες οι ενέργειες που ορίστηκαν ώστε να βελτιωθεί η διαχείριση της ασφάλειας των πληροφοριών.

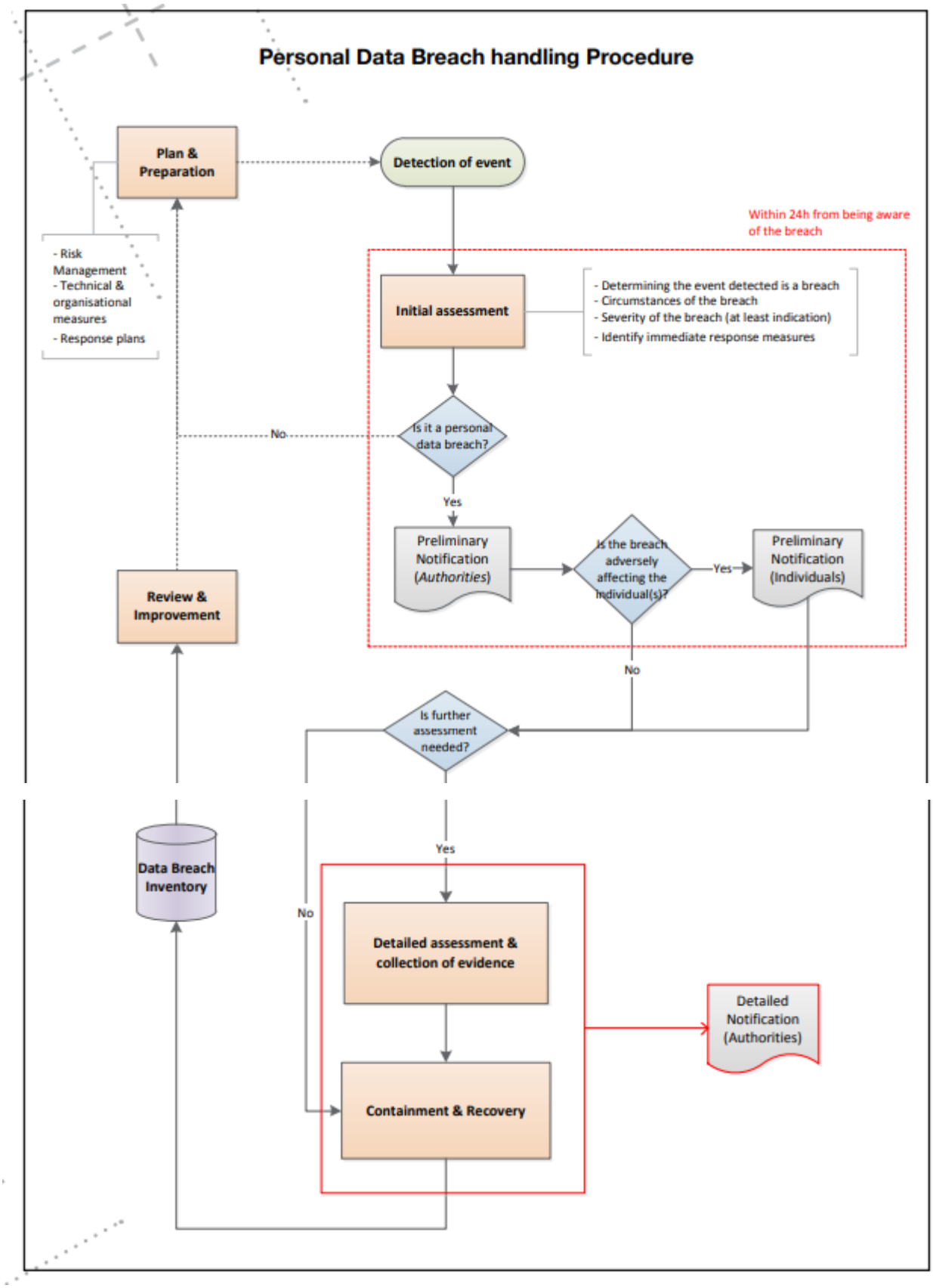


Εικόνα 10: ISO 14001 plan-do-check-act model. Πηγή : http://www.alexfert.com/new/content_ones/view/1/menuid:224

Στη διαδικασία επιλογής των μέτρων προστασίας, λαμβάνονται υπόψη ανάμεσα σε άλλα, το κόστος υλοποίησής τους, το κόστος των επιπτώσεών τους, νομικοί, κανονιστικοί και ποιοτικοί

παράγοντες. Κατά πόσο δηλαδή τα μέτρα αυτά έχουν ικανοποιητικό κόστος σε σχέση με τις απειλές που αντιμετωπίζουν, κατά πόσο είναι σύμφωνα με τους νόμους και το κανονιστικό πλαίσιο που διέπει τη λειτουργία της επιχείρησης και τέλος, κατά πόσο επηρεάζει τη φήμη και την αξιοπιστία της επιχείρησης. Ένα από τα μέτρα αυτά είναι και η διαχείριση των συμβάντων ασφαλείας. Σαν συμβάν ασφαλείας αναφέρεται ένα μεμονωμένο ή μια σειρά απρόσμενων γεγονότων ασφαλείας που έχουν μεγάλη πιθανότητα να διακυβεύσουν τη λειτουργική συνέχειά της και να απειλήσουν την ασφάλεια των πληροφοριών της επιχείρησης [43] . Ένα τέτοιο συμβάν ασφαλείας είναι και η παραβίαση/διαρροή προσωπικών δεδομένων. Στη διαχείριση τέτοιων περιστατικών ασφαλείας, εκτός από την αρμόδια ομάδα πληροφορικής (IT) της επιχείρησης, εμπλέκονται και άλλες ομάδες τόσο από το εσωτερικό της επιχείρησης (νομικό τμήμα, τμήμα ανθρωπίνου δυναμικού, τμήμα μάρκετινγκ), όσο και εξωτερικοί ειδικοί συνεργάτες (δικηγορικά γραφεία, σύμβουλοι ασφαλείας κ.λπ.)[20]. Σύμφωνα με τον NIST [13], η διαχείριση ενός τέτοιου συμβάντος ασφαλείας περιλαμβάνει πέντε στάδια (βασιζόμενα στα υπάρχοντα πρότυπα και μεθοδολογίες αντιμετώπισης περιστατικών ασφαλείας, όπως το πρότυπο ISO). Τα στάδια αυτά είναι: ο σχεδιασμός, η αναγνώριση και η εκτίμηση του αντικτύπου του, η κοινοποίηση, η ανάλυση και η αντίδραση.

