ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

18/EL

WP250rev.01

Κατευθυντήριες γραμμές σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679

Εκδόθηκαν στις 3 Οκτωβρίου 2017

Όπως τελικώς αναθεωρήθηκαν και εκδόθηκαν στις 6 Φεβρουαρίου 2018

Η ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΩΝ ΕΝΑΝΤΙ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

που συστάθηκε με την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995,

έχοντας υπόψη τα άρθρα 29 και 30 της εν λόγω οδηγίας,

έχοντας υπόψη τον εσωτερικό κανονισμό της,

ΕΞΕΔΩΣΕ ΤΙΣ ΠΑΡΟΥΣΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ:

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) θεσπίζει την απαίτηση γνωστοποίησης μιας παραβίασης δεδομένων προσωπικού χαρακτήρα (εφεξής «παραβίαση») στην αρμόδια εθνική εποπτική αρχή[1] (ή, σε περίπτωση διασυνοριακής παραβίασης, στην επικεφαλής αρχή) και, σε ορισμένες περιπτώσεις, την απαίτηση ανακοίνωσης της παραβίασης στα πρόσωπα τα δεδομένα προσωπικού χαρακτήρα των οποίων έχουν επηρεαστεί από την παραβίαση.

Υποχρεώσεις γνωστοποίησης σε περιπτώσεις παραβιάσεων προβλέπονται επί του παρόντος για ορισμένους οργανισμούς, όπως οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών [όπως ορίζονται στην οδηγία 2009/136/ΕΚ και στον κανονισμό (ΕΕ) αριθ. 611/2013][2]. Υπάρχουν επίσης ορισμένα κράτη μέλη της ΕΕ που έχουν ήδη θεσπίσει τη δική τους εθνική υποχρέωση γνωστοποίησης παραβιάσεων. Αυτό μπορεί να περιλαμβάνει την υποχρέωση γνωστοποίησης παραβιάσεων στις οποίες εμπλέκονται κατηγορίες υπευθύνων επεξεργασίας εκτός από παρόχους υπηρεσιών διαθέσιμων στο κοινό ηλεκτρονικών επικοινωνιών (για παράδειγμα, στη Γερμανία και την Ιταλία) ή την υποχρέωση αναφοράς όλων των παραβιάσεων που αφορούν δεδομένα προσωπικού χαρακτήρα (όπως στις Κάτω Χώρες). Άλλα κράτη μέλη ενδέχεται να διαθέτουν σχετικούς κώδικες ορθής πρακτικής (για παράδειγμα η Ιρλανδία[3]). Παρότι αρκετές αρχές προστασίας δεδομένων της ΕΕ ενθαρρύνουν επί του παρόντος τους υπευθύνους επεξεργασίας να αναφέρουν τις παραβιάσεις, η οδηγία 95/46/ΕΚ για την προστασία των δεδομένων[4], την οποία αντικαθιστά ο ΓΚΠΔ, δεν περιέχει ειδική υποχρέωση γνωστοποίησης των παραβιάσεων και, συνεπώς, αυτή η υποχρέωση θα είναι νέα για πολλούς οργανισμούς. Ο ΓΚΠΔ καθιστά υποχρεωτική τη γνωστοποίηση για όλους τους υπευθύνους επεξεργασίας, εκτός εάν η παραβίαση δεν ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των προσώπων[5]. Οι εκτελούντες την επεξεργασία διαδραματίζουν επίσης σημαντικό ρόλο και πρέπει να γνωστοποιούν οποιαδήποτε παραβίαση στον υπεύθυνο επεξεργασίας τους[6].

Η ομάδα εργασίας του άρθρου 29 (ΟΕ29) θεωρεί ότι η νέα απαίτηση γνωστοποίησης έχει διάφορα οφέλη. Κατά τη γνωστοποίηση στην εποπτική αρχή, οι υπεύθυνοι επεξεργασίας μπορούν να λαμβάνουν συμβουλές σχετικά με το εάν τα επηρεαζόμενα πρόσωπα πρέπει να ενημερωθούν. Πράγματι, η εποπτική αρχή μπορεί να δώσει στον υπεύθυνο επεξεργασίας την εντολή να ενημερώσει αυτά τα πρόσωπα σχετικά με την παραβίαση[7]. Η γνωστοποίηση μιας παραβίασης στα ενδιαφερόμενα πρόσωπα επιτρέπει στον υπεύθυνο επεξεργασίας να παράσχει ενημέρωση σχετικά με τους κινδύνους

[1] Βλ. άρθρο 4 σημείο 21) του ΓΚΠΔ.

[2] Βλ. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32009L0136 και https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32013R0611

[3] Βλ. https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Βλ. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046

[5] Δικαιώματα που κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, ο οποίος είναι διαθέσιμος στη διεύθυνση https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:12012P/TXT

[6] Βλ. άρθρο 33 παράγραφος 2. Παρεμφερές είναι το πνεύμα που διέπει το άρθρο 5 του κανονισμού (ΕΕ) αριθ. 611/2013, το οποίο ορίζει ότι ένας πάροχος με τον οποίο συνάπτεται σύμβαση για την παροχή μέρους των υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό (χωρίς να έχει άμεση συμβατική σχέση με τους συνδρομητές) υποχρεούται να ενημερώνει τον συμβατικό πάροχο σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα.

[7] Βλ. άρθρο 34 παράγραφος 4 και άρθρο 58 παράγραφος 2 στοιχείο ε).

που προκύπτουν ως αποτέλεσμα της παραβίασης και τις ενέργειες στις οποίες μπορούν να προβούν αυτά τα πρόσωπα προκειμένου να προστατευθούν από τις πιθανές συνέπειες της παραβίασης. Οποιοδήποτε σχέδιο αντιμετώπισης παραβιάσεων θα πρέπει να εστιάζει στην προστασία των προσώπων και των δεδομένων προσωπικού χαρακτήρα τους. Συνεπώς, η γνωστοποίηση παραβιάσεων θα πρέπει να θεωρείται ένα εργαλείο που βελτιώνει τη συμμόρφωση όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα. Παράλληλα, θα πρέπει να σημειωθεί ότι η μη αναφορά μιας παραβίασης είτε σε ένα πρόσωπο είτε σε μια εποπτική αρχή μπορεί να σημαίνει ότι, δυνάμει του άρθρου 83, είναι πιθανό να επιβληθεί κύρωση στον υπεύθυνο επεξεργασίας.

Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία ενθαρρύνονται να σχεδιάζουν εκ των προτέρων και να εφαρμόζουν διαδικασίες με στόχο τον εντοπισμό και τον έγκαιρο περιορισμό μιας παραβίασης, την αξιολόγηση του κινδύνου για τα πρόσωπα[8] και, στη συνέχεια, τη λήψη απόφασης σχετικά με το αν είναι αναγκαία η ενημέρωση της αρμόδιας εποπτικής αρχής και η ανακοίνωση της παραβίασης στα ενδιαφερόμενα πρόσωπα, όταν είναι αναγκαίο. Η γνωστοποίηση στην εποπτική αρχή θα πρέπει να αποτελεί μέρος αυτού του σχεδίου αντιμετώπισης περιστατικών.

Ο ΓΚΠΔ περιέχει διατάξεις σχετικά με το πότε μια παραβίαση πρέπει να γνωστοποιείται και σε ποιον, καθώς και σχετικά με τις πληροφορίες που θα πρέπει να παρέχονται στο πλαίσιο της γνωστοποίησης. Οι πληροφορίες που απαιτούνται για τη γνωστοποίηση μπορούν να παρέχονται σε στάδια, ωστόσο σε κάθε περίπτωση οι υπεύθυνοι επεξεργασίας θα πρέπει να αναλαμβάνουν εγκαίρως δράση για οποιαδήποτε παραβίαση.

Στη γνωμοδότησή της 03/2014 σχετικά με την παραβίαση προσωπικών δεδομένων[9], η ΟΕ29 παρέσχε καθοδήγηση στους υπευθύνους επεξεργασίας ώστε να τους βοηθήσει να αποφασίζουν εάν πρέπει να ενημερώνουν τα υποκείμενα των δεδομένων σε περίπτωση παραβίασης. Στο πλαίσιο της γνωμοδότησης εξετάστηκε η υποχρέωση των παρόχων ηλεκτρονικών επικοινωνιών σχετικά με την οδηγία 2002/58/ΕΚ και παρασχέθηκαν παραδείγματα από πολλαπλούς τομείς, στο πλαίσιο του τότε σχεδίου του ΓΚΠΔ, ενώ παράλληλα παρουσιάστηκαν ορθές πρακτικές για όλους τους υπευθύνους επεξεργασίας.

Οι παρούσες κατευθυντήριες γραμμές επεξηγούν τις απαιτήσεις του ΓΚΠΔ ως προς τη γνωστοποίηση παραβιάσεων και την ενημέρωση, καθώς και ορισμένες από τις ενέργειες στις οποίες μπορούν να προβαίνουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία ώστε να συμμορφώνονται μ' αυτές τις νέες υποχρεώσεις. Παρέχουν επίσης παραδείγματα για διάφορα είδη παραβιάσεων και διευκρινίζουν ποιος θα πρέπει να ενημερώνεται σε διάφορα σενάρια.

I. Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα δυνάμει του ΓΚΠΔ

Α. Βασικά ζητήματα σχετικά με την ασφάλεια

Μία από τις απαιτήσεις του ΓΚΠΔ είναι ότι, με τη χρησιμοποίηση κατάλληλων τεχνικών και οργανωτικών μέτρων, τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ

[8] Αυτό μπορεί να διασφαλιστεί στο πλαίσιο της υποχρέωσης παρακολούθησης και επανεξέτασης μιας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ), η οποία αφορά τις διαδικασίες επεξεργασίας που ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (άρθρο 35 παράγραφοι 1 και 11).

[9] Βλ. γνωμοδότηση 03/2014 σχετικά με τη γνωστοποίηση παραβίασης προσωπικών δεδομένων http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_el.pdf

άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά[10].

Ως εκ τούτου, ο ΓΚΠΔ απαιτεί τόσο από τους υπευθύνους επεξεργασίας όσο και από τους εκτελούντες την επεξεργασία να θεσπίζουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι του κινδύνου που τίθεται για τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Θα πρέπει να λαμβάνουν υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[11]. Επίσης, ο ΓΚΠΔ απαιτεί να εφαρμόζονται όλα τα κατάλληλα μέτρα τεχνολογικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης δεδομένων προσωπικού χαρακτήρα και την άμεση ενημέρωση της εποπτικής αρχής και του υποκειμένου των δεδομένων[12].

Κατά συνέπεια, βασικό χαρακτηριστικό οποιασδήποτε πολιτικής ασφάλειας δεδομένων είναι να παρέχει τη δυνατότητα, όταν είναι εφικτό, αποτροπής μιας παραβίασης και, αν παρ' ελπίδα αυτή συμβεί, έγκαιρης αντίδρασης.

Β. Σε τι συνίσταται η παραβίαση δεδομένων προσωπικού χαρακτήρα;

1. Ορισμός

Στο πλαίσιο οποιασδήποτε προσπάθειας αντιμετώπισης μιας παραβίασης, ο υπεύθυνος επεξεργασίας θα πρέπει σε πρώτο στάδιο να είναι σε θέση να την αναγνωρίσει. Σύμφωνα με το άρθρο 4 σημείο 12) του ΓΚΠΔ, ως «παραβίαση δεδομένων προσωπικού χαρακτήρα» νοείται:

> «η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία».

Θα πρέπει να είναι απόλυτα σαφές τι σημαίνει «καταστροφή» δεδομένων προσωπικού χαρακτήρα: πρόκειται για την περίπτωση όπου τα δεδομένα παύουν πλέον να υπάρχουν ή παύουν πλέον να υπάρχουν σε μορφή την οποία μπορεί να χρησιμοποιήσει ο υπεύθυνος επεξεργασίας. Ο όρος «φθορά» θα πρέπει επίσης να είναι σχετικά σαφής: πρόκειται για την περίπτωση όπου τα δεδομένα προσωπικού χαρακτήρα έχουν μεταβληθεί, αλλοιωθεί ή δεν είναι πλέον πλήρη. Όσον αφορά την «απώλεια» δεδομένων προσωπικού χαρακτήρα, ο όρος θα πρέπει να ερμηνεύεται ως μια περίπτωση όπου τα δεδομένα μπορεί να εξακολουθούν να υπάρχουν, αλλά ο υπεύθυνος επεξεργασίας έχει χάσει τον έλεγχό τους ή την πρόσβαση σ' αυτά ή δεν τα έχει πλέον στην κατοχή του. Τέλος, η μη εξουσιοδοτημένη ή παράνομη επεξεργασία μπορεί να περιλαμβάνει την αποκάλυψη δεδομένων προσωπικού χαρακτήρα σε (ή την πρόσβαση από) αποδέκτες που δεν είναι εξουσιοδοτημένοι να λαμβάνουν τα δεδομένα (ή να έχουν πρόσβαση σ' αυτά) ή οποιαδήποτε άλλη μορφή επεξεργασίας που παραβιάζει τον ΓΚΠΔ.