[43] ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary (4.2.3 Information Security-Information security incident: 'An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security'


Personal Data Breach handling Procedure
Plan & Preparation
Detection of event
Within 24h from being aware of the breach
- Risk Management
- Technical & organisational measures
- Response plans
Initial assessment
- Determining the event detected is a breach
- Circumstances of the breach
- Severity of the breach (at least indication)
- Identify immediate response measures
Is it a personal data breach?
No
Yes
Preliminary Notification (Authorities)
Is the breach adversely affecting the individual(s)?
Yes
Preliminary Notification (Individuals)
No
Review & Improvement
Is further assessment needed?
Yes
No
Data Breach Inventory
Detailed assessment & collection of evidence
Detailed Notification (Authorities)
Containment & Recovery

Εικόνα 11: Διαχείριση περιστατικών ασφάλειας σύμφωνα με το NIST

Κατά τη διάρκεια του σχεδιασμού έχουν αναγνωριστεί τα περιουσιακά στοιχεία της επιχείρησης (διαδικασίες και δεδομένα), οι ευπάθειές τους και οι επιπτώσεις που μπορεί να επιφέρει η εκμετάλλευση των ευπαθειών αυτών. Έχοντας σαφώς οριστεί τα παραπάνω, μια παραβίαση προσωπικών δεδομένων είναι δυνατό να ανιχνευθεί και να αντιμετωπιστεί έγκαιρα. Η έγκαιρη ανίχνευση τέτοιων περιστατικών γίνεται συνήθως με τη χρήση ειδικών συστημάτων (IDS- intrusion detection systems), μηχανισμών καταχώρησης συμβάντων, τοίχων προστασίας κλπ. Όταν ένα τέτοιο συμβάν ανιχνευθεί, γίνεται η εκτίμηση του αντικτύπου του. Η διαδικασία αυτή είναι και η διαδικασία που εκκινεί τη διαδικασία κοινοποίησης. Σύμφωνα με την αντίστοιχη νομοθεσία της κοινοποίησης, για να κοινοποιηθεί μια παραβίαση προσωπικών δεδομένων είτε προ τις αρμόδιες αρχές, είτε και προς τα υποκείμενα των δεδομένων, θα πρέπει να έχει πιστοποιηθεί σαν περιστατικό ασφαλείας και θα πρέπει επίσης να έχει αξιολογηθεί αν από το περιστατικό αυτό προκύπτουν κίνδυνοι για τα δικαιώματα και τις ελευθερίες των ατόμων[44]. Η αξιολόγηση του κινδύνου είναι μια διαδικασία υποκειμενική. Αρκετοί οργανισμοί έχουν αναπτύξει εργαλεία και οδηγίες που βοηθούν τους υπεύθυνους επεξεργασίας να καθορίσουν το επίπεδο του κινδύνου. Αν δεν υπάρχει πραγματικός κίνδυνος για τα υποκείμενα των δεδομένων, τότε η γνωστοποίηση της παραβίασης σ ’αυτά καθίσταται περιττή. Αντίστοιχα, αν ο κίνδυνος είναι μικρός, η παραβίαση δεν γνωστοποιείται καθόλου.

Για παράδειγμα στις ΗΠΑ, βάσει του νόμου HITECH (Health Information Technology or Economical Clinical Health Act), σχετικού με την ασφάλεια των δεδομένων υγείας, ο οργανισμός NCHICA (North Carolina HealthCare Information and Communication Alliance[45]) ανέπτυξε ένα εργαλείο αξιολόγησης κινδύνου βάσει του οποίου καθορίζεται η υποχρέωση κοινοποίησης μιας παραβίασης δεδομένων υγείας. Το εργαλείο ιεραρχεί τα περιστατικά βάσει μιας διαδικασίας αξιολόγησης ορισμένων χαρακτηριστικών τους, όπως ο τύπος των δεδομένων που παραβιάστηκαν, οι συνθήκες της παραβίασης, τι συνέβη στα δεδομένα αυτά αφού είχαν διαρρεύσει, η μέθοδος παραβίασης κ.α.. Σε κάθε ένα από αυτά τα χαρακτηριστικά αντιστοιχεί ένας αριθμός από το 1 μέχρι το 3 . Το άθροισμα που προκύπτει κυμαίνεται από 6 μέχρι 18 μονάδες. Το χαμηλότερο άθροισμα των 6 μονάδων υποδηλώνει ότι δεν είναι υποχρεωτική περεταίρω ενέργεια, ενώ το υψηλότερο άθροισμα των 18 μονάδων συνιστά είτε την ανάγκη κοινοποίησης της παραβίασης, είτε την ανάγκη λήψης επιπλέον μέτρων. Αντίστοιχα εργαλεία και οδηγίες έχουν αναπτυχθεί και από άλλους οργανισμούς, όπως το Aurora Health Care Breach Notification Assessment of Harm Guidance, HIPPA Collaborative of Wisconsin-HIPPA COW[46] .

Στην Ευρώπη, αντίστοιχη μεθοδολογία εκτίμησης του κινδύνου μιας παραβίασης προσωπικών δεδομένων, έχει αναπτυχθεί από τον ENISA (European Union Agency for Cybersecurity)σε συνεργασία με τις αρχές προστασίας δεδομένων της Ελλάδας και της Γερμανίας. Η σοβαρότητα μιας παραβίασης δεδομένων, όπως αυτή ορίζεται στην οδηγία 2009/136/ΕΚ, είναι η εκτίμηση του μεγέθους του πιθανού αντικτύπου που μπορεί να έχει αυτή. Με την προτεινόμενη μεθοδολογία, οι υπεύθυνοι επεξεργασίας αλλά και οι εποπτικές αρχές μπορούν να κάνουν μια καθολική εκτίμηση μιας παραβίασης στηριζόμενοι σε ορισμένα ποσοτικά μετρήσιμα κριτήρια [23] , όπως είναι:

[44] GDPR άρθρο 33

[45] www.nchica.com

[46] https://assets.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2012/304handout5.pdf

- Το γενικό πλαίσιο των δεδομένων και της επεξεργασίας τους (DPC). Για τη μέτρηση του κριτηρίου αυτού λαμβάνονται υπόψη ο τύπος των δεδομένων που παραβιάστηκαν (απλά, συμπεριφοριστικά, οικονομικά, ευαίσθητα) καθώς και η ύπαρξη κάποιων παραγόντων που σχετίζονται με την επεξεργασία των παραπάνω δεδομένων, όπως το πλήθος, η φύση τους, η εγκυρότητά τους, αν αυτά ήταν δημόσια διαθέσιμα, παράγοντες οι οποίοι μπορούν να καθορίσουν την τελική βαθμολογία του κριτηρίου αυτού.
- Η ευκολία αναγνώρισης των προσώπων βάσει των δεδομένων που παραβιάστηκαν (EI). Για το κριτήριο αυτό ορίζονται 4 επίπεδα – αμελητέα, περιορισμένη, σημαντική και μέγιστη. Στο χαμηλότερο επίπεδο η πιθανότητα αναγνώρισης των υποκειμένων είναι αμελητέα, αλλά μπορεί να επιτευχθεί υπό ορισμένες συνθήκες. Στο υψηλότερο επίπεδο η ταυτότητα των υποκειμένων μπορεί να αποκαλυφθεί από τα δεδομένα χωρίς ειδική επεξεργασία. Η αποκάλυψη της ταυτότητας των υποκειμένων μπορεί να είναι άμεση ή έμμεση και εξαρτάται κάθε φορά από το γενικότερο πλαίσιο της παραβίασης.
- Οι συνθήκες της παραβίασης (CB). Στο κριτήριο αυτό λαμβάνεται υπόψη η πρόθεση της παραβίασης σε συνδυασμό με το είδος της. Εξετάζεται αν η παραβίαση οφείλεται σε λάθος ανθρώπινο ή τεχνικό, ακούσια ή εκούσια και αν η παραβίαση αυτή οδήγησε σε απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων.