Παράδειγμα

[10] Βλ. άρθρο 5 παράγραφος 1 στοιχείο στ) και άρθρο 32.

[11] Άρθρο 32· βλ. επίσης αιτιολογική σκέψη 83.

[12] Βλ. αιτιολογική σκέψη 87.

Ένα παράδειγμα απώλειας δεδομένων προσωπικού χαρακτήρα μπορεί να περιλαμβάνει την περίπτωση απώλειας ή κλοπής μιας συσκευής η οποία περιέχει ένα αντίγραφο βάσης δεδομένων πελάτη του υπευθύνου επεξεργασίας. Ένα άλλο παράδειγμα απώλειας μπορεί να είναι η περίπτωση όπου το μοναδικό αντίγραφο ενός συνόλου δεδομένων προσωπικού χαρακτήρα έχει κρυπτογραφηθεί από λυτρισμικό ή έχει κρυπτογραφηθεί από τον υπεύθυνο επεξεργασίας με τη χρήση κλειδιού που δεν είναι πλέον στην κατοχή του.

Εκείνο που θα πρέπει να αποσαφηνιστεί είναι ότι η παραβίαση είναι ένα είδος περιστατικού ασφάλειας. Ωστόσο, όπως αναφέρεται στο άρθρο 4 σημείο 12), ο ΓΚΠΔ ισχύει μόνο όταν υπάρχει παραβίαση *δεδομένων προσωπικού χαρακτήρα*. Η συνέπεια μιας τέτοιας παραβίασης είναι ότι ο υπεύθυνος επεξεργασίας δεν θα είναι σε θέση να διασφαλίσει τη συμμόρφωση με τις αρχές που αφορούν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, όπως περιγράφονται στο άρθρο 5 του ΓΚΠΔ. Δεδομένου τούτου, επισημαίνεται η διαφορά ενός περιστατικού ασφάλειας από μια παραβίαση δεδομένων προσωπικού χαρακτήρα. Ουσιαστικά, ενώ όλες οι παραβιάσεις δεδομένων προσωπικού χαρακτήρα είναι περιστατικά ασφάλειας, δεν συνιστούν απαραιτήτως όλα τα περιστατικά ασφάλειας παραβιάσεις δεδομένων προσωπικού χαρακτήρα[13].

Οι ενδεχόμενες δυσμενείς συνέπειες μιας παραβίασης στα πρόσωπα εξετάζονται παρακάτω.

2. Είδη παραβιάσεων δεδομένων προσωπικού χαρακτήρα

Στη γνωμοδότησή της 03/2014 σχετικά με τη γνωστοποίηση παραβιάσεων προσωπικών δεδομένων, η ΟΕ29 εξήγησε ότι οι παραβιάσεις μπορούν να κατηγοριοποιηθούν σύμφωνα με τις ακόλουθες τρεις ευρέως γνωστές αρχές ασφάλειας πληροφοριών[14]:

- «Παραβίαση απορρήτου» – όταν υπάρχει μη εξουσιοδοτημένη ή τυχαία αποκάλυψη δεδομένων προσωπικού χαρακτήρα ή μη εξουσιοδοτημένη ή τυχαία πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.
- «Παραβίαση ακεραιότητας» – όταν υπάρχει μη εξουσιοδοτημένη ή τυχαία αλλοίωση δεδομένων προσωπικού χαρακτήρα.
- «Παραβίαση διαθεσιμότητας» – όταν υπάρχει τυχαία ή μη εξουσιοδοτημένη απώλεια πρόσβασης[15] σε δεδομένα προσωπικού χαρακτήρα ή τυχαία ή μη εξουσιοδοτημένη καταστροφή δεδομένων προσωπικού χαρακτήρα.

Θα πρέπει να σημειωθεί επίσης ότι, ανάλογα με τις περιστάσεις, μια παραβίαση μπορεί να αφορά την εμπιστευτικότητα (απόρρητο), την ακεραιότητα και τη διαθεσιμότητα δεδομένων προσωπικού χαρακτήρα ταυτόχρονα, καθώς και οποιονδήποτε συνδυασμό αυτών.

---

[13] Θα πρέπει να σημειωθεί ότι ένα περιστατικό ασφάλειας δεν περιορίζεται σε μοντέλα απειλής όπου γίνεται επίθεση σε έναν οργανισμό από μια εξωτερική πηγή, αλλά περιλαμβάνει και την περίπτωση περιστατικού από εσωτερική επεξεργασία η οποία παραβιάζει τις αρχές ασφάλειας.

[14] Βλ. γνωμοδότηση 03/2014.

[15] Αποτελεί κοινή παραδοχή ότι η «πρόσβαση» αποτελεί θεμελιώδες μέρος της «διαθεσιμότητας». Βλ., για παράδειγμα, το πρότυπο NIST SP800-53rev4, το οποίο ορίζει τη «διαθεσιμότητα» ως εξής: «Εξασφάλιση έγκαιρης και αξιόπιστης πρόσβασης σε πληροφορίες και χρήσης αυτών», διαθέσιμο στη διεύθυνση http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Το πρότυπο CNSSI-4009 αναφέρεται επίσης στην: «Έγκαιρη, αξιόπιστη πρόσβαση σε δεδομένα και υπηρεσίες των πληροφοριών για εξουσιοδοτημένους χρήστες.» Βλ. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Το πρότυπο ISO/IEC 27000:2016 ορίζει επίσης τη «διαθεσιμότητα» ως την «Ιδιότητα προσβασιμότητας και ετοιμότητας προς χρήση κατόπιν αιτήματος εξουσιοδοτημένου φορέα»: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Παρότι το εάν έχει διαπραχθεί παραβίαση της εμπιστευτικότητας ή της ακεραιότητας είναι σχετικά σαφές, το εάν έχει διαπραχθεί παραβίαση της διαθεσιμότητας ενδέχεται να είναι λιγότερο προφανές. Μια παραβίαση θα θεωρείται πάντα ότι συνιστά παραβίαση της διαθεσιμότητας όταν υπάρχει οριστική απώλεια ή καταστροφή δεδομένων προσωπικού χαρακτήρα.

Παράδειγμα

Παραδείγματα απώλειας της διαθεσιμότητας περιλαμβάνουν περιπτώσεις όπου τα δεδομένα έχουν διαγραφεί είτε τυχαία είτε από μη εξουσιοδοτημένο πρόσωπο ή, στην περίπτωση κρυπτογραφημένων με ασφάλεια δεδομένων, το κλειδί αποκρυπτογράφησης έχει χαθεί. Στην περίπτωση που ο υπεύθυνος επεξεργασίας δεν μπορεί να αποκαταστήσει την πρόσβαση στα δεδομένα, για παράδειγμα από αντίγραφο ασφαλείας, το γεγονός αυτό θεωρείται οριστική απώλεια της διαθεσιμότητας.

Απώλεια της διαθεσιμότητας ενδέχεται επίσης να προκύψει όταν διαταράσσεται σε σημαντικό βαθμό η κανονική λειτουργία ενός οργανισμού, για παράδειγμα, διακοπή ρεύματος ή επίθεση «άρνησης υπηρεσίας», με αποτέλεσμα να καθίστανται μη διαθέσιμα τα δεδομένα προσωπικού χαρακτήρα.

Ενδέχεται να τεθεί το ερώτημα κατά πόσο μια προσωρινή απώλεια της διαθεσιμότητας δεδομένων προσωπικού χαρακτήρα θα πρέπει να θεωρείται ότι συνιστά παραβίαση και, εάν ναι, παραβίαση η οποία πρέπει να γνωστοποιηθεί. Στο άρθρο 32 του ΓΚΠΔ («Ασφάλεια επεξεργασίας») επεξηγείται ότι, κατά την εφαρμογή τεχνικών και οργανωτικών μέτρων προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, θα πρέπει να λαμβάνονται υπόψη, μεταξύ άλλων, η δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση και η δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος.

Συνεπώς, ένα περιστατικό ασφάλειας που έχει ως αποτέλεσμα τη μη διαθεσιμότητα δεδομένων προσωπικού χαρακτήρα για ένα χρονικό διάστημα είναι επίσης ένα είδος παραβίασης, δεδομένου ότι η έλλειψη πρόσβασης στα δεδομένα μπορεί να έχει σημαντικό αντίκτυπο στα δικαιώματα και στις ελευθερίες των φυσικών προσώπων. Για λόγους σαφήνειας αναφέρεται ότι, όταν τα δεδομένα προσωπικού χαρακτήρα καθίστανται μη διαθέσιμα λόγω της πραγματοποίησης προγραμματισμένης συντήρησης του συστήματος, αυτό δεν συνιστά «παραβίαση της ασφάλειας», όπως ορίζεται στο άρθρο 4 σημείο 12).

Όπως στην περίπτωση της απώλειας ή της καταστροφής δεδομένων προσωπικού χαρακτήρα (ή, ουσιαστικά, οποιουδήποτε άλλου είδους παραβίασης), μια παραβίαση που αφορά την προσωρινή απώλεια της διαθεσιμότητας θα πρέπει να τεκμηριώνεται σύμφωνα με το άρθρο 33 παράγραφος 5. Αυτό βοηθάει τον υπεύθυνο επεξεργασίας να αποδεικνύει ότι λογοδοτεί στην εποπτική αρχή, η οποία ενδέχεται να ζητήσει να δει αυτά τα αρχεία[16]. Ωστόσο, ανάλογα με τις περιστάσεις της παραβίασης, ενδέχεται να απαιτείται ή να μην απαιτείται γνωστοποίηση στην εποπτική αρχή και ενημέρωση των επηρεαζόμενων προσώπων. Ο υπεύθυνος επεξεργασίας θα πρέπει να αξιολογεί την πιθανότητα και τη σοβαρότητα του αντικτύπου στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων ως αποτέλεσμα της έλλειψης διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με το άρθρο 33, ο υπεύθυνος επεξεργασίας θα πρέπει να προβαίνει σε γνωστοποίηση, εκτός εάν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων. Βεβαίως, αυτό θα πρέπει να αξιολογείται κατά περίπτωση.

Παραδείγματα

[16] Βλ. άρθρο 33 παράγραφος 5.

Σε νοσοκομειακό περιβάλλον, εάν ιατρικά δεδομένα κρίσιμης σημασίας που αφορούν ασθενείς καταστούν μη διαθέσιμα, ακόμη και προσωρινά, αυτό θα μπορούσε να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων. Για παράδειγμα, ενδέχεται να ακυρωθούν επεμβάσεις, με αποτέλεσμα να τεθούν ζωές σε κίνδυνο.

Αντιθέτως, στην περίπτωση που τα συστήματα μιας εταιρείας μέσων ενημέρωσης καταστούν μη διαθέσιμα για αρκετές ώρες (π.χ., λόγω διακοπής ρεύματος), εάν η συγκεκριμένη εταιρεία δεν μπορεί να αποστείλει ενημερωτικά δελτία στους συνδρομητές της, αυτό είναι απίθανο να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων.

Θα πρέπει να σημειωθεί ότι, παρότι η απώλεια της διαθεσιμότητας των συστημάτων μιας εταιρείας μπορεί να είναι μόνο προσωρινή και μπορεί να μην έχει αντίκτυπο στα πρόσωπα, είναι σημαντικό ο υπεύθυνος επεξεργασίας να εξετάζει όλες τις ενδεχόμενες συνέπειες μιας παραβίασης, καθώς μπορεί να απαιτείται γνωστοποίηση για άλλους λόγους.

Παράδειγμα

Τυχόν μόλυνση από λυτρισμικό (κακόβουλο λογισμικό το οποίο κρυπτογραφεί τα δεδομένα του υπευθύνου επεξεργασίας μέχρι να πληρωθούν λύτρα) θα μπορούσε να έχει ως αποτέλεσμα προσωρινή απώλεια της διαθεσιμότητας, εάν τα δεδομένα μπορούν να αποκατασταθούν από αντίγραφο ασφαλείας. Ωστόσο, δεν παύει να έχει σημειωθεί εισβολή στο δίκτυο και θα μπορούσε να απαιτείται γνωστοποίηση εάν το περιστατικό χαρακτηρίζεται ως παραβίαση της εμπιστευτικότητας (δηλ. αυτός που κάνει την επίθεση αποκτά πρόσβαση στα δεδομένα προσωπικού χαρακτήρα) και αυτό επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων.

3. Οι ενδεχόμενες συνέπειες μιας παραβίασης δεδομένων προσωπικού χαρακτήρα

Μια παραβίαση μπορεί δυνητικά να έχει διάφορες σημαντικές δυσμενείς συνέπειες στα πρόσωπα, οι οποίες μπορούν να οδηγήσουν σε σωματική, υλική ή ηθική βλάβη. Στον ΓΚΠΔ επεξηγείται ότι αυτή η βλάβη μπορεί να περιλαμβάνει απώλεια του ελέγχου επί των δεδομένων προσωπικού χαρακτήρα τους, περιορισμό των δικαιωμάτων τους, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, βλάβη της φήμης και απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο. Μπορεί επίσης να περιλαμβάνει οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα γι' αυτά τα πρόσωπα[17].