Τα παραπάνω κριτήρια μετρούνται και συνδυάζονται σύμφωνα με τον τύπο: SE=DPC*EI+CB. Η τελική βαθμολογία δείχνει το επίπεδο της σοβαρότητας μιας παραβίασης δεδομένων, λαμβάνοντας υπόψη το αντίκτυπο στα επηρεαζόμενα άτομα. Το DPC είναι η βάση του υπολογισμού, καθώς καθορίζει τη σημαντικότητα των δεδομένων. Το EI είναι ο διορθωτικός παράγοντας για το DPC. Όσο πιο χαμηλά είναι η βαθμολογία, τόσο πιο εύκολη είναι η αναγνώριση των υποκειμένων, επομένως πιο χαμηλή και η συνολική βαθμολογία. Το CB ποσοτικοποιεί τις ειδικές συνθήκες της παραβίασης και προστίθεται με τη σειρά του στον γενικό τύπο. Το αποτέλεσμα του παραπάνω τύπου ανήκει σε μια κλίμακα που αντιστοιχεί σε ένα από τα 4 επίπεδα σοβαρότητας (Εικόνα 12).

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Εικόνα 12: Κατηγοριοποίηση περιστατικών παραβίασης δεδομένων ανάλογα με τον κίνδυνο. Πηγή: ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches Working Document, v1.0, December 2013

Αυτό, σε συνδυασμό και με ορισμένα επιπλέον κριτήρια, όπως ο αριθμός των ατόμων που επηρεάστηκαν, το αν τα δεδομένα είναι κρυπτογραφημένα ή όχι, μπορεί να χρησιμοποιηθεί ώστε να καθοριστεί η ανάγκη ενημέρωσης των αρχών αλλά και των υποκειμένων.

Τα παραπάνω εργαλεία δρουν επικουρικά. Βοηθούν τους υπεύθυνους επεξεργασίας των δεδομένων, αλλά και τις εποπτικές αρχές να λάβουν την απόφαση της κοινοποίησης μιας παραβίασης προσωπικών δεδομένων, χωρίς να λαμβάνουν την απόφαση για αυτούς. Υπάρχει μια πληθώρα παραγόντων σε μια παραβίαση που δεν μπορούν τα εργαλεία αυτά να προβλέψουν. Στόχος των εργαλείων αυτών είναι να παρέχουν μια ποσοτικοποιημένη μέτρηση του κινδύνου μιας παραβίασης δεδομένων, υποστηρίζοντας το έργο των διάφορων εποπτικών αρχών και υπεύθυνων επεξεργασίας, αποτελώντας ένα ενιαίο εργαλείο στη διάθεσή τους. Η κοινή αυτή μεθοδολογία είναι ιδιαίτερα σημαντική σε περιπτώσεις διασυνοριακών παραβιάσεων. Βοηθούν, τέλος, τις παραπάνω αρχές στην καταγραφή όλων των συνισταμένων μιας παραβίασης.

Ανεξάρτητα με το αν μια παραβίαση πρέπει να γνωστοποιηθεί στην εποπτική αρχή, η συλλογιστική κάθε υπεύθυνου επεξεργασίας για τις αποφάσεις που έλαβε σχετικά με την παραβίαση, πρέπει να τεκμηριώνονται. Αυτό ορίζεται επίσης από τους νόμους και τους

αντίστοιχους κανονισμούς. Για τον ΓΚΠΔ[47], και σύμφωνα με την αρχή της λογοδοσίας[48] , η απόφαση γνωστοποίησης ή όχι της παραβίασης πρέπει να τεκμηριώνεται. Η διατήρηση ενός τέτοιου καταλόγου υπάρχει σαν βήμα στη διαχείριση ενός περιστατικού παραβίασης δεδομένων, στη φάση της αξιολόγησης και ενίσχυσης, σαν στοιχείο της Δράσης, στη διαχείριση της ασφάλειας πληροφοριών κατά ISO. Στόχος κάθε πολιτικής διαχείρισης παραβιάσεων είναι η διασφάλιση ενός δίαυλου ενημέρωσης, σε σχέση με τα περιστατικά και τις ενέργειες που πραγματοποιούνται για την ανίχνευση και την αντιμετώπισή του, ώστε να μπορούν στο μέλλον τέτοιες παραβιάσεις να εντοπίζονται και να αντιμετωπίζονται έγκαιρα, αλλά και να υπάρχει χώρος για βελτίωση των διαδικασιών. Επίσης, οι εποπτικές αρχές μέσω της καταγραφής αυτής επιβλέπουν τα μέτρα που έχουν ληφθεί από τους υπεύθυνους και εξασφαλίζουν έτσι τη συμμόρφωση με τους νόμους.

[47] GDPR, άρθρο 33, παρ.5
[48] GDPR, άρθρο 5, παρ.2

5. ΠΑΡΑΤΗΡΗΣΕΙΣ

5.1 ΚΟΣΤΟΣ ΜΙΑΣ ΚΟΙΝΟΠΟΙΗΣΗΣ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Οι διαρροές προσωπικών δεδομένων είναι οι πιο επιζήμιες για τις επιχειρήσεις από οποιοδήποτε άλλο περιστατικό ασφαλείας. Σύμφωνα με την ετήσια έκθεση του ινστιτούτου Ponemon και της IBM για το 2021 [14], περίπου τα μισά περιστατικά διαρροής δεδομένων (44%) αφορούσαν προσωπικά δεδομένα, με το κόστος για κάθε record δεδομένων που διέρρευσε να ανέρχεται στα 180$ όταν η μέση αξία κάθε record δεδομένων ανέρχεται στα 161$. Σύμφωνα με την ίδια μελέτη, το κόστος μιας διαρροής δεδομένων, υπολογίζεται βάσει τεσσάρων κέντρων κόστους:

- Τα κόστη ανίχνευσης και κλιμάκωσης. Σε αυτά περιλαμβάνονται κόστη που αφορούν ενέργειες ανίχνευσης, εκτίμησης και παρακολούθησης περιστατικών ασφαλείας, καθώς και κόστη που έχουν να κάνουν με τη συγκρότηση αντίστοιχης ομάδας διαχείρισης και επικοινωνίας της με τα υπόλοιπα μέρη της επιχείρησης.
- Το κόστος κοινοποίησης, το οποίο περιλαμβάνει το κόστος για την επικοινωνία με τα υποκείμενα των δεδομένων και τους υπόλοιπους εξωτερικούς συνδέσμους και εποπτικά όργανα, καθώς και το κόστος συμμόρφωσης με τους αντίστοιχους νόμους.
- Το κόστος των ενεργειών που γίνονται μετά την κοινοποίηση της παραβίασης, όπως είναι ενέργειες αποκατάστασης και νομικά έξοδα.
- Τα λειτουργικά κόστη, όπως το κόστος της απώλειας των πελατών ή της προσέλκυσης νέων και τα κόστη από την απώλεια της καλής φήμης [15].

Η κοινοποίηση μιας παραβίασης προσωπικών δεδομένων έχει τόσο άμεσα κόστη για τις επιχειρήσεις και τα υποκείμενα των δεδομένων-πελατών τους, όσο και έμμεσα. Τα άμεσα κόστη αφορούν την ίδια τη διαδικασία της κοινοποίησης και βαραίνουν κυρίως τις ίδιες τις επιχειρήσεις. Οι τρόποι κοινοποίησης μιας παραβίασης τόσο προς τα υποκείμενα των δεδομένων που παραβιάστηκαν, όσο και προς τα τρίτα μέρη, όπως εποπτικοί φορείς, νομικά και συμβουλευτικά γραφεία, στους οποίους περιλαμβάνονται e-mails, αλληλογραφία, τηλεφωνικές κλήσεις, ενημέρωση στον τύπο ή τα μέσα κοινωνικής δικτύωσης, ανεβάζουν το κόστος για μια επιχείρηση. Ο τρόπος κοινοποίησης της παραβίασης έχει μεγάλη σημασία και κάποιες φορές επιβάλλεται από τα αντίστοιχα νομικά πλαίσια. Για παράδειγμα, στην Καλιφόρνια, ο νόμος απαιτεί γραπτή ή ηλεκτρονική ενημέρωση, αλλά επιτρέπει «εναλλακτικούς» τρόπους ενημέρωσης όταν το κόστος της πρώτης υπερβαίνει τα 250.000$ ή τα υποκείμενα των δεδομένων είναι περισσότερα από 500.000. Τέτοιοι εναλλακτικοί τρόποι κοινοποίησης περιλαμβάνουν emails, ενημέρωση στο διαδίκτυο ή σε μεγάλους τηλεοπτικούς σταθμούς, οι οποίοι περιορίζουν το απαιτούμενο κόστος[49]. Η διαδικασία της ενημέρωσης των υποκειμένων απαιτεί περισσότερο χρόνο όταν η παραβίαση είναι περισσότερο σημαντική, καθώς τα υποκείμενα απαιτούν από τις επιχειρήσεις περισσότερες πληροφορίες. Στο κόστος της κοινοποίησης στην περίπτωση αυτή έρχονται να προστεθούν τα κόστη για την έρευνα και την υιοθέτηση πρόσθετων μέτρων εξυπηρέτησης των πελατών για την αντιμετώπιση της παραβίασης αυτής. Τέτοια είναι η πλήρης και λεπτομερής καταγραφή των δεδομένων που παραβιάστηκαν, πληροφορίες για τον τρόπο παραβίασης, πιθανά ρίσκα για τα

[49] California Security Breach Information Act, 2002

υποκείμενα από τη διαρροή των δεδομένων τους καθώς και πιθανές ενέργειες από μέρους τους, που μπορούν να μετριάσουν τα ρίσκα αυτά. Η διατήρηση τέτοιων στοιχείων για κάθε παραβίαση δεδομένων, όπως αυτό επιβάλλεται εξάλλου από αρκετές νομοθεσίες κοινοποίησης[50] ανεβάζει σημαντικά το λειτουργικό κόστος μιας επιχείρησης [24], [25].

Τα έμμεσα κόστη, αφορούν τα κόστη που ακολουθούν μια διαδικασία κοινοποίησης παραβίασης προσωπικών δεδομένων. Αυτά αφορούν τόσο τις επιχειρήσεις, όσο και τα υποκείμενα των δεδομένων. Για τους οργανισμούς, ένα βασικό κόστος που δεν είναι μόνο οικονομικό, είναι η απώλεια της καλής φήμης της επιχείρησης και της εμπιστοσύνης των πελατών της. Σύμφωνα με τον Campbell [16], οι παραβιάσεις δεδομένων προσωπικού χαρακτήρα είναι περισσότερο επιζήμιες στην αξία της μετοχής μιας επιχείρησης από τις υπόλοιπες παραβιάσεις. Οι Cavusoglu, Mishra & Raghunathan [17], αναφέρουν ότι παραβιάσεις δεδομένων οδηγούν σε απώλεια του 2,1% της εμπορικής αξίας της επιχείρησης, μόλις μέσα σε δύο ημέρες από την κοινοποίησή τους. Η ίδια η κοινοποίηση μιας παραβίασης δεδομένων, οδηγεί τους πελάτες στο να χάσουν την εμπιστοσύνη τους στις επιχειρήσεις που διαχειρίζονται τα προσωπικά τους δεδομένα και πολύ πιθανό και στην επιλογή να σταματήσουν τις συναλλαγές μαζί τους ή στη δυσφήμισή τους, γεγονός που επιφέρει μακροπρόθεσμα σημαντικά κόστη στις επιχειρήσεις αυτές και στη λειτουργία τους. Αυτό συμβαίνει ειδικότερα όταν παραβιάσεις δεδομένων κοινοποιούνται πολύ συχνά, είτε λόγω ελλιπών διαδικασιών αξιολόγησης των κινδύνων, είτε σε λανθασμένων πολιτικών επιχειρήσεων με σκοπό να εξασφαλίσουν τη συμμόρφωση με τους νόμους της κοινοποίησης. Οι πελάτες στις περιπτώσεις αυτές ενδέχεται να κουραστούν. Επέρχεται αυτό που ορίζεται από αρκετούς, ως «κούραση κοινοποίησης» (notification fatigue), τόσο στα υποκείμενα των δεδομένων, όσο και στις επιχειρήσεις[15]. Η κούραση αυτή μπορεί να οδηγήσει και τα υποκείμενα των δεδομένων στην αδιαφορία και κατ' επέκταση στη δυσαρέσκεια απέναντι στις επιχειρήσεις, πλήττοντας έτσι το κύρος και τη φήμη τους.

Ένα επιπλέον κόστος για τις επιχειρήσεις, είναι και το κόστος συμμόρφωσης με τις νομοθεσίες τις σχετικές με την κοινοποίηση τέτοιων παραβιάσεων. Η εφαρμογή οργανωτικών και τεχνολογικών μέτρων που εξασφαλίζουν την εμπιστευτικότητα και την ασφάλεια της επεξεργασίας προσωπικών δεδομένων είναι μια απαίτηση που ορίζεται ρητά τόσο από τον GDPR (άρθρο 32), όσο και από την οδηγία προστασίας δεδομένων(Data Protection Directive)(άρθρα 16-17). Ωστόσο η ύπαρξη μιας παραβίασης και η κοινοποίησή της μπορεί να οδηγήσει μια επιχείρηση στη λήψη υπερβολικών μέτρων για την προστασία της. Περισσότερα μέτρα έχουν σαν αποτέλεσμα και την αύξηση του κόστους. Αντίστοιχα, μια παραβίαση που δεν γνωστοποιείται ή μια παραβίαση που καθυστερεί να γνωστοποιηθεί, είτε λόγω αστοχίας στις διαδικασίες κοινοποίησης, είτε λόγω πολιτικής της επιχείρησης, επιφέρει και αυτή κόστη στις επιχειρήσεις. Τα κόστη αυτά αφορούν ποινές και πρόστιμα μη συμμόρφωσης με τους νόμους για την επεξεργασία των προσωπικών δεδομένων. Οι ποινές αυτές ίσως είναι και το κυριότερο κίνητρο για τις επιχειρήσεις για την έγκαιρη και σωστή κοινοποίηση παραβιάσεων προσωπικών δεδομένων. Σύμφωνα με τον GDPR, σε περίπτωση μη συμμόρφωσης με τον κανονισμό, επιβάλλεται στους υπεύθυνους επεξεργασίας, στις επιχειρήσεις πρόστιμο ύψους 10.000.000 ευρώ ή το 2% των ετήσιων εσόδων της, όπως αναφέρθηκε παραπάνω[51]. Νομικά κόστη όμως μπορεί να

50

[51] GDPR Άρθρο 8, παρ.4

προκύψουν και σε περίπτωση έγκαιρης κοινοποίησης, που επιβάλλονται στις επιχειρήσεις εξαιτίας μηνύσεων που υποβάλλονται από τα υποκείμενα των δεδομένων που παραβιάστηκαν.