Κατά συνέπεια, ο ΓΚΠΔ απαιτεί από τον υπεύθυνο επεξεργασίας να γνωστοποιεί μια παραβίαση στην αρμόδια εποπτική αρχή, εκτός εάν η παραβίαση δεν ενδέχεται να δημιουργήσει κίνδυνο τέτοιων δυσμενών επιπτώσεων. Όταν είναι πιθανό να δημιουργηθεί υψηλός κίνδυνος να προκύψουν αυτές οι δυσμενείς συνέπειες, ο ΓΚΠΔ απαιτεί από τον υπεύθυνο επεξεργασίας να ανακοινώσει την παραβίαση στα επηρεαζόμενα πρόσωπα το συντομότερο δυνατόν[18].

Η σημασίας της ικανότητας εντοπισμού μιας παραβίασης με στόχο την αξιολόγηση του κινδύνου για τα πρόσωπα και, στη συνέχεια, η γνωστοποίησή της, εάν απαιτείται, τονίζεται στην αιτιολογική σκέψη 87 του ΓΚΠΔ:

[17] Βλ. επίσης αιτιολογικές σκέψεις 85 και 75.

[18] Βλ. επίσης αιτιολογική σκέψη 86.

«Θα πρέπει να εξακριβώνεται κατά πόσον έχουν τεθεί σε εφαρμογή όλα τα κατάλληλα μέτρα τεχνολογικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης δεδομένων προσωπικού χαρακτήρα και την άμεση ενημέρωση της εποπτικής αρχής και του υποκειμένου των δεδομένων. Θα πρέπει να διαπιστώνεται ότι η κοινοποίηση πραγματοποιήθηκε χωρίς αδικαιολόγητη καθυστέρηση, λαμβανομένων υπόψη ιδίως της φύσης και της σοβαρότητας της παραβίασης δεδομένων προσωπικού χαρακτήρα, καθώς και των συνεπειών και των δυσμενών αποτελεσμάτων της για το υποκείμενο των δεδομένων. Η γνωστοποίηση αυτή μπορεί να οδηγεί σε παρέμβαση της εποπτικής αρχής, σύμφωνα με τα καθήκοντα και τις εξουσίες της που ορίζονται στον παρόντα κανονισμό.»

Περαιτέρω κατευθυντήριες γραμμές για την αξιολόγηση του κινδύνου δυσμενών συνεπειών για τα πρόσωπα εξετάζονται στην ενότητα IV.

Εάν οι υπεύθυνοι επεξεργασίας δεν ενημερώσουν είτε την εποπτική αρχή είτε τα υποκείμενα των δεδομένων, είτε και τις δύο πλευρές, για μια παραβίαση δεδομένων, παρότι πληρούνται οι απαιτήσεις του άρθρου 33 και/ή 34, η επιλογή που έχει η εποπτική αρχή πρέπει να περιλαμβάνει την εξέταση όλων των διορθωτικών μέτρων που έχει στη διάθεσή της, καθώς και του ενδεχομένου επιβολής του κατάλληλου διοικητικού προστίμου[19], το οποίο θα συνδυάζεται με διορθωτικό μέτρο δυνάμει του άρθρου 58 παράγραφος 2 ή θα επιβάλλεται μεμονωμένα. Όταν επιλέγεται η επιβολή διοικητικού προστίμου, η αξία του μπορεί να φτάνει έως 10 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών δυνάμει του άρθρου 83 παράγραφος 4 στοιχείο α) του ΓΚΠΔ. Είναι επίσης σημαντικό να λαμβάνεται υπόψη ότι, σε ορισμένες περιπτώσεις, η μη γνωστοποίηση μιας παραβίασης θα μπορούσε να υποδεικνύει είτε την απουσία υφιστάμενων μέτρων ασφάλειας είτε την ανεπάρκεια των υφιστάμενων μέτρων ασφάλειας. Οι κατευθυντήριες γραμμές της ΟΕ29 για τα διοικητικά πρόστιμα αναφέρουν: «Η σωρευτική τέλεση πολλών διαφορετικών παραβάσεων σε οποιαδήποτε μεμονωμένη περίπτωση σημαίνει ότι η εποπτική αρχή δύναται να επιβάλει τα διοικητικά πρόστιμα σε επίπεδο αποτελεσματικό, αναλογικό και αποτρεπτικό εντός του ορίου της βαρύτερης παράβασης.» Σ' αυτή την περίπτωση, η εποπτική αρχή θα έχει επίσης τη δυνατότητα να επιβάλλει κυρώσεις για μη γνωστοποίηση ή ανακοίνωση της παραβίασης (άρθρα 33 και 34), αφενός, και για απουσία (επαρκών) μέτρων ασφάλειας (άρθρο 32), αφετέρου, δεδομένου ότι πρόκειται για δύο ξεχωριστές παραβιάσεις.

II. **Άρθρο 33 - Γνωστοποίηση στην εποπτική αρχή**

Γ. Πότε πρέπει να γίνεται γνωστοποίηση

1. Οι απαιτήσεις του άρθρου 33

Το άρθρο 33 παράγραφος 1 προβλέπει ότι:

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

[19] Για περισσότερες λεπτομέρειες, βλ. κατευθυντήριες γραμμές της ΟΕ29 για την εφαρμογή και τον καθορισμό διοικητικών προστίμων, οι οποίες είναι διαθέσιμες στη διεύθυνση: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών συνοδεύεται από τους λόγους της καθυστέρησης.»

Στην αιτιολογική σκέψη 87 αναφέρονται τα εξής[20]:

«Θα πρέπει να εξακριβώνεται κατά πόσον έχουν τεθεί σε εφαρμογή όλα τα κατάλληλα μέτρα τεχνολογικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης δεδομένων προσωπικού χαρακτήρα και την άμεση ενημέρωση της εποπτικής αρχής και του υποκειμένου των δεδομένων. Θα πρέπει να διαπιστώνεται ότι η κοινοποίηση πραγματοποιήθηκε χωρίς αδικαιολόγητη καθυστέρηση, λαμβανομένων υπόψη ιδίως της φύσης και της σοβαρότητας της παραβίασης δεδομένων προσωπικού χαρακτήρα, καθώς και των συνεπειών και των δυσμενών αποτελεσμάτων της για το υποκείμενο των δεδομένων. Η γνωστοποίηση αυτή μπορεί να οδηγεί σε παρέμβαση της εποπτικής αρχής, σύμφωνα με τα καθήκοντα και τις εξουσίες της που ορίζονται στον παρόντα κανονισμό.»

2. Πότε ένας υπεύθυνος επεξεργασίας αποκτά «γνώση»;

Όπως αναφέρεται λεπτομερώς παραπάνω, ο ΓΚΠΔ απαιτεί, σε περίπτωση παραβίασης, ο υπεύθυνος επεξεργασίας να γνωστοποιεί την παραβίαση αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος. Αυτό μπορεί να εγείρει το ερώτημα πότε ένας υπεύθυνος επεξεργασίας μπορεί να θεωρείται ότι αποκτά «γνώση» μιας παραβίασης. Η ΟΕ29 θεωρεί ότι ένας υπεύθυνος επεξεργασίας θα πρέπει να θεωρείται ότι έχει αποκτά «γνώση» όταν ο εν λόγω υπεύθυνος επεξεργασίας έχει εύλογο βαθμό βεβαιότητας ότι έχει προκύψει περιστατικό ασφάλειας το οποίο έχει ως αποτέλεσμα να τεθούν σε κίνδυνο τα δεδομένα προσωπικού χαρακτήρα.

Ωστόσο, όπως προαναφέρθηκε, ο ΓΚΠΔ απαιτεί από τον υπεύθυνο επεξεργασίας να εφαρμόζει όλα τα κατάλληλα μέτρα τεχνικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης και την άμεση ενημέρωση της εποπτικής αρχής και των υποκειμένων των δεδομένων. Αναφέρει επίσης ότι θα πρέπει να διαπιστώνεται ότι η γνωστοποίηση πραγματοποιήθηκε χωρίς αδικαιολόγητη καθυστέρηση, λαμβανομένων υπόψη ιδίως της φύσης και της σοβαρότητας της παραβίασης δεδομένων, καθώς και των συνεπειών και των δυσμενών αποτελεσμάτων της για το υποκείμενο των δεδομένων[21]. Κατ' αυτόν τον τρόπο, ο υπεύθυνος επεξεργασίας υπόκειται στην υποχρέωση να εξασφαλίζει ότι θα αποκτά «γνώση» οποιωνδήποτε παραβιάσεων εγκαίρως ώστε να μπορεί να προβεί στις κατάλληλες ενέργειες.

Το ακριβές χρονικό σημείο όπου ένας υπεύθυνος επεξεργασίας μπορεί να θεωρείται ότι αποκτά «γνώση» μιας συγκεκριμένης παραβίασης θα εξαρτάται από τις περιστάσεις της συγκεκριμένης παραβίασης. Σε ορισμένες περιπτώσεις, θα προκύπτει με σχετική σαφήνεια από την αρχή ότι έχει διαπραχθεί παραβίαση, ενώ, σε άλλες, ενδέχεται να χρειάζεται κάποιος χρόνος για να διαπιστωθεί εάν τα δεδομένα προσωπικού χαρακτήρα έχουν τεθεί σε κίνδυνο. Ωστόσο, η έμφαση θα πρέπει να δίνεται στην έγκαιρη ανάληψη δράσης για τη διερεύνηση ενός περιστατικού, ώστε να διαπιστωθεί κατά πόσο τα δεδομένα προσωπικού χαρακτήρα έχουν παραβιαστεί και, σε τέτοια περίπτωση, να λαμβάνονται διορθωτικά μέτρα και να γίνεται γνωστοποίηση, εάν απαιτείται.

Παραδείγματα

1. Στην περίπτωση της απώλειας ενός κλειδιού USB με κρυπτογραφημένα δεδομένα προσωπικού χαρακτήρα, συχνά μπορεί να μην είναι δυνατό να εξακριβωθεί εάν μη εξουσιοδοτημένα πρόσωπα

[20] Η αιτιολογική σκέψη 85 είναι επίσης σημαντική σ' αυτό το πλαίσιο.

[21] Βλ. αιτιολογική σκέψη 87.

έχουν αποκτήσει πρόσβαση σ' αυτά τα δεδομένα. Ωστόσο, ακόμη και αν υποθέσουμε ότι ο υπεύθυνος επεξεργασίας δεν μπορεί να εντοπίσει παραβίαση της εμπιστευτικότητας, η περίπτωση θα πρέπει να γνωστοποιείται καθώς υπάρχει εύλογος βαθμός βεβαιότητας ότι έχει διαπραχθεί παραβίαση διαθεσιμότητας· ο υπεύθυνος επεξεργασίας αποκτά «γνώση» όταν συνειδητοποιήσει ότι το κλειδί USB έχει χαθεί.

2. Ένας τρίτος ενημερώνει έναν υπεύθυνο επεξεργασίας ότι έχει λάβει τυχαία τα δεδομένα προσωπικού χαρακτήρα ενός από τους πελάτες του και παρέχει στοιχεία για τη μη εξουσιοδοτημένη κοινολόγηση. Δεδομένου ότι ο υπεύθυνος επεξεργασίας έχει λάβει σαφή στοιχεία για παραβίαση της εμπιστευτικότητας, δεν μπορεί να υπάρχει αμφιβολία ότι έχει αποκτήσει «γνώση».

3. Ένας υπεύθυνος επεξεργασίας διαπιστώνει ότι ενδέχεται να έχει γίνει εισβολή στο δίκτυό του. Ο υπεύθυνος επεξεργασίας ελέγχει τα συστήματά του για να διαπιστώσει εάν τα δεδομένα προσωπικού χαρακτήρα που τηρούνται σ' αυτά τα συστήματα έχουν τεθεί σε κίνδυνο και επιβεβαιώνει ότι, πράγματι, αυτό συμβαίνει. Για άλλη μία φορά, δεδομένου ότι ο υπεύθυνος επεξεργασίας έχει λάβει σαφή στοιχεία για παραβίαση, δεν μπορεί να υπάρχει αμφιβολία ότι έχει αποκτήσει «γνώση».

4. Ένας κυβερνοεγκληματίας επικοινωνεί με τον υπεύθυνο επεξεργασίας αφού έχει παραβιάσει το σύστημά του με σκοπό να ζητήσει λύτρα. Σ' αυτή την περίπτωση, αφού ελέγξει το σύστημά του για να επιβεβαιώσει ότι έχει δεχτεί επίθεση, ο υπεύθυνος επεξεργασίας έχει σαφή στοιχεία ότι έχει διαπραχθεί παραβίαση και δεν υπάρχει αμφιβολία ότι έχει αποκτήσει γνώση.

Αφού ενημερώθηκε πρώτα για πιθανή παραβίαση από πρόσωπο, έναν οργανισμό μέσων ενημέρωσης ή άλλη πηγή ή όταν έχει εντοπίσει ο ίδιος ένα περιστατικό ασφάλειας, ο υπεύθυνος επεξεργασίας μπορεί να διενεργήσει έρευνα μικρής χρονικής διάρκειας για να διαπιστώσει εάν έχει όντως διαπραχθεί παραβίαση. Κατά τη διάρκεια αυτής της περιόδου έρευνας, ο υπεύθυνος επεξεργασίας δεν μπορεί να θεωρείται ότι έχει αποκτήσει «γνώση». Ωστόσο, αναμένεται ότι η αρχική έρευνα θα πρέπει να ξεκινά το συντομότερο δυνατό και να εξακριβώνεται με εύλογο βαθμό βεβαιότητας εάν έχει σημειωθεί παραβίαση· στη συνέχεια, μπορεί να ακολουθήσει πιο ενδελεχής έρευνα.