Τα έμμεσα κόστη μιας κοινοποίησης, που αφορούν τα υποκείμενα των δεδομένων, έχουν να κάνουν αρχικά με την αντίδρασή τους στην κοινοποίηση. Ο χρόνος και το χρήμα που ξοδεύουν για την ανάλυση της παραβίασης και τον περιορισμό της ζημιάς της συμπεριλαμβάνονται στο συνολικό κόστος που ακολουθεί μια διαδικασία κοινοποίησης παραβίασης. Αυτό μπορεί να μοιάζει αμελητέο για ένα record, αλλά για διαρροές εκατοντάδων χιλιάδων records, ο αριθμός αυτός αυξάνει σημαντικά[52] και επιπλέον πάνω από 70% των κλοπών ταυτότητας συμβαίνει σε offline δραστηριότητες.

5.2 ΕΞΑΙΡΕΣΕΙΣ ΣΤΗΝ ΥΠΟΧΡΕΩΣΗ ΚΟΙΝΟΠΟΙΗΣΗΣ -Η ΠΡΟΒΛΗΜΑΤΙΚΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Ένα βασικό ζητούμενο για την υποχρεωτικότητα της κοινοποίησης μιας παραβίασης προσωπικών δεδομένων αποτελεί ο περιορισμός της υποχρέωσης αυτής. Όπως αναφέρθηκε προηγούμενα, οι συνέπειες μιας κοινοποίησης, οικονομικές, ηθικές, νομικές, είναι τέτοιες ώστε είναι ζητούμενο από επιχειρήσεις και οργανισμούς, η υποχρέωση της κοινοποίησης να περιορίζεται σε όσο πιο σοβαρές παραβάσεις. Η έννοια της κρυπτογράφησης υπεισέρχεται στον καθορισμό της σοβαρότητας μιας παραβίασης και κατ' επέκταση στο κατά πόσο η παραβίαση αυτή θα πρέπει να κοινοποιηθεί ή όχι. Αρκετοί νόμοι και οδηγίες συμπεριλαμβάνουν την κρυπτογράφηση σαν ένα από τα μέτρα προστασίας των δεδομένων, αλλά και σαν μέσο περιορισμού της κοινοποίησης μιας παραβίασής τους.

Η κρυπτογράφηση είναι η διαδικασία κατά την οποία δεδομένα μετατρέπονται σε μια μορφή, με τη βοήθεια κάποιου αλγόριθμου κρυπτογράφησης- το κλειδί-, ακατάληπτη σε κάποιον που δεν διαθέτει το αντίστοιχο κλειδί για να τα μετατρέψει στην αρχική τους μορφή. Η διαδικασία αυτή ελαχιστοποιεί τον κίνδυνο παραβίασης των δεδομένων στα οποία εφαρμόζεται, που δεν κατέχουν το αντίστοιχο κλειδί αποκρυπτογράφησης.

Σύμφωνα με τον ΓΚΠΔ, η κρυπτογράφηση, μαζί με την ψευδοανωνυμοποίηση, αναγνωρίζεται σαν ένα βασικό τεχνικό κομμάτι της προστασίας των προσωπικών δεδομένων [7]. Συγκεκριμένα, απαιτεί από τις επιχειρήσεις και τους οργανισμούς να ενσωματώνουν την κρυπτογράφηση ή κάτι αντίστοιχο, στην πολίτική ασφάλειάς τους ώστε να προστατεύονται τα δεδομένα και να ελαχιστοποιείται το ρίσκο της επεξεργασίας τους. Ο GDPR εσκεμμένα δεν ορίζει κάποια συγκεκριμένα τεχνικά και οργανωτικά μέτρα για κάθε περίπτωση, αλλά παρέχει στον υπεύθυνο επεξεργασίας έναν κατάλογο κριτηρίων που πρέπει να ληφθούν υπόψη κατά την επιλογή τέτοιων μέτρων προστασίας. Αυτά περιλαμβάνουν τις τελευταίες τεχνολογικές εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας[53]. Παρ'ολ'αυτά, δεν αναφέρει συγκεκριμένη και ενδεδειγμένη μεθοδολογία

[52] Match ADO- Javellin report: Ο μέσος χρόνος ανίχνευσης μιας απάτης από έλεγχο έγχαρτων αποδεικτικών είναι 114 μέρες με κόστος 4.543$ ενώ οι αντίστοιχοι αριθμοί για ηλεκτρονικούς λογαριασμούς είναι 18 μέρες και 551$.
[53] GDPR, 2016/679: Άρθρο 32, παρ. 1

κρυπτογράφησης. Κατά την επιλογή του λογισμικού κρυπτογράφησης, οι υπεύθυνοι θα πρέπει να σταθμίζουν προσεκτικά την ποιότητα και την ορθή εφαρμογή της μεθόδου κρυπτογράφησης και να κατανοούν το επίπεδο προστασίας που παρέχει το λογισμικό και πόσο κατάλληλο είναι για τους κινδύνου που παρουσιάζονται[54].

Αντίστοιχες προτάσεις υπάρχουν και σε νόμους για την προστασία των προσωπικών δεδομένων πέραν του GDPR. Συγκεκριμένα, σύμφωνα με τον νόμο HIPAA, η κρυπτογράφηση δεδομένων υγείας ορίζεται σαν συγκεκριμένος τρόπος προστασίας των δεδομένων αυτών και καθορίζεται βάσει συγκεκριμένων προτύπων που έχουν οριστεί από τον NIST (HIPAA security rule)[55]. Στην Καλιφόρνια προτείνεται στις επιχειρήσεις και τους οργανισμούς η χρήση μεθόδων προστασίας των προσωπικών δεδομένων που επεξεργάζονται χωρίς ωστόσο να αναφέρεται συγκεκριμένα η κρυπτογράφηση σαν μία από αυτές[56].

Παρ'όλ'αυτά, η καταλληλότητα της μεθόδου προστασίας αποτελεί σημαντικό παράγοντα καθορισμού για τα παραπάνω νομοθετήματα, μιας παραβίασης προσωπικών δεδομένων ως περιστατικό ασφαλείας και κατ' επέκταση την κοινοποίηση αυτής στα υποκείμενα των δεδομένων ή/και στα αρμόδια εποπτικά όργανα. Αρκετοί νόμοι σε πολλές πολιτείες της Αμερικής δεν απαιτούν την κοινοποίηση διαρροών προσωπικών δεδομένων που έχουν κρυπτογραφηθεί, εξαιρώντας την κρυπτογράφηση των προσωπικών δεδομένων από τον ορισμό της παραβίασης που χρειάζεται κοινοποίηση. Σε άλλες πάλι, όπως η Νέα Υόρκη, στον ορισμό της παραβίασης δεδομένων συμπεριλαμβάνονται τα προσωπικά δεδομένα που έχουν κρυπτογραφηθεί μόνο στην περίπτωση που έχει διαρρεύσει και το κλειδί της κρυπτογράφησης[57]. Άλλες απαιτούν συγκεκριμένες μεθόδους κρυπτογράφησης, για παράδειγμα με αλγόριθμο 128-bit ή παραπάνω ή μια γενικά αποδεκτής μεθόδου κρυπτογράφησης βασισμένης σε πρότυπα όπως NIST και FIPS[58][8]. Σύμφωνα με τον GDPR από την άλλη, κάθε παραβίαση προσωπικών δεδομένων αποτελεί περιστατικό ασφαλείας και κατ' επέκταση πρέπει να κοινοποιηθεί στις αρμόδιες αρχές. Η κρυπτογράφηση σαν μέθοδος προστασίας των δεδομένων καθορίζει την κοινοποίηση ή όχι της παραβίασης στα υποκείμενα των δεδομένων. Σύμφωνα με το άρθρο 34, η ανακοίνωση μιας παραβίασης προσωπικών δεδομένων στα υποκείμενα αυτών δεν είναι υποχρεωτική, εφόσον τα δεδομένα έχουν καταστεί ακατάληπτα για αυτόν που τα έχει υποκλέψει μέσω διαδικασίας όπως η κρυπτογράφηση[59] και εφόσον δεν έχει παραβιαστεί ή διαρρεύσει το κλειδί της κρυπτογράφησης.

---

[54] Αιτιολογική Σκέψη 83

[55] HIPAA Security Rule, 45 CFR 164.304 (definition of encryption) "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key"

[56] California Civil Code Section 1798.81.5, "an organization that processes a California resident's personal data is obligated to implement and maintain reasonable security procedures and practices appropriate to the nature of the information it processes."

[57] N.Y. Gen. Bus. Law § 899-aa (Westlaw through L. 2019, ch. 1 to 19) (effective Mar. 28, 2013)

[58] Mass. Gen. Laws Ann. ch. 93H, § 1(a) (Westlaw 2018) (effective Oct. 31, 2007),11 R.I. Gen. Laws Ann. § 11-49.3-3(a)(2) (Westlaw 2018) (effective July 2, 2016), Cal. Civ. Code § 1798.82(i)(4) (Westlaw 2019), effective Jan. 1, 2017), Colo. Rev. Stat. Ann. § 6-1-716(1)(d) (Westlaw 2018) (effective Sept. 1, 2018), Me. Rev. Stat. Ann. tit. 10 § 1347(2) (2017) (effective Sept. 12, 2009), Tenn. Code Ann. § 47-18-2107(a)(2) (Westlaw 2018) (effective Apr. 4, 2017)

[59] GDPR, Άρθρο 34 Παρ.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

Το αν η κρυπτογράφηση μπορεί να αποτελέσει «λιμένα ασφαλείας» (safe harbor) για την κοινοποίηση διαρροών, εξαρτάται από την καταλληλότητα της μεθόδου κρυπτογράφησης και του βαθμού που η μέθοδος αυτή είναι ικανοποιητική για την προστασία των δεδομένων. Ποιος όμως καθορίζει την καταλληλότητα και το επίπεδο προστασίας που προσφέρει η κάθε μέθοδος κρυπτογράφησης και κατά πόσο αυτή η επιλογή μπορεί να αποτελέσει βασικό κριτήριο για την κοινοποίηση ή μη των παραβιάσεων;

Είναι φανερό ότι το βάρος αυτό πέφτει στους υπεύθυνους επεξεργασίας των προσωπικών δεδομένων. Είναι αυτοί που μέσα στο πλαίσιο της πολιτικής ασφάλειας μιας επιχείρησης και σε συνεργασία με τους αρμόδιους για την εφαρμογή της πρέπει να επιλέξουν την κατάλληλη μέθοδο, βασιζόμενοι στις οδηγίες και τις κατευθύνσεις των αντίστοιχων νόμων ή κανόνων ή να δικαιολογήσουν τη μη χρήση καμίας από αυτές. Θα πρέπει επίσης να ορίσουν και τους τρόπους προστασίας του κλειδιού της κρυπτογράφησης, το οποίο όπως προτείνεται από αρκετές οδηγίες θα πρέπει να φυλάσσεται σε διαφορετικό χώρο από τα δεδομένα της κρυπτογράφησης. Η κρυπτογράφηση είναι καλή μόνο αν το κλειδί της είναι προστατευμένο.

Σύμφωνα με τον GDPR, ακόμα και στην περίπτωση που τα δεδομένα που παραβιάστηκαν έχουν κωδικοποιηθεί, η απώλεια ή η αλλοίωση των δεδομένων αυτών μπορεί να έχει αρνητικές συνέπειες για τα υποκείμενα, αν ο υπεύθυνος επεξεργασίας δεν διαθέτει επαρκή αριθμό αντιγράφων ασφαλείας. Αντίστοιχα, σε περιπτώσεις που το χρονικό διάστημα ανάκτησης των κρυπτογραφημένων δεδομένων από το αντίγραφο ασφαλείας είναι μεγάλο, η διαθεσιμότητα των δεδομένων αυτών περιορίζεται και η παραβίαση αυτή πρέπει να κοινοποιείται στα υποκείμενα των δεδομένων εξίσου[60]. Ακόμα και αν μια παραβίαση προσωπικών δεδομένων δεν έχει κοινοποιηθεί επειδή το επίπεδο της κρυπτογράφησης των δεδομένων κρίθηκε επαρκές, αυτό δεν είναι κάτι οριστικό. Μια τέτοια παραβίαση πρέπει να επανεξετάζεται και ο κίνδυνός της να αξιολογείται εκ νέου. Η εξέλιξη της τεχνολογίας, η αποκάλυψη κάποιου τρωτού σημείου στο λογισμικό της κρυπτογράφησης, η μετέπειτα ανάκτηση ή παραβίαση του κλειδιού, αλλάζει τα δεδομένα της κοινοποίησης, η οποία πλέον καθίσταται υποχρεωτική.

Οι εξελίξεις της τεχνολογίας καθιστούν τη διαδικασία της κρυπτογράφησης επισφαλή. Επομένως, ακόμα και στην περίπτωση παραβίασης προσωπικών δεδομένων που έχουν κρυπτογραφηθεί, η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα αυτών ενδέχεται να απειληθεί. Για τον λόγο αυτό, η μέθοδος αυτή δεν μπορεί με σιγουριά να θεωρηθεί σαν «λιμένας ασφαλείας» για τις επιχειρήσεις, στην υποχρέωσή τους για κοινοποίηση παραβιάσεων προσωπικών δεδομένων που αυτές επεξεργάζονται.

κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση,

[60] GDPR Άρθρο 32 Παρ.1. γ.