Μόλις ο υπεύθυνος επεξεργασίας αποκτήσει γνώση, μια γνωστοποιήσιμη παραβίαση πρέπει να γνωστοποιείται αμελλητί και, ει δυνατόν, το αργότερο εντός 72 ωρών. Κατά τη διάρκεια αυτής της περιόδου, ο υπεύθυνος επεξεργασίας θα πρέπει να αξιολογεί τον πιθανό κίνδυνο για τα πρόσωπα, ώστε να προσδιορίζει εάν έχει ενεργοποιηθεί η απαίτηση για γνωστοποίηση, καθώς και τις ενέργειες που απαιτούνται για την αντιμετώπιση της παραβίασης. Ωστόσο, ένας υπεύθυνος επεξεργασίας μπορεί να διαθέτει ήδη αξιολόγηση του πιθανού κινδύνου που θα μπορούσε να συνεπάγεται μια παραβίαση βάσει μιας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ)[22] που πραγματοποιήθηκε πριν από τη διενέργεια της σχετικής πράξης επεξεργασίας. Ωστόσο, η ΕΑΠΔ μπορεί να είναι πιο γενικευμένη σε σύγκριση με τις ειδικές περιστάσεις οποιασδήποτε πραγματικής παραβίασης και, συνεπώς, σε κάθε περίπτωση θα πρέπει να διενεργείται πρόσθετη αξιολόγηση η οποία θα λαμβάνει υπόψη αυτές τις περιστάσεις. Για περισσότερες λεπτομέρειες σχετικά με την αξιολόγηση κινδύνου, βλ. ενότητα IV.

Στις περισσότερες περιπτώσεις, αυτές οι προκαταρκτικές δράσεις θα πρέπει να ολοκληρώνονται σύντομα μετά την αρχική ειδοποίηση (δηλαδή όταν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει την υποψία ότι έχει προκύψει περιστατικό ασφάλειας το οποίο ενδέχεται να αφορά δεδομένα προσωπικού χαρακτήρα.) – θα πρέπει να διαρκούν περισσότερο μόνο σε εξαιρετικές περιπτώσεις.

[22] Βλ. κατευθυντήριες γραμμές της ΟΕ29 για τις ΕΑΠΔ εδώ: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Παράδειγμα

Ένα πρόσωπο ενημερώνει τον υπεύθυνο επεξεργασίας ότι έχει λάβει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι εστάλη από τον υπεύθυνο επεξεργασίας και που περιέχει δεδομένα προσωπικού χαρακτήρα τα οποία αφορούν την (πραγματική) χρήση, από το εν λόγω πρόσωπο, της υπηρεσίας του υπευθύνου επεξεργασίας, με τον ισχυρισμό ότι η ασφάλεια του υπευθύνου επεξεργασίας έχει τεθεί σε κίνδυνο. Ο υπεύθυνος επεξεργασίας διενεργεί μια έρευνα σύντομης διάρκειας και εντοπίζει εισβολή στο δίκτυό του, καθώς και στοιχεία μη εξουσιοδοτημένης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα. Ο υπεύθυνος επεξεργασίας θεωρείται πλέον ότι έχει αποκτήσει «γνώση», ενώ παράλληλα απαιτείται η γνωστοποίηση στην εποπτική αρχή, εκτός εάν είναι απίθανο η παραβίαση να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων. Ο υπεύθυνος επεξεργασίας θα χρειαστεί να λάβει τα κατάλληλα διορθωτικά μέτρα για να αντιμετωπίσει την παραβίαση.

Ο υπεύθυνος επεξεργασίας θα πρέπει, συνεπώς, να έχει σχεδιάσει εσωτερικές διαδικασίες μέσω των οποίων θα είναι δυνατός ο εντοπισμός και η αντιμετώπιση μιας παραβίασης. Για παράδειγμα, για να εντοπίσει ορισμένες παρατυπίες στην επεξεργασία των δεδομένων, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί να χρησιμοποιεί ορισμένα τεχνικά μέτρα, όπως η ροή δεδομένων και οι αναλυτές αρχείων καταγραφής, με τα οποία είναι δυνατόν να καθοριστούν περιστατικά και ειδοποιήσεις μέσω της συσχέτισης οποιωνδήποτε δεδομένων καταγραφής[23]. Όταν εντοπίζεται μια παραβίαση, είναι σημαντικό να αναφέρεται στο κατάλληλο ανώτερο διοικητικό επίπεδο ώστε να είναι δυνατή η αντιμετώπισή της και, εάν απαιτείται, η γνωστοποίησή της σύμφωνα με το άρθρο 33 και, εάν είναι απαραίτητο, σύμφωνα με το άρθρο 34. Αυτά τα μέτρα και οι μηχανισμοί αναφοράς θα μπορούσαν να περιγράφονται λεπτομερώς στα σχέδια αντιμετώπισης περιστατικών και/ή στις ρυθμίσεις διακυβέρνησης του υπευθύνου επεξεργασίας. Θα βοηθήσουν τον υπεύθυνο επεξεργασίας ώστε να σχεδιάσει αποτελεσματικά και να προσδιορίσει ποιος έχει επιχειρησιακή ευθύνη εντός του οργανισμού για τη διαχείριση μιας παραβίασης, καθώς και το πώς ή το εάν πρέπει να κλιμακώνεται ένα περιστατικό, ανάλογα με την περίπτωση.

Ο υπεύθυνος επεξεργασίας θα πρέπει επίσης να θεσπίζει ρυθμίσεις που θα ισχύουν για τους εκτελούντες την επεξεργασία που χρησιμοποιεί, οι οποίοι έχουν υποχρέωση να ενημερώνουν τον υπεύθυνο επεξεργασίας σε περίπτωση παραβίασης (βλ. παρακάτω).

Παρότι αποτελεί ευθύνη των υπευθύνων επεξεργασίας και των εκτελούντων των επεξεργασία να θεσπίζουν κατάλληλα μέτρα για την αποτροπή μιας παραβίασης, την αντίδραση σ' αυτήν και την αντιμετώπισή της, υπάρχουν ορισμένα πρακτικά βήματα που πρέπει να ακολουθούνται σε όλες τις περιπτώσεις.

- Οι πληροφορίες σχετικά με όλα τα περιστατικά που αφορούν την ασφάλεια θα πρέπει να υποβάλλονται στο αρμόδιο πρόσωπο ή στα αρμόδια πρόσωπα που είναι επιφορτισμένα με την αντιμετώπιση περιστατικών, την εξακρίβωση της ύπαρξης παραβίασης και την αξιολόγηση του κινδύνου.
- Στη συνέχεια, θα πρέπει να αξιολογούνται οι κίνδυνοι για τα πρόσωπα οι οποίοι απορρέουν από την παραβίαση (πιθανότητα μηδενικού κινδύνου, κίνδυνος ή υψηλός κίνδυνος) και να ενημερώνονται τα αρμόδια τμήματα του οργανισμού.
- Εάν απαιτείται, θα πρέπει να γίνει γνωστοποίηση στην εποπτική αρχή και, πιθανώς, ανακοίνωση της παραβίασης στα επηρεαζόμενα πρόσωπα.

[23] Θα πρέπει να σημειωθεί ότι τα δεδομένα καταγραφής που διευκολύνουν τη δυνατότητα ελέγχου, π.χ. της αποθήκευσης, των τροποποιήσεων ή της διαγραφής δεδομένων, δύνανται επίσης να χαρακτηριστούν ως δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με το πρόσωπο που ξεκίνησε την αντίστοιχη πράξη επεξεργασίας.

- Παράλληλα, ο υπεύθυνος επεξεργασίας θα πρέπει να ενεργεί ώστε να περιορίζει και να θεραπεύει την παραβίαση.
- Η παραβίαση θα πρέπει να τεκμηριώνεται καθώς εξελίσσεται.

Συνεπώς, θα πρέπει να είναι σαφές ότι ο υπεύθυνος επεξεργασίας έχει υποχρέωση να αναλαμβάνει δράση βάσει οποιασδήποτε αρχικής ειδοποίησης και να διαπιστώνει εάν έχει όντως σημειωθεί παραβίαση. Αυτό το σύντομο χρονικό διάστημα επιτρέπει σε ορισμένο βαθμό τη διερεύνηση, ενώ ο υπεύθυνος επεξεργασίας μπορεί να συλλέξει στοιχεία και άλλες σχετικές λεπτομέρειες. Ωστόσο, μόλις ο υπεύθυνος επεξεργασίας διαπιστώσει με εύλογο βαθμό βεβαιότητας ότι έχει σημειωθεί παραβίαση, εφόσον πληρούνται οι προϋποθέσεις που προβλέπονται στο άρθρο 33 παράγραφος 1, πρέπει να το γνωστοποιήσει στην εποπτική αρχή αμελλητί και, ει δυνατόν, το αργότερο εντός 72 ωρών[24]. Εάν ένας υπεύθυνος επεξεργασίας δεν ενεργήσει εγκαίρως και καταστεί εμφανές ότι όντως σημειώθηκε παραβίαση, θα μπορούσε να θεωρηθεί ότι δεν έγινε γνωστοποίηση σύμφωνα με το άρθρο 33.

Το άρθρο 32 καθιστά σαφές ότι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία θα πρέπει να θεσπίζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζουν κατάλληλο επίπεδο ασφάλειας των δεδομένων προσωπικού χαρακτήρα: η ικανότητα έγκαιρου εντοπισμού, αντιμετώπισης και αναφοράς μιας παραβίασης θα πρέπει να θεωρείται βασικό στοιχείο αυτών των μέτρων.

3. Από κοινού υπεύθυνοι επεξεργασίας

Το άρθρο 26 αφορά τους από κοινού υπευθύνους επεξεργασίας και διευκρινίζει ότι οι από κοινού υπεύθυνοι επεξεργασίας καθορίζουν τις αντίστοιχες αρμοδιότητές τους όσον αφορά τη συμμόρφωση με τον ΓΚΠΔ[25]. Σ' αυτό θα περιλαμβάνεται ο καθορισμός του μέρους που θα έχει την ευθύνη για τη συμμόρφωση με τις υποχρεώσεις δυνάμει των άρθρων 33 και 34. Η ΟΕ29 συνιστά οι συμβατικές ρυθμίσεις μεταξύ των από κοινού υπευθύνων επεξεργασίας να περιλαμβάνουν διατάξεις που να καθορίζουν ποιος υπεύθυνος επεξεργασίας θα φέρει την ευθύνη για τη συμμόρφωση με τις υποχρεώσεις γνωστοποίησης παραβιάσεων του ΓΚΠΔ.

4. Υποχρεώσεις των εκτελούντων την επεξεργασία

Ο υπεύθυνος επεξεργασίας διατηρεί τη γενική ευθύνη για την προστασία των δεδομένων προσωπικού χαρακτήρα, ωστόσο ο εκτελών την επεξεργασία διαδραματίζει σημαντικό ρόλο βοηθώντας τον υπεύθυνο επεξεργασίας να συμμορφώνεται με τις υποχρεώσεις του. Αυτό αφορά επίσης τη γνωστοποίηση παραβιάσεων. Πράγματι, το άρθρο 28 παράγραφος 3 διευκρινίζει ότι η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη. Το άρθρο 28 παράγραφος 3 στοιχείο στ) αναφέρει ότι η σύμβαση ή άλλη πράξη προβλέπει ότι ο εκτελών την επεξεργασία «συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 32 έως 36, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία».

Το άρθρο 33 παράγραφος 2 καθιστά σαφές ότι, εάν ένας εκτελών την επεξεργασία χρησιμοποιείται από έναν υπεύθυνο επεξεργασίας και ο εκτελών την επεξεργασία αποκτήσει γνώση παραβίασης των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται για λογαριασμό του υπεύθυνου επεξεργασίας, ο εκτελών την επεξεργασία πρέπει να ενημερώνει τον υπεύθυνο επεξεργασίας «αμελλητί». Θα πρέπει

[24] Βλ. κανονισμό αριθ. 1182/71 περί καθορισμού των κανόνων που εφαρμόζονται στις προθεσμίες, ημερομηνίες και διορίες, ο οποίος είναι διαθέσιμος στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] Βλ. επίσης αιτιολογική σκέψη 79.

να σημειωθεί ότι ο εκτελών την επεξεργασία δεν χρειάζεται να αξιολογήσει πρώτα την πιθανότητα κινδύνου που προκύπτει από παραβίαση προτού ενημερώσει τον υπεύθυνο επεξεργασίας· ο υπεύθυνος επεξεργασίας είναι εκείνος που πρέπει να διενεργήσει αυτή την αξιολόγηση μόλις λάβει γνώση της παραβίασης. Ο εκτελών την επεξεργασία πρέπει απλώς να διαπιστώσει εάν έχει σημειωθεί παραβίαση και, εν συνεχεία, να ενημερώσει τον υπεύθυνο επεξεργασίας. Ο υπεύθυνος επεξεργασίας χρησιμοποιεί τον εκτελούντα την επεξεργασία για την επίτευξη των σκοπών του· συνεπώς, θα πρέπει, καταρχήν, να θεωρείται ότι ο υπεύθυνος επεξεργασίας αποκτά «γνώση» μόλις ο εκτελών την επεξεργασία τον ενημερώσει σχετικά με την παραβίαση. Η υποχρέωση του εκτελούντος την επεξεργασία να ενημερώνει τον υπεύθυνο επεξεργασίας του επιτρέπει στον υπεύθυνο επεξεργασίας να αντιμετωπίσει την παραβίαση και να αποφασίσει κατά πόσο απαιτείται να ενημερώσει την εποπτική αρχή σύμφωνα με το άρθρο 33 παράγραφος 1 και τα επηρεαζόμενα πρόσωπα σύμφωνα με το άρθρο 34 παράγραφος 1. Ο υπεύθυνος επεξεργασίας ενδέχεται επίσης να θέλει να διερευνήσει την παραβίαση, καθώς ο εκτελών την επεξεργασία μπορεί να μην είναι σε θέση να γνωρίζει όλα τα πραγματικά γεγονότα που αφορούν το ζήτημα, εάν, για παράδειγμα, ο υπεύθυνος επεξεργασίας έχει ακόμη στην κατοχή του ένα αντίγραφο ή αντίγραφο ασφαλείας των δεδομένων προσωπικού χαρακτήρα που καταστράφηκαν ή απωλέσθηκαν. Αυτό ενδέχεται να επηρεάσει την ανάγκη ή μη γνωστοποίησης στη συνέχεια από τον υπεύθυνο επεξεργασίας.

Ο ΓΚΠΔ δεν προβλέπει ρητή προθεσμία εντός της οποίας ο εκτελών την επεξεργασία πρέπει να ειδοποιήσει τον υπεύθυνο επεξεργασίας, πέραν της υποχρέωσής του να το πράξει «αμελλητί». Κατά συνέπεια, η ΟΕ29 συνιστά ο εκτελών την επεξεργασία να ενημερώνει αμελλητί τον υπεύθυνο επεξεργασίας και να παρέχονται σταδιακά περαιτέρω πληροφορίες σχετικά με την παραβίαση καθώς θα καθίστανται διαθέσιμες περισσότερες λεπτομέρειες. Αυτό είναι σημαντικό ώστε ο υπεύθυνος επεξεργασίας να βοηθείται στην εκπλήρωση της απαίτησης γνωστοποίησης στην εποπτική αρχή εντός 72 ωρών.

Όπως επεξηγείται παραπάνω, η σύμβαση μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία θα πρέπει να διευκρινίζει τον τρόπο με τον οποίο θα πρέπει να πληρούνται οι απαιτήσεις που αναφέρονται στο άρθρο 33 παράγραφος 2 πέραν των λοιπών διατάξεων του ΓΚΠΔ. Σ' αυτές τις απαιτήσεις μπορούν να περιλαμβάνονται οι απαιτήσεις για έγκαιρη γνωστοποίηση από τον εκτελούντα την επεξεργασία, οι οποίες βοηθούν με τη σειρά τους τον υπεύθυνο επεξεργασίας στην εκπλήρωση των υποχρεώσεων αναφοράς στην εποπτική αρχή εντός 72 ωρών.

Στην περίπτωση που ο εκτελών την επεξεργασία παρέχει υπηρεσίες σε πολλαπλούς υπευθύνους επεξεργασίας, οι οποίοι επηρεάζονται όλοι από το ίδιο περιστατικό, ο εκτελών την επεξεργασία θα πρέπει να αναφέρει τις λεπτομέρειες του περιστατικού σε κάθε υπεύθυνο επεξεργασίας.

Ένας εκτελών την επεξεργασία θα μπορούσε να προβεί σε γνωστοποίηση για λογαριασμό του υπευθύνου επεξεργασίας, εάν ο υπεύθυνος επεξεργασίας έχει παράσχει στον εκτελούντα την επεξεργασία την κατάλληλη άδεια και αυτό αποτελεί μέρος των συμβατικών ρυθμίσεων μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία. Αυτή η γνωστοποίηση πρέπει να γίνεται σύμφωνα με τα άρθρα 33 και 34. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η νομική ευθύνη για τη γνωστοποίηση εξακολουθεί να βαρύνει τον υπεύθυνο επεξεργασίας.

Δ. Παροχή πληροφοριών στην εποπτική αρχή

5. Απαιτούμενες πληροφορίες

Όταν ένας υπεύθυνος επεξεργασίας γνωστοποιεί μια παραβίαση στην εποπτική αρχή, το άρθρο 33 παράγραφος 3 αναφέρει ότι θα πρέπει κατ' ελάχιστο να:

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

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

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

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

Ο ΓΚΠΔ δεν ορίζει τις κατηγορίες υποκειμένων των δεδομένων ή αρχείων δεδομένων προσωπικού χαρακτήρα. Ωστόσο, η ΟΕ29 προτείνει κατηγορίες υποκειμένων των δεδομένων για να αναφερθεί στους διάφορους τύπους προσώπων τα δεδομένα προσωπικού χαρακτήρα των οποίων έχουν επηρεαστεί από παραβίαση: ανάλογα με τις περιγραφικές παραμέτρους που χρησιμοποιούνται, τα υποκείμενα των δεδομένων θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, παιδιά και άλλες ευάλωτες ομάδες, άτομα με αναπηρίες, εργαζομένους ή πελάτες. Ομοίως, οι κατηγορίες αρχείων δεδομένων προσωπικού χαρακτήρα μπορούν να αφορούν τους διαφόρους τύπους αρχείων που ο υπεύθυνος επεξεργασίας μπορεί να επεξεργάζεται, όπως δεδομένα υγείας, εκπαιδευτικά αρχεία, πληροφορίες κοινωνικής πρόνοιας, χρηματοπιστωτικά στοιχεία, αριθμούς τραπεζικών λογαριασμών, αριθμούς διαβατηρίων κ.ο.κ.

Η αιτιολογική σκέψη 85 καθιστά σαφές ότι ένας από τους σκοπούς της γνωστοποίησης είναι ο περιορισμός της ζημίας για τα πρόσωπα. Συνακόλουθα, εάν τα είδη υποκειμένων των δεδομένων ή τα είδη δεδομένων προσωπικού χαρακτήρα υποδεικνύουν έναν κίνδυνο συγκεκριμένης ζημίας που προκύπτει ως αποτέλεσμα μιας παραβίασης (π.χ., κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, απειλή για το επαγγελματικό απόρρητο), είναι σημαντικό αυτές οι κατηγορίες να αναφέρονται στο πλαίσιο της γνωστοποίησης. Κατ' αυτό τον τρόπο, υπάρχει σύνδεση με την απαίτηση περιγραφής των πιθανών συνεπειών της παραβίασης.

Όταν δεν υπάρχουν διαθέσιμες ακριβείς πληροφορίες (π.χ., ο ακριβής αριθμός υποκειμένων των δεδομένων που επηρεάζεται), αυτό δεν θα πρέπει να συνιστά εμπόδιο στην έγκαιρη γνωστοποίηση της παραβίασης. Ο ΓΚΠΔ επιτρέπει να γίνονται κατά προσέγγιση εκτιμήσεις ως προς τον αριθμό των επηρεαζόμενων προσώπων και τον αριθμό των σχετικών αρχείων δεδομένων προσωπικού χαρακτήρα. Η έμφαση θα πρέπει να δίνεται στην αντιμετώπιση των δυσμενών συνεπειών της παραβίασης και όχι στην παροχή ακριβών αριθμητικών στοιχείων. Ως εκ τούτου, όταν έχει καταστεί σαφές ότι πρόκειται για παραβίαση, αλλά δεν είναι ακόμη γνωστός ο βαθμός αυτής, η γνωστοποίηση σε στάδια (βλ. παρακάτω) είναι ένας ασφαλής τρόπος για την εκπλήρωση των υποχρεώσεων γνωστοποίησης.

Το άρθρο 33 παράγραφος 3 αναφέρει ότι ο υπεύθυνος επεξεργασίας παρέχει «κατ' ελάχιστο» αυτές τις πληροφορίες με μια γνωστοποίηση. Συνεπώς, ένας υπεύθυνος επεξεργασίας μπορεί, εάν είναι απαραίτητο, να επιλέξει να παράσχει περαιτέρω λεπτομέρειες. Τα διάφορα είδη παραβιάσεων (εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας) ενδέχεται να απαιτούν την παροχή περαιτέρω πληροφοριών για την πλήρη επεξήγηση των περιστάσεων κάθε περίπτωσης.

Παράδειγμα

Στο πλαίσιο της γνωστοποίησής του στην εποπτική αρχή, ένας υπεύθυνος επεξεργασίας μπορεί να κρίνει ότι είναι χρήσιμο να αναφέρει το όνομα του εκτελούντος την επεξεργασία εάν εμπλέκεται στη γενεσιουργό αιτία μιας παραβίασης, και ιδίως εάν αυτό έχει οδηγήσει σε περιστατικό που επηρεάζει τα αρχεία δεδομένων προσωπικού χαρακτήρα πολλών άλλων υπευθύνων επεξεργασίας που χρησιμοποιούν τον ίδιο εκτελούντα την επεξεργασία.

Σε κάθε περίπτωση, η εποπτική αρχή δύναται να ζητάει περαιτέρω λεπτομέρειες στο πλαίσιο της έρευνάς της για την παραβίαση.

6. Σταδιακή γνωστοποίηση

Ανάλογα με τη φύση μιας παραβίασης, ενδέχεται να απαιτείται περαιτέρω διερεύνηση από τον υπεύθυνο επεξεργασίας ώστε να εξακριβώσει όλα τα σχετικά γεγονότα που αφορούν το περιστατικό. Συνεπώς, το άρθρο 33 παράγραφος 4 αναφέρει ότι:

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

Αυτό σημαίνει ότι ο ΓΚΠΔ αναγνωρίζει ότι οι υπεύθυνοι επεξεργασίας δεν θα έχουν πάντα όλες τις απαραίτητες πληροφορίες σχετικά με μια παραβίαση εντός 72 ωρών από τη στιγμή που απέκτησαν γνώση αυτής, καθώς οι πλήρεις και ολοκληρωμένες λεπτομέρειες του περιστατικού ενδέχεται να μην είναι πάντα διαθέσιμες κατά τη διάρκεια αυτής της αρχικής περιόδου. Ως εκ τούτου, επιτρέπει τη σταδιακή γνωστοποίηση. Αυτό είναι πιο πιθανό να συμβαίνει στην περίπτωση παραβιάσεων με πιο περίπλοκο χαρακτήρα, όπως ορισμένα περιστατικά κυβερνοασφάλειας όπου, για παράδειγμα, ενδέχεται να απαιτείται διεξοδική εγκληματολογική έρευνα ώστε να διαπιστωθούν πλήρως η φύση της παραβίασης και ο βαθμός στον οποίο τα δεδομένα προσωπικού χαρακτήρα έχουν τεθεί σε κίνδυνο. Συνεπώς, σε πολλές περιπτώσεις, ο υπεύθυνος επεξεργασίας θα πρέπει να διεξάγει περαιτέρω έρευνα και να δίνει συνέχεια με πρόσθετες πληροφορίες που θα αποκτά σε μεταγενέστερο στάδιο. Αυτό επιτρέπεται εφόσον ο υπεύθυνος επεξεργασίας αιτιολογεί την καθυστέρηση, σύμφωνα με το άρθρο 33 παράγραφος 1. Η ΟΕ29 θεωρεί ότι, όταν ο υπεύθυνος επεξεργασίας ενημερώνει για πρώτη φορά την εποπτική αρχή, θα πρέπει να ενημερώνει επίσης την εποπτική αρχή εάν ο ίδιος δεν διαθέτει ακόμη όλες τις απαιτούμενες πληροφορίες και ότι θα παράσχει περισσότερες λεπτομέρειες σε μεταγενέστερο στάδιο. Η εποπτική αρχή θα πρέπει να συμφωνήσει όσον αφορά τον τρόπο και τον χρόνο με τον οποίο θα πρέπει να παρέχονται οι πρόσθετες πληροφορίες. Το γεγονός αυτό δεν εμποδίζει τον υπεύθυνο επεξεργασίας από το να παρέχει περαιτέρω πληροφορίες σε οποιοδήποτε άλλο στάδιο, εάν λάβει γνώση πρόσθετων σχετικών λεπτομερειών για την παραβίαση οι οποίες πρέπει να παρασχεθούν στην εποπτική αρχή.