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Το ζήτημα της ασφάλειας των πληροφοριών είναι πολύ σημαντικό, ιδιαίτερα στα σύγχρονα πληροφοριακά συστήματα. Η εξέλιξη της τεχνολογίας, οι σύγχρονες τεχνικές επεξεργασίας και αποθήκευσης, καθιστούν τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών, βασικό τους στόχο. Τα προσωπικά δεδομένα, αποτελούν το κύριο περιουσιακό στοιχείο κάθε πληροφοριακού συστήματος. Η διατήρηση ενός υψηλού επιπέδου ασφάλειάς τους για κάθε οργανισμό και επιχείρηση είναι βασική προτεραιότητα για τις ίδιες τις επιχειρήσεις αλλά και τις κυβερνήσεις. Ένα μέτρο για να επιτευχθεί αυτό είναι και η υιοθέτηση εκ μέρους των κυβερνήσεων κατάλληλων νόμων. Οι νόμοι αυτοί έχουν σαν στόχο αρχικά την οριοθέτηση ενός συγκεκριμένου πλαισίου εφαρμογής και έπειτα την παροχή κινήτρων προς τις επιχειρήσεις για ενίσχυση των μέτρων προστασίας των προσωπικών δεδομένων [21], αλλά και του δικαιώματος στη γνώση για τα υποκείμενα των δεδομένων [22]. Η κοινοποίηση των παραβιάσεων που αφορούν προσωπικά δεδομένα είναι βασικό χαρακτηριστικό των νόμων αυτών. Η κοινοποίηση ενισχύει την έννοια της διαφάνειας και της λογοδοσίας των επιχειρήσεων και αποτελεί κίνητρο για τους υπεύθυνους της ασφάλειας να επενδύουν περισσότερα στην ασφάλεια των δεδομένων που διαχειρίζονται. Επιπλέον, οι αντίστοιχοι νόμοι προωθούν ευρέως αποδεκτά κριτήρια για τον χαρακτηρισμό και την αξιολόγηση των περιστατικών ασφαλείας και των αντίστοιχων διαδικασιών αντιμετώπισής τους, τη διατήρηση ενιαίου καταλόγου παραβιάσεων και τη συνεργασία ανάμεσα στις επιχειρήσεις, τα υποκείμενα των δεδομένων και τους εποπτικούς φορείς και τον διαμοιρασμό των σχετικών ευρημάτων με πιο επίσημο τρόπο[18]. Το ζητούμενο είναι πώς θα επιτευχθεί αυτό. Με βάση τα όσα παρουσιάστηκαν παραπάνω, οι στόχοι της κοινοποίησης μιας παραβίασης προσωπικών δεδομένων, καθορίζονται από τα παρακάτω στοιχεία:

- Από τον σαφή και συγκεκριμένο ορισμό των βασικών στοιχείων της, δηλαδή των προσωπικών δεδομένων και της παραβίασης της ασφάλειας αυτών. Αυτό αποτελεί τη βάση για κάθε διαδικασία, τον καθορισμό των περιουσιακών στοιχείων που προστατεύουν και τους κινδύνους που αυτά διατρέχουν. Νόμοι όπως ο ΓΚΠΔ, παρέχουν έναν ορισμό για τα προσωπικά δεδομένα, ενώ άλλοι, όπως ο νόμος προστασίας προσωπικών δεδομένων στην πολιτεία του Κάνσας των ΗΠΑ, χρησιμοποιούν συγκεκριμένα παραδείγματα προσωπικών δεδομένων. Έτσι γίνεται σαφές στον υπεύθυνο επεξεργασίας της επιχείρησης για το είδος των δεδομένων που διαχειρίζεται και που πρέπει να προστατέψει. Κάτι αντίστοιχο συμβαίνει και για την παραβίαση προσωπικών δεδομένων. Ο ορισμός πρέπει να είναι σαφής ως προς τι συνίσταται παραβίαση, αλλά και ως προς τα ποια προσωπικά δεδομένα επηρεάζει. Εδώ συναντάται η προβληματική της κρυπτογράφησης. Μπορεί να θεωρηθεί η παραβίαση κρυπτογραφημένων προσωπικών δεδομένων περιστατικό ασφαλείας και αν ναι, κάτω από ποιες συνθήκες; Δεν φτάνει τα δεδομένα να είναι κρυπτογραφημένα, αλλά πρέπει να πιστοποιείται η ασφάλεια της κρυπτογράφησης με χρήση σύγχρονων τεχνικών μεθόδων, η διασφάλιση του κλειδιού της κρυπτογράφησης, η ύπαρξη επαρκούς αριθμού αντιγράφων ασφαλείας.
- Από το πότε εκκινείται η διαδικασία της κοινοποίησης. Στο σημείο αυτό, σημαντικό ρόλο παίζει ο ορισμός ενός κατάλληλου ορίου, πάνω από το οποίο η κοινοποίηση απαιτείται. Το όριο αυτό δεν ορίζεται από τον κάθε νόμο κοινοποίησης παραβιάσεων, αλλά υπολογίζεται βάσει διαδικασιών εκτίμησης κινδύνων. Κατά συνέπεια, βασικό ρόλο στο σημείο αυτό έχει η επιλογή και η ορθή χρήση των κατάλληλων εργαλείων αξιολόγησης κινδύνων. Όπως είδαμε πιο πάνω, με λανθασμένη εκτίμηση κινδύνων, η αδυναμία

κοινοποίησης παραβιάσεων προσωπικών δεδομένων μπορεί να οδηγήσει σε απώλεια της φήμης μιας επιχείρησης, πτώση της τιμής της μετοχής της, ακόμα και επιβολή σ ’αυτήν ποινικών και κανονιστικών κυρώσεων λόγω μη συμμόρφωσης με τους αντίστοιχους νόμους. Αντίστοιχα, η άκριτη κοινοποίηση περιστατικών παραβίασης προσωπικών δεδομένων που θα μπορούσαν να μη γνωστοποιηθούν στα υποκείμενα των δεδομένων μπορεί να επιφέρει «κούραση» (notification fatigue). Η κοινοποίηση παραβιάσεων, οι οποίες δεν επιφέρουν σημαντικό ρίσκο για τα υποκείμενα, κλονίζει την εμπιστοσύνη των πελατών και επιφέρει κούραση τόσο στους ίδιους, όσο και στους υπεύθυνους επεξεργασίας και τις εποπτικές αρχές, με αποτέλεσμα αυτοί να προσπερνούν κοινοποιήσεις παραβιάσεων που θα έπρεπε να έχουν διαχειριστεί. Για τον λόγο αυτό πρέπει να οριστούν συγκεκριμένα κριτήρια που καθορίζουν τη σοβαρότητα μιας παραβίασης και να είναι κοινά για τη μεθοδολογία που ακολουθούν. Για παράδειγμα, τέτοια μπορεί να είναι; Ο αριθμός των ανθρώπων που επηρεάστηκαν, η φύση των δεδομένων που παραβιάστηκαν(οικονομικά, υγείας κ.λπ.), η φύση της παραβίασης (εκτενής ή περιορισμένη), και το επίπεδο ασφάλειας (τα δεδομένα ήταν κρυπτογραφημένα) [13].