Η απαίτηση γνωστοποίησης θα πρέπει να εστιάζει στο να ενθαρρύνει τους υπευθύνους επεξεργασίας να ενεργούν άμεσα σε περίπτωση παραβίασης, να την περιορίζουν και, εάν είναι δυνατόν, να ανακτούν τα δεδομένα προσωπικού χαρακτήρα που έχουν τεθεί σε κίνδυνο, καθώς και ζητούν σχετικές συμβουλές από την εποπτική αρχή. Η γνωστοποίηση στην εποπτική αρχή εντός των πρώτων 72 ωρών μπορεί να παράσχει στον υπεύθυνο επεξεργασίας τη δυνατότητα να βεβαιωθεί ότι οι αποφάσεις σχετικά με την ενημέρωση ή μη των προσώπων είναι ορθές.

Ωστόσο, ο σκοπός της γνωστοποίησης στην εποπτική αρχή δεν είναι μόνο η λήψη καθοδήγησης όσον αφορά το εάν πρέπει να ενημερωθούν τα επηρεαζόμενα πρόσωπα. Θα είναι προφανές σε ορισμένες περιπτώσεις ότι, λόγω της φύσης της παραβίασης και της σοβαρότητας του κινδύνου, ο υπεύθυνος θα πρέπει να ενημερώνει αμελλητί τα επηρεαζόμενα πρόσωπα. Για παράδειγμα, εάν υπάρχει άμεση απειλή υποκλοπής ταυτότητας ή εάν έχουν κοινοποιηθεί στο διαδίκτυο ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα[26], ο υπεύθυνος επεξεργασίας θα πρέπει να ενεργεί αμελλητί για να περιορίσει την παραβίαση και να την ανακοινώσει στα ενδιαφερόμενα πρόσωπα (βλ. ενότητα ΙΙΙ). Σε εξαιρετικές περιστάσεις, αυτό μπορεί να γίνεται ακόμη και πριν από τη γνωστοποίηση στην εποπτική αρχή. Γενικότερα, η γνωστοποίηση στην εποπτική αρχή δεν πρέπει να χρησιμεύει ως αιτιολογία για τη μη ανακοίνωση της παραβίασης στο υποκείμενο των δεδομένων, στις περιπτώσεις όπου απαιτείται.

Θα πρέπει επίσης να είναι σαφές ότι, μετά την αρχική γνωστοποίηση, ένας υπεύθυνος επεξεργασίας θα μπορούσε ενημερώνει την εποπτική αρχή εάν, στο πλαίσιο έρευνας παρακολούθησης, προκύψουν στοιχεία ότι το περιστατικό ασφάλειας ήταν περιορισμένο και στην πραγματικότητα δεν συνέβη

[26] Βλ. άρθρο 9.

παραβίαση. Αυτές οι πληροφορίες θα μπορούσαν στη συνέχεια να προστεθούν στις πληροφορίες που έχουν ήδη παρασχεθεί στην εποπτική αρχή και το περιστατικό να καταγραφεί, συνεπώς, ως μη παραβίαση. Δεν προβλέπεται κύρωση για την αναφορά συμβάντος που εν τέλει προκύπτει ότι δεν συνιστά παραβίαση.

Παράδειγμα

Ένας υπεύθυνος επεξεργασίας ενημερώνει την εποπτική αρχή εντός 72 ώρες από τον εντοπισμό μιας παραβίασης ότι έχει χάσει το κλειδί USB του που περιέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα ορισμένων από τους πελάτες του. Το κλειδί USB εντοπίζεται αργότερα καταχωρισμένο σε λανθασμένο αρχείο στις εγκαταστάσεις του υπευθύνου επεξεργασίας και ανακτάται. Ο υπεύθυνος επεξεργασίας ενημερώνει την εποπτική αρχή και ζητάει την τροποποίηση της γνωστοποίησης.

Θα πρέπει να σημειωθεί ότι μια σταδιακή προσέγγιση της γνωστοποίησης ακολουθείται ήδη στο πλαίσιο των υφιστάμενων υποχρεώσεων που προβλέπονται στην οδηγία 2002/58/ΕΚ, στον κανονισμό (ΕΕ) αριθ. 611/2013, καθώς και για άλλα περιστατικά που αναφέρονται από τα επηρεαζόμενα μέρη.

7. Καθυστερημένες γνωστοποιήσεις

Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση. Το γεγονός αυτό, σε συνδυασμό με την προσέγγιση της σταδιακής γνωστοποίησης, συνεπάγεται την αναγνώριση ότι ένας υπεύθυνος επεξεργασίας ενδέχεται να μην είναι πάντα σε θέση να γνωστοποιήσει μια παραβίαση εντός του συγκεκριμένου χρονικού διαστήματος και ότι μπορεί να γίνει αποδεκτή μια καθυστερημένη γνωστοποίηση.

Αυτό μπορεί να συμβαίνει όταν, για παράδειγμα, ένας υπεύθυνος επεξεργασίας έρχεται αντιμέτωπος με πολλαπλές, παρεμφερούς φύσεως παραβιάσεις της εμπιστευτικότητας σε σύντομο χρονικό διάστημα, οι οποίες επηρεάζουν μεγάλο αριθμό υποκειμένων των δεδομένων κατά τον ίδιο τρόπο. Ένας υπεύθυνος επεξεργασίας θα μπορούσε να αποκτήσει γνώση μιας παραβίασης και, ενώ έχει ξεκινήσει να τη διερευνά, και πριν από τη γνωστοποίηση, να εντοπίσει κι άλλες παρεμφερείς παραβιάσεις, οι οποίες οφείλονται σε διαφορετικές αιτίες. Ανάλογα με τις περιστάσεις, ο υπεύθυνος επεξεργασίας ενδέχεται να χρειαστεί κάποιο χρόνο για να διαπιστώσει την έκταση των παραβιάσεων και, αντί να γνωστοποιήσει κάθε παραβίαση ξεχωριστά, διαμορφώνει μια ουσιαστική γνωστοποίηση η οποία αφορά διάφορες πολύ παρεμφερείς παραβιάσεις, με πιθανώς διαφορετικές αιτίες. Το γεγονός αυτό θα μπορούσε να έχει ως αποτέλεσμα τη γνωστοποίηση στην εποπτική αρχή με καθυστέρηση μεγαλύτερη των 72 ωρών αφότου ο υπεύθυνος επεξεργασίας απέκτησε για πρώτη φορά γνώση αυτών των παραβιάσεων.

Με τη στενή έννοια του όρου, κάθε μεμονωμένη παραβίαση είναι ένα περιστατικό που πρέπει να αναφέρεται. Ωστόσο, για να μην είναι υπερβολικά επαχθής η διαδικασία, ο υπεύθυνος επεξεργασίας ενδέχεται να μπορεί να διενεργήσει μια «ομαδοποιημένη» γνωστοποίηση για όλες αυτές τις παραβιάσεις, υπό την προϋπόθεση ότι αφορούν το ίδιο είδος δεδομένων προσωπικού χαρακτήρα, τα οποία παραβιάζονται με τον ίδιο τρόπο, σε σχετικά σύντομο χρονικό διάστημα. Εάν προκύψουν διάφορες παραβιάσεις οι οποίες αφορούν διαφορετικό είδος δεδομένων προσωπικού χαρακτήρα, τα οποία παραβιάζονται κατά τρόπο διαφορετικό, η γνωστοποίηση θα πρέπει να πραγματοποιείται με τον συνήθη τρόπο και κάθε παραβίαση αναφέρεται σύμφωνα με το άρθρο 33.

Παρότι ο ΓΚΠΔ επιτρέπει σε ορισμένο βαθμό την υποβολή γνωστοποιήσεων με καθυστέρηση, το γεγονός αυτό δεν θα πρέπει να οδηγεί στο συμπέρασμα ότι πρόκειται για κάτι που συμβαίνει τακτικά. Αξίζει να επισημανθεί ότι ομαδοποιημένες γνωστοποιήσεις μπορούν επίσης να γίνονται για πολλαπλές παρεμφερείς παραβιάσεις που αναφέρονται εντός 72 ωρών.

Ε. Διασυνοριακές παραβιάσεις και παραβιάσεις σε εγκαταστάσεις τρίτων χωρών

8. Διασυνοριακές παραβιάσεις

Όταν υπάρχει διασυνοριακή επεξεργασία[27] δεδομένων προσωπικού χαρακτήρα, μια παραβίαση ενδέχεται να επηρεάζει υποκείμενα των δεδομένων σε περισσότερα από ένα κράτη μέλη. Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι, σε περίπτωση παραβίασης, ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώνει την εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55 του ΓΚΠΔ[28]. Το άρθρο 55 παράγραφος 1 αναφέρει ότι:

> «Κάθε εποπτική αρχή είναι αρμόδια να εκτελεί τα καθήκοντα και να ασκεί τις εξουσίες που της ανατίθενται σύμφωνα με τον παρόντα κανονισμό στο έδαφος του κράτους μέλους της.»

Ωστόσο, το άρθρο 56 παράγραφος 1 αναφέρει:

> «Με την επιφύλαξη του άρθρου 55, η εποπτική αρχή της κύριας ή της μόνης εγκατάστασης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία είναι αρμόδια να ενεργεί ως επικεφαλής εποπτική αρχή για τις διασυνοριακές πράξεις επεξεργασίας του εν λόγω υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σύμφωνα με τη διαδικασία που προβλέπεται στο άρθρο 60.»

Επιπλέον, το άρθρο 56 παράγραφος 6 αναφέρει:

> «Η επικεφαλής εποπτική αρχή είναι ο μοναδικός συνομιλητής του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία για τη διασυνοριακή πράξη επεξεργασίας του εν λόγω υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.»

Αυτό σημαίνει ότι, όταν προκύπτει μια παραβίαση στο πλαίσιο διασυνοριακής επεξεργασίας και απαιτείται γνωστοποίηση, ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώνει την επικεφαλής εποπτική αρχή[29]. Συνεπώς, κατά την κατάρτιση ενός σχεδίου αντιμετώπισης παραβιάσεων, ο υπεύθυνος επεξεργασίας πρέπει να διενεργεί αξιολόγηση όσον αφορά το ποια εποπτική αρχή είναι η επικεφαλής εποπτική αρχή στην οποία πρέπει να απευθύνει τη γνωστοποίηση[30]. Κατ' αυτόν τον τρόπο, ο υπεύθυνος επεξεργασίας θα μπορεί να ανταποκρίνεται άμεσα σε μια παραβίαση, καθώς και να εκπληρώνει τις υποχρεώσεις του όσον αφορά το άρθρο 33. Θα πρέπει να είναι σαφές ότι, σε περίπτωση παραβίασης που αφορά διασυνοριακή επεξεργασία, η γνωστοποίηση θα πρέπει να γίνεται στην επικεφαλής εποπτική αρχή, η οποία δεν βρίσκεται απαραίτητα εκεί όπου βρίσκονται τα επηρεαζόμενα υποκείμενα των δεδομένων ή εκεί όπου έχε προκύψει η παραβίαση. Κατά τη γνωστοποίηση στην επικεφαλής αρχή, ο υπεύθυνος επεξεργασίας θα πρέπει να αναφέρει, κατά περίπτωση, εάν η παραβίαση αφορά εγκαταστάσεις που βρίσκονται σε άλλα κράτη μέλη, καθώς και σε ποια κράτη μέλη τα υποκείμενα των δεδομένων είναι πιθανό να έχουν επηρεαστεί από την παραβίαση. Εάν ο υπεύθυνος επεξεργασίας έχει οποιαδήποτε αμφιβολία όσον αφορά την ταυτότητα της επικεφαλής εποπτικής αρχής, θα πρέπει, κατ' ελάχιστο, να ενημερώνει την τοπική εποπτική αρχή στην τοποθεσία όπου έχει προκύψει η παραβίαση.

---

[27] Βλ. άρθρο 4 σημείο 23).

[28] Βλ. επίσης αιτιολογική σκέψη 122.

[29] Βλ. κατευθυντήριες γραμμές της ΟΕ29 για τον εντοπισμό της επικεφαλής εποπτικής αρχής ενός υπευθύνου επεξεργασίας ή εντός εκτελούντος την επεξεργασία, οι οποίες είναι διαθέσιμες στη διεύθυνση http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] Κατάλογος με τα στοιχεία επικοινωνίας για όλες τις ευρωπαϊκές εθνικές αρχές προστασίας δεδομένων είναι διαθέσιμος στη διεύθυνση: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

9. Παραβιάσεις σε εγκαταστάσεις τρίτων χωρών

Το άρθρο 3 αφορά το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ, μεταξύ άλλων όταν ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία που δεν είναι εγκατεστημένος στην ΕΕ. Πιο συγκεκριμένα, το άρθρο 3 παράγραφος 2 αναφέρει ότι[31]:

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

Το άρθρο 3 παράγραφος 3 είναι επίσης σχετικό και αναφέρει ότι[32]:

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

Συνεπώς, όταν ένας υπεύθυνος επεξεργασίας που δεν είναι εγκατεστημένος στην ΕΕ υπόκειται στο άρθρο 3 παράγραφος 2 ή στο άρθρο 3 παράγραφος 3 και έρχεται αντιμέτωπος με μια παραβίαση, εξακολουθεί να δεσμεύεται από τις υποχρεώσεις γνωστοποίησης των άρθρων 33 και 34. Το άρθρο 27 απαιτεί από τον υπεύθυνο επεξεργασίας (και τον εκτελούντα την επεξεργασία) να ορίζει εκπρόσωπο στην ΕΕ στις περιπτώσεις που εφαρμόζεται το άρθρο 3 παράγραφος 2. Σε τέτοιες περιπτώσεις, η ΟΕ29 συνιστά η γνωστοποίηση να γίνεται στην εποπτική αρχή του κράτους μέλους στο οποίο είναι εγκατεστημένος ο εκπρόσωπος του υπευθύνου επεξεργασίας στην ΕΕ[33]. Ομοίως, όταν ένας εκτελών την επεξεργασία υπόκειται στο άρθρο 3 παράγραφος 2, θα δεσμεύεται από τις υποχρεώσεις που ισχύουν για τους εκτελούντες την επεξεργασία –και οι οποίες έχουν ιδιαίτερη σημασία στην προκειμένη περίπτωση– να γνωστοποιεί μια παραβίαση στον υπεύθυνο επεξεργασίας δυνάμει του άρθρου 33 παράγραφος 2.

ΣΤ. Προϋποθέσεις σύμφωνα με τις οποίες δεν απαιτείται γνωστοποίηση

Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι, σε περίπτωση παραβίασης που «δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων», δεν απαιτείται γνωστοποίηση στην εποπτική αρχή. Ένα παράδειγμα μπορεί να είναι η περίπτωση όπου τα δεδομένα προσωπικού χαρακτήρα είναι ήδη διαθέσιμα στο κοινό και η κοινοποίησή τους δεν επιφέρει πιθανό κίνδυνο για το πρόσωπο. Αυτό έρχεται σε αντίθεση με τις υφιστάμενες απαιτήσεις γνωστοποίησης παραβιάσεων για τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό που προβλέπονται στην οδηγία 2009/136/ΕΚ, σύμφωνα με την οποία όλες οι σχετικές παραβιάσεις πρέπει να γνωστοποιούνται στην αρμόδια αρχή.

---

[31] Βλ. επίσης αιτιολογικές σκέψεις 23 και 24.

[32] Βλ. επίσης αιτιολογική σκέψη 25.

[33] Βλ. αιτιολογική σκέψη 80 και άρθρο 27.

Στη γνωμοδότησή της 03/2014 σχετικά τη γνωστοποίηση παραβιάσεων προσωπικών δεδομένων[34], η ΟΕ29 διευκρινίζει ότι μια παραβίαση της εμπιστευτικότητας δεδομένων προσωπικού χαρακτήρα τα οποία κρυπτογραφήθηκαν με τη χρήση αλγορίθμου προηγμένης τεχνολογίας δεν παύει να συνιστά παραβίαση δεδομένων προσωπικού χαρακτήρα και πρέπει να γνωστοποιείται. Ωστόσο, εάν η εμπιστευτικότητα του κλειδιού δεν έχει επηρεαστεί, δηλαδή το κλειδί δεν τέθηκε σε κίνδυνο στο πλαίσιο παραβίασης της ασφάλειας και δημιουργήθηκε ώστε να μην μπορεί να εξακριβωθεί με διαθέσιμα τεχνικά μέσα από κανένα άτομο που δεν διαθέτει άδεια πρόσβασης σ' αυτό, τα δεδομένα είναι καταρχήν ακατάληπτα. Ως εκ τούτου, η παραβίαση δεν ενδέχεται να επηρεάσει δυσμενώς τα πρόσωπα και, κατά συνέπεια, δεν απαιτείται η ανακοίνωση σ' αυτά τα πρόσωπα[35]. Ωστόσο, ακόμη και όταν τα δεδομένα είναι κρυπτογραφημένα, τυχόν απώλεια ή αλλοίωση μπορεί να έχει αρνητικές συνέπειες για τα υποκείμενα των δεδομένων σε περίπτωση που ο υπεύθυνος επεξεργασίας δεν διαθέτει επαρκή αριθμό αντιγράφων ασφαλείας. Σ' αυτή την περίπτωση, απαιτείται η ανακοίνωση στα υποκείμενα των δεδομένων, ακόμη και αν στα δεδομένα είχαν εφαρμοστεί κατάλληλα μέτρα κρυπτογράφησης.

Η ΟΕ29 εξήγησε επίσης ότι αυτό θα συνέβαινε επίσης εάν δεδομένα προσωπικού χαρακτήρα, όπως κωδικοί πρόσβασης, διασφαλίζονταν με πρόσθετο επίπεδο ασφάλειας και κρυπτογραφική συνάρτηση κατακερματισμού, η τιμή κατακερματισμού τους είχε υπολογιστεί με εξελιγμένη κρυπτοθετημένη συνάρτηση κατακερματισμού, το κλειδί που χρησιμοποιήθηκε για την αποκρυπτοθέτηση των δεδομένων δεν είχε παραβιαστεί σε οποιαδήποτε παραβίαση ασφαλείας και το κλειδί που είχε χρησιμοποιηθεί για την αποκρυπτοθέτηση των δεδομένων είχε δημιουργηθεί κατά τρόπο που να μην μπορεί να εξακριβωθεί με τα διαθέσιμα τεχνολογικά μέσα από οποιοδήποτε πρόσωπο που δεν έχει εξουσιοδοτημένη πρόσβαση στο κλειδί.

Συνακόλουθα, εάν τα δεδομένα προσωπικού χαρακτήρα έχουν καταστεί ουσιαστικά ακατάληπτα για πρόσωπα που δεν διαθέτουν άδεια πρόσβασης και όταν τα δεδομένα είναι αντίγραφο ή υπάρχει αντίγραφο ασφαλείας, τυχόν παραβίαση της εμπιστευτικότητας που αφορά δεόντως κρυπτογραφημένα δεδομένα προσωπικού χαρακτήρα ενδέχεται να χρειάζεται να γνωστοποιηθεί στην εποπτική αρχή. Αυτό συμβαίνει διότι μια τέτοια παραβίαση δεν ενδέχεται να επιφέρει κίνδυνο για δικαιώματα και τις ελευθερίες των προσώπων. Αυτό σημαίνει, βεβαίως, ότι ούτε το πρόσωπο θα χρειαστεί να ενημερωθεί, καθώς δεν ενδέχεται να υπάρχει υψηλός κίνδυνος. Ωστόσο, θα πρέπει να λαμβάνεται υπόψη ότι, ενώ μπορεί αρχικά να μην απαιτείται γνωστοποίηση εάν δεν υπάρχει κανένας κίνδυνος για τα δικαιώματα και τις ελευθερίες των προσώπων, αυτό το δεδομένο μπορεί να αλλάξει με την πάροδο του χρόνου και ο κίνδυνος θα πρέπει να αξιολογείται εκ νέου. Για παράδειγμα, εάν διαπιστωθεί μεταγενέστερα ότι το κλειδί έχει παραβιαστεί ή αποκαλυφθεί τρωτό σημείο στο λογισμικό κρυπτογράφησης, μπορεί να απαιτείται γνωστοποίηση.

Επιπλέον, θα πρέπει να σημειωθεί ότι, εάν έχει σημειωθεί παραβίαση και δεν υπάρχουν αντίγραφα ασφαλείας των κρυπτογραφημένων δεδομένων προσωπικού χαρακτήρα, τότε θα πρόκειται για παραβίαση της διαθεσιμότητας, η οποία θα μπορούσε να επιφέρει κινδύνους για τα πρόσωπα και, συνεπώς, ενδέχεται να απαιτείται γνωστοποίηση. Ομοίως, όταν προκύπτει παραβίαση η οποία αφορά την απώλεια κρυπτογραφημένων δεδομένων, ακόμη και αν υπάρχει αντίγραφο ασφαλείας των δεδομένων προσωπικού χαρακτήρα, μπορεί να πρόκειται για παραβίαση που πρέπει να αναφερθεί, ανάλογα με το χρονικό διάστημα που απαιτείται για την επαναφορά των δεδομένων από αυτό το αντίγραφο και τις συνέπειες που έχει στα πρόσωπα αυτή η έλλειψη διαθεσιμότητας. Όπως αναφέρει το άρθρο 32 παράγραφος 1 στοιχείο γ), ένας σημαντικός παράγοντας ασφάλειας είναι η δυνατότητα

[34] ΟΕ29, γνωμοδότηση 03/2014 σχετικά με τη γνωστοποίηση παραβιάσεων, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_el.pdf

[35] Βλ. επίσης άρθρο 4 παράγραφοι 1 και 2 του κανονισμού (ΕΕ) αριθ. 611/2013.

αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος.

Παράδειγμα

Μια παραβίαση για την οποία δεν θα απαιτούταν γνωστοποίηση στην εποπτική αρχή θα ήταν η απώλεια μιας ασφαλώς κρυπτογραφημένης κινητής συσκευής που χρησιμοποιείται από τον υπεύθυνο επεξεργασίας και το προσωπικό του. Υπό την προϋπόθεση ότι το κλειδί κρυπτογράφησης παραμένει στην ασφαλή κατοχή του υπευθύνου επεξεργασίας και δεν είναι το μοναδικό αντίγραφο των δεδομένων προσωπικού χαρακτήρα, τα δεδομένα προσωπικού χαρακτήρα δεν θα είναι προσβάσιμα σε κάποιον που κάνει επίθεση. Αυτό σημαίνει ότι η παραβίαση είναι απίθανο να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των οικείων υποκειμένων των δεδομένων. Εάν, σε μεταγενέστερο στάδιο, καταστεί εμφανές ότι το κλειδί κρυπτογράφησης τέθηκε σε κίνδυνο ή το λογισμικό κρυπτογράφησης ή ο αλγόριθμος είναι ευάλωτα, ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων θα αλλάξει και, συνεπώς, ενδέχεται να απαιτείται πλέον γνωστοποίηση.

Ωστόσο, δεν θα υπάρχει συμμόρφωση με το άρθρο 33 όταν ένας υπεύθυνος επεξεργασίας δεν ενημερώσει την εποπτική αρχή σε περίπτωση που τα δεδομένα δεν έχουν στην πραγματικότητα κρυπτογραφηθεί με ασφάλεια. Ως εκ τούτου, κατά την επιλογή του λογισμικού κρυπτογράφησης, οι υπεύθυνοι επεξεργασίας θα πρέπει να σταθμίζουν προσεκτικά την ποιότητα και την ορθή εφαρμογή της κρυπτογράφησης που προσφέρεται και να κατανοούν το επίπεδο προστασίας που παρέχει στην πραγματικότητα το λογισμικό και κατά πόσο είναι κατάλληλο για τους κινδύνους που παρουσιάζονται. Οι υπεύθυνοι επεξεργασίας θα πρέπει επίσης να είναι εξοικειωμένοι με τις λεπτομέρειες του τρόπου λειτουργίας του προϊόντος κρυπτογράφησής τους. Για παράδειγμα, μια συσκευή μπορεί να κρυπτογραφηθεί μόλις απενεργοποιηθεί, αλλά όχι ενόσω βρίσκεται σε κατάσταση αναμονής. Ορισμένα προϊόντα που χρησιμοποιούν κρυπτογράφηση έχουν «προεπιλεγμένα κλειδιά» τα οποία πρέπει να αλλάζει ο κάθε πελάτης ώστε να είναι αποτελεσματικά. Η κρυπτογράφηση ενδέχεται επίσης να θεωρείται επί του παρόντος επαρκής από τους ειδικούς στον τομέα της ασφάλειας, ωστόσο μπορεί να καταστεί παρωχημένη σε λίγα έτη. Αυτό σημαίνει ότι είναι αμφίβολο κατά πόσο τα δεδομένα θα είναι επαρκώς κρυπτογραφημένα από το συγκεκριμένο προϊόν και θα παρέχουν κατάλληλο επίπεδο προστασίας.

III. Άρθρο 34 – Ανακοίνωση στο υποκείμενο των δεδομένων

Z. Ενημέρωση των προσώπων

Σε ορισμένες περιπτώσεις, εκτός από τη γνωστοποίηση στην εποπτική αρχή, ο υπεύθυνος επεξεργασίας υποχρεούται επίσης να ανακοινώσει μια παραβίαση στα επηρεαζόμενα πρόσωπα.

Το άρθρο 34 παράγραφος 1 αναφέρει ότι:

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

Οι υπεύθυνοι επεξεργασίας θα πρέπει να θυμούνται ότι η γνωστοποίηση στην εποπτική αρχή είναι υποχρεωτική, εκτός εάν είναι απίθανο να δημιουργηθεί κίνδυνος για τα δικαιώματα και τις ελευθερίες των προσώπων ως αποτέλεσμα της παραβίασης. Επιπλέον, όταν ενδέχεται να τεθούν σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες των προσώπων ως αποτέλεσμα μιας παραβίασης, τα πρόσωπα πρέπει επίσης να ενημερώνονται. Το κατώφλι για την ανακοίνωση μιας παραβίασης στα πρόσωπα είναι, συνεπώς, υψηλότερο απ' ό,τι για τη γνωστοποίηση στις εποπτικές αρχές και,

συνακόλουθα, δεν θα απαιτείται για όλες τις παραβιάσεις η ανακοίνωση στα πρόσωπα, γεγονός που τα προστατεύει από περιττή κόπωση λόγω φόρτου γνωστοποιήσεων.