- Από το ποιος θα λαμβάνει την κοινοποίηση, πότε και τι θα περιλαμβάνει αυτή. Όλες οι παραβιάσεις πρέπει να αναφέρονται σε ένα κοινό σημείο, είτε αυτό είναι η εποπτική αρχή, είτε ο γενικός εισαγγελέας κ.α. Σκοπός αυτού είναι η αποφυγή της μη κοινοποίησης κάποιας σημαντικής παραβίασης, αλλά και η διατήρηση αυτού του δημόσιου καταλόγου παραβιάσεων για την ενίσχυση της διαφάνειας και της λογοδοσίας των επιχειρήσεων. Παρόλο που ένα τέτοιο καθήκον ίσως φαίνεται υπερβολικό για τις εποπτικές αρχές, εντούτοις αποτελεί πλεονέκτημα τόσο για τις ίδιες όσο και για τα υποκείμενα. Παραβιάσεις οι οποίες δύναται να βλάψουν τα υποκείμενα των δεδομένων και τις ελευθερίες του, πρέπει να αναφέρονται σ ‘αυτά. Το αμελλητί που προτείνει ο GDPR, είναι ένας ασαφής χρονικός προσδιορισμός. Ο καθορισμός συγκεκριμένου χρονικού διαστήματος, αποτελεί μια δικλείδα ασφαλείας τόσο για τους υπεύθυνους επεξεργασίας για την έγκαιρη κοινοποίηση των παραβιάσεων για την αποφύγει κυρώσεων, όσο και για τις εποπτικές αρχές για την εναρμόνιση με τους αντίστοιχους νόμους. Το περιεχόμενο μιας κοινοποίησης, ειδικά όταν αυτή απευθύνεται στα υποκείμενα των δεδομένων έχει σημαντικό ρόλο, ειδικά για τη φήμη των επιχειρήσεων και την ίδια την αποτελεσματικότητα της κοινοποίησης και πρέπει να καθορίζεται λαμβάνοντας υπόψη το κόστος μιας τέτοιας κοινοποίησης. Μια κοινοποίηση πρέπει να είναι ξεκάθαρη για το μήνυμα που κουβαλά, να παρέχει επαρκείς πληροφορίες και κίνητρα για τον έλεγχο και την αντιμετώπιση της παραβίασης που παρουσιάζει. Το γεγονός ότι πολλοί νόμοι δεν απαιτούν την ελάχιστη πληροφορία για την παραβίαση, καταδεικνύει την ανεπάρκειά τους και την αδυναμία της κοινοποίησης να καταφέρει να ικανοποιήσει τον στόχο της: την έγκαιρη ενημέρωση των υποκειμένων για την υιοθέτηση κατάλληλων μέτρων για τον περιορισμό των επιπτώσεων της παραβίασης. Ακόμη και για εκείνους όμως που ορίζουν την ελάχιστη πληροφορία που πρέπει να παρέχεται σε μια κοινοποίηση, εκτός από τα συγκεκριμένα στοιχεία όπως η ημερομηνία της παραβίασης ή τα στοιχεία της επικοινωνίας, τα υπόλοιπα μπορούν να παρουσιαστούν ανάλογα με το στυλ που η κοινοποίηση έχει.
- Οι νόμοι που επιβάλλουν την κοινοποίηση σε περιπτώσεις παραβιάσεων δεδομένων με σκοπό την προστασία των ατόμων, πρέπει συνεχώς να ενημερώνονται ώστε να συμβαδίζουν με τις εξελίξεις της εποχής. Οι υπεύθυνοι της επεξεργασίας των δεδομένων και οι αρμόδιοι εποπτικοί φορείς έχουν σημαίνοντα ρόλο στη διαδικασία της

κοινοποίησης. Αυτοί καθορίζουν το σημείο εκείνο πέρα από το οποίο μια παραβίαση πρέπει να κοινοποιηθεί και είναι αυτοί που καταρτίζουν τους καταλόγους των παραβιάσεων. Συνεπώς, αφενός πρέπει να είναι κατάλληλα εκπαιδευμένοι ώστε να ορίζουν σαφώς και με ασφάλεια το πότε ένα περιστατικό ασφαλείας αφορά παραβίαση προσωπικών δεδομένων και πόσο σοβαρό είναι αυτό και αφεταίρου, πρέπει να συγκεντρώνουν και να καταγράφουν όλα τα στοιχεία της παραβίασης και τις ενέργειές τους μετά την ανακάλυψη αυτής. Μόνο έτσι τα μαθήματα αυτά από προηγούμενες περιπτώσεις μπορούν να φανούν χρήσιμα.

Η κοινοποίηση είναι μια διαδικασία σχετικά καινούργια στην κουλτούρα της προστασίας των προσωπικών δεδομένων. Το σίγουρο είναι ότι η υποχρεωτικότητά της πρέπει να δρα υποστηρικτικά, να δίνει κίνητρα για την ενίσχυση της ασφάλειας των προσωπικών δεδομένων και όχι τιμωρητικά για τις επιχειρήσεις και τα άτομα. Η εξέλιξή της σαν μέρος των διάφορων νομοθετικών πράξεων, θα απασχολήσει τη σχετική έρευνα για αρκετό καιρό ακόμα.

7. ΑΝΑΦΟΡΕΣ – ΠΑΡΑΡΤΗΜΑ

1. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (9 April 2014)

2. Risk Based Security, 2020 Year End Report

3. EDPB (2019): First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities

4. DLA Piper GDPR Data Breach Survey (2019)

5 ENISA (2011): “Data Breach Notifications in Europe”

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

7. František Kasl (2020): THE US LESSONS FOR THE EU PERSONAL DATA BREACH NOTIFICATION: PART I – WHAT IS PERSONAL DATA BREACH AND INTRODUCTION OF THE US REGULATORY PERSPECTIVE

8. Mark Verstraete, Tal Zarsky (2009): OPTIMIZING BREACH NOTIFICATION

9. Mohammad Abdu Al-esaiy et al (2011): ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORKS, , International Journal of Computer Science and Mobile Computing, Vol.10 Issue.11, November- 2021, pg. 29-46

10. Cavalli, E., Mattasoglio, A., Pinciroli, F., & Spaggiari, P. (2004). Information security concepts and practices: the case of a provincial multi-specialty hospital. International Journal of Medical Informatics, 73(3), pg. 297-303.

11. Manik Dey, Member, IEEE (2007): Information Security Management - A Practical Approach

12. ΕΦΗΜΕΡΙΔΑ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ Τεύχος Β’ 1622/10.05.2019

13. ENISA (April 2012), Recommendations on technical implementation guidelines of Article 4

14. IBM Security - Cost of a Data Breach Report 2021

15. Narendra Sharma, Ebere A. Oriaku, Ngozi Oriaku (2020): Cost and Effects of Data Breaches, Precautions, and Disclosure Laws

16. Campbell (2003): Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb., and Lei Zhou. “The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market.” Journal of Computer Security 11

17. Mishra & Raghunathan (2004): “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers.” International Journal of Electronic Commerce 9

18. Karyda, Mitrou (2016): Data Breach Notification: Issues and Challenges for Security Management

19. Bisogni, F (2020), Information availability and data breaches Data breach notification laws and their effects.

20. Anshuman Awasthi (2019), How to respond to an information security incident

21. Ranger, S. (2007), Data breach laws make companies serious about security

22. Schwartz, P., & Janger, E. (2007). Notification of Data Security Breaches. 105 Michigan Law Review, pg. 913

23. ENISA (2013), Recommendations for a methodology of the assessment of severity of personal data breaches

24. Fabio Bisogni, Hadi Asghari, Michel J.G. Van Eeten (2017): Estimating the size of the iceberg from itstip an investigation into unreported data breach notifications

25. Thomas M. Lenard, Paul H. Rubin (2014): Much Ado About Notification, Article in “TELECOMMUNICATIONS & TECHNOLOGY”, REGULATION SPRING 2006, pg.44-50

ΠΑΡΑΡΤΗΜΑ 1
ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