Ο ΓΚΠΔ αναφέρει ότι η ανακοίνωση μιας παραβίασης στα πρόσωπα θα πρέπει να γίνεται «αμελλητί», δηλαδή το συντομότερο δυνατόν. Ο κύριος στόχος της ανακοίνωσης στα πρόσωπα είναι η παροχή συγκεκριμένων πληροφοριών σχετικά με τις ενέργειες στις οποίες θα πρέπει να προβούν τα ίδια για να προστατευτούν[36]. Όπως αναφέρεται παραπάνω, ανάλογα με τη φύση της παραβίασης και τον κίνδυνο που τίθεται, η έγκαιρη ανακοίνωση θα βοηθήσει τα πρόσωπα να προβούν σε ενέργειες ώστε να προστατευτούν από τυχόν αρνητικές συνέπειες της παραβίασης.

Το παράτημα Β των παρουσών κατευθυντήριων γραμμών παρέχει ενδεικτικό κατάλογο παραδειγμάτων όσον αφορά το πότε μια παραβίαση μπορεί να ενδέχεται να επιφέρει υψηλό κίνδυνο για τα πρόσωπα και, συνακόλουθα, όσον αφορά το πότε ένας υπεύθυνος επεξεργασίας θα πρέπει να ανακοινώνει μια παραβίαση στα επηρεαζόμενα πρόσωπα.

Η. Απαιτούμενες πληροφορίες

Κατά την ανακοίνωση σε πρόσωπα, το άρθρο 34 παράγραφος 2 διευκρινίζει ότι:

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

Σύμφωνα μ' αυτή τη διάταξη, ο υπεύθυνος επεξεργασίας θα πρέπει κατ' ελάχιστο να παρέχει τις ακόλουθες πληροφορίες:

- σύντομη περιγραφή της φύσεως της παραβίασης·
- το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας των δεδομένων ή άλλου σημείου επικοινωνίας·
- περιγραφή των ενδεχόμενων συνεπειών της παραβίασης· και
- περιγραφή των ληφθέντων ή των προτεινόμενων προς λήψη μέτρων από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης, καθώς και, όπου ενδείκνυται, μέτρων για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Ως παράδειγμα μέτρων που έχουν ληφθεί για την αντιμετώπιση της παραβίασης και την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της, ο υπεύθυνος επεξεργασίας θα μπορούσε να αναφέρει ότι, αφού γνωστοποίησε την παραβίαση στην αρμόδια εποπτική αρχή, έλαβε συμβουλές σχετικά με τη διαχείριση της παραβίασης και τον μετριασμό των επιπτώσεών της. Ο υπεύθυνος επεξεργασίας θα πρέπει επίσης, κατά περίπτωση, να παρέχει ειδικές συμβουλές στα πρόσωπα για την προστασία τους από ενδεχόμενες δυσμενείς συνέπειες της παραβίασης, όπως επαναφορά κωδικού πρόσβασης σε περίπτωση που έχουν τεθεί σε κίνδυνο τα διαπιστευτήρια πρόσβασής τους. Ο υπεύθυνος επεξεργασίας μπορεί και πάλι να επιλέξει να παράσχει πληροφορίες επιπλέον εκείνων που απαιτούνται σ' αυτή την περίπτωση.

Θ. Επικοινωνία με τα πρόσωπα

Καταρχήν, η σχετική παραβίαση θα πρέπει να ανακοινώνεται στα επηρεαζόμενα υποκείμενα των δεδομένων, εκτός εάν αυτή η ενέργεια προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή λαμβάνεται παρόμοιο μέτρο με το οποίο τα υποκείμενα

[36] Βλ. επίσης αιτιολογική σκέψη 86.

των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο [άρθρο 34 παράγραφος 3 στοιχείο γ)].

Κατά την ανακοίνωση μιας παραβίασης στα υποκείμενα των δεδομένων θα πρέπει να χρησιμοποιούνται ειδικά μηνύματα, τα οποία δεν θα πρέπει να αποστέλλονται μαζί με άλλες πληροφορίες, όπως τακτικές ενημερώσεις, ενημερωτικά δελτία ή τυποποιημένα μηνύματα. Αυτό βοηθάει ώστε η ανακοίνωση της παραβίασης να καταστεί σαφής και διαφανής.

Παραδείγματα διαφανών μεθόδων ανακοίνωσης περιλαμβάνουν την απευθείας αποστολή μηνυμάτων (π.χ., μήνυμα ηλεκτρονικού ταχυδρομείου, μήνυμα SMS, άμεσο μήνυμα), τα πλαίσια γνωστοποίησης σε περίοπτη θέση σε ιστοτόπους, τις ανακοινώσεις μέσω ταχυδρομείου και τις διαφημίσεις σε έντυπα μέσα ενημέρωσης σε περίοπτη θέση. Μια ανακοίνωση που περιορίζεται αποκλειστικά σε ένα δελτίο Τύπου ή σε ένα εταιρικό ιστολόγιο δεν θα αποτελούσε αποτελεσματικό μέσο ανακοίνωσης μιας παραβίασης σε ένα πρόσωπο. Η ΟΕ29 συνιστά οι υπεύθυνοι επεξεργασίας να επιλέγουν το μέσο που μεγιστοποιεί τις πιθανότητες δέουσας ανακοίνωσης των πληροφοριών σε όλα τα επηρεαζόμενα πρόσωπα. Ανάλογα με τις περιστάσεις, αυτό μπορεί να σημαίνει ότι ο υπεύθυνος επεξεργασίας χρησιμοποιεί διάφορους τρόπους ανακοίνωσης αντί ενός μόνο διαύλου επικοινωνίας.

Οι υπεύθυνοι επεξεργασίας μπορεί επίσης να πρέπει να εξασφαλίζουν ότι η ανακοίνωση είναι προσβάσιμη σε κατάλληλους εναλλακτικούς μορφοτύπους και στις σχετικές γλώσσες, ώστε να διασφαλίζεται ότι τα πρόσωπα μπορούν να κατανοήσουν τις πληροφορίες που τους παρέχονται. Για παράδειγμα, κατά την ανακοίνωση μιας παραβίασης σε ένα πρόσωπο, η γλώσσα που χρησιμοποιήθηκε κατά την προηγούμενη συνήθη πορεία των επιχειρηματικών εργασιών με τον αποδέκτη θα είναι σε γενικές γραμμές κατάλληλη. Ωστόσο, εάν η παραβίαση επηρεάζει υποκείμενα των δεδομένων με τα οποία ο υπεύθυνος επεξεργασίας δεν είχε αλληλεπιδράσει κατά το παρελθόν ή ιδίως εκείνα τα υποκείμενα που διαμένουν σε διαφορετικό κράτος μέλος ή σε άλλη χώρα –εκτός της ΕΕ– από εκείνη στην οποία είναι εγκατεστημένος ο υπεύθυνος επεξεργασίας, η ανακοίνωση στην τοπική εθνική γλώσσα θα μπορούσε να είναι αποδεκτή, λαμβανομένων υπόψη των πόρων που απαιτούνται. Αυτό που έχει σημασία είναι τα υποκείμενα των δεδομένων να κατανοήσουν τη φύση της παραβίασης και τις ενέργειες στις οποίες μπορούν να προβούν για να προστατευτούν.

Οι υπεύθυνοι επεξεργασίας βρίσκονται στην καταλληλότερη θέση για να καθορίζουν τον πλέον κατάλληλο δίαυλο επικοινωνίας για την ανακοίνωση μιας παραβίασης στα πρόσωπα, ιδίως εάν αλληλεπιδρούν με τους πελάτες τους σε τακτική βάση. Ωστόσο, είναι σαφές ότι ένας υπεύθυνος επεξεργασίας θα πρέπει να είναι επιφυλακτικός ως προς τη χρήση ενός διαύλου επικοινωνίας που έχει τεθεί σε κίνδυνο από την παραβίαση, καθώς αυτός ο δίαυλος θα μπορούσε να χρησιμοποιηθεί επίσης από επιτιθέμενους που παριστάνουν τον υπεύθυνο επεξεργασίας.

Παράλληλα, στην αιτιολογική σκέψη 86 επεξηγείται ότι:

> «Οι ανακοινώσεις αυτές στα υποκείμενα των δεδομένων θα πρέπει να πραγματοποιούνται το συντομότερο δυνατόν, σε στενή συνεργασία με την ελεγκτική αρχή, τηρώντας την καθοδήγηση που παρέχεται από αυτήν ή άλλες σχετικές αρχές, όπως αρχές επιβολής του νόμου. Για παράδειγμα, η ανάγκη να μετριαστεί άμεσος κίνδυνος ζημίας θα απαιτούσε την άμεση ανακοίνωση στα υποκείμενα των δεδομένων, ενώ η αναγκαιότητα εφαρμογής κατάλληλων μέτρων κατά συνεχών ή παρόμοιων παραβιάσεων δεδομένων προσωπικού χαρακτήρα μπορεί να δικαιολογεί περισσότερο χρόνο για την ανακοίνωση.»

Συνεπώς, οι υπεύθυνοι επεξεργασίας ενδέχεται επίσης να επιθυμούν να επικοινωνήσουν και να συζητήσουν με την εποπτική αρχή, όχι μόνο με σκοπό την αναζήτηση συμβουλών σχετικά με την ενημέρωση των υποκειμένων δεδομένων για μια παραβίαση, σύμφωνα με το άρθρο 34, αλλά και για τα κατάλληλα μηνύματα που πρέπει να αποσταλούν στα πρόσωπα, καθώς και τον πλέον κατάλληλο τρόπο επικοινωνίας μαζί τους.

Μ' αυτό συνδέεται η συμβουλή που παρέχεται στην αιτιολογική σκέψη 88 ότι, κατά τη γνωστοποίηση μιας παραβίασης, θα πρέπει να λαμβάνονται υπόψη τα έννομα συμφέροντα των αρχών επιβολής του νόμου, όταν η πρόωρη κοινολόγηση μπορεί να εμποδίσει χωρίς λόγο τη διερεύνηση των συνθηκών μιας παραβίασης δεδομένων προσωπικού χαρακτήρα. Αυτό σημαίνει ότι, σε ορισμένες περιστάσεις, όταν αυτό δικαιολογείται και κατόπιν συμβουλής των αρχών επιβολής του νόμου, ο υπεύθυνος επεξεργασίας μπορεί να καθυστερεί την ανακοίνωση της παραβίασης στα επηρεαζόμενα πρόσωπα μέχρι ότου αυτή δεν θα επηρεάζει αυτές τις έρευνες. Ωστόσο, τα υποκείμενα των δεδομένων θα πρέπει να ενημερωθούν άμεσα έπειτα από αυτό το χρονικό διάστημα.

Όταν δεν είναι δυνατόν για τον υπεύθυνο επεξεργασίας να ανακοινώσει μια παραβίαση σε ένα πρόσωπο λόγω του ότι δεν υπάρχουν επαρκή δεδομένα αποθηκευμένα για να επικοινωνήσει με το πρόσωπο, σ' αυτήν συγκεκριμένη περίσταση ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώνει το πρόσωπο μόλις είναι ευλόγως εφικτό να το πράξει (π.χ., όταν ένα πρόσωπο ασκεί το δικαίωμά του, σύμφωνα με το άρθρο 15, για πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και παρέχει στον υπεύθυνο τις απαραίτητες πρόσθετες πληροφορίες για να επικοινωνήσει μαζί του).

I. Προϋποθέσεις σύμφωνα με τις οποίες δεν απαιτείται ανακοίνωση

Το άρθρο 34 παράγραφος 3 αναφέρει τρεις προϋποθέσεις οι οποίες, εάν πληρούνται, δεν απαιτούν την ανακοίνωση στα πρόσωπα σε περίπτωση παραβίασης. Αυτές είναι οι εξής:

- Ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας για την προστασία των δεδομένων προσωπικού χαρακτήρα πριν από την παραβίαση, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σ' αυτά. Τα μέτρα αυτά θα μπορούσαν, για παράδειγμα, να περιλαμβάνουν την προστασία των δεδομένων προσωπικού χαρακτήρα με κρυπτογράφηση προηγμένης τεχνολογίας ή δειγματοποίηση.
- Αμέσως έπειτα από μια παραβίαση, ο υπεύθυνος επεξεργασίας έλαβε μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει ο υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των προσώπων. Για παράδειγμα, αναλόγως με τις περιστάσεις της περίπτωσης, ο υπεύθυνος επεξεργασίας μπορεί να έχει εξακριβώσει την ταυτότητα και να έχει λάβει δράση αμέσως έναντι του προσώπου που έχει αποκτήσει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα προτού αυτό μπορέσει να τα χρησιμοποιήσει με οποιονδήποτε τρόπο. Εξακολουθεί να υπάρχει η ανάγκη να λαμβάνονται δεόντως υπόψη οι ενδεχόμενες συνέπειες οποιασδήποτε παραβίασης, πάντα σε συνάρτηση με τη φύση των σχετικών δεδομένων.
- Η επικοινωνία με τα πρόσωπα θα συνεπάγεται δυσανάλογες προσπάθειες, ίσως εάν τα στοιχεία επικοινωνίας έχουν χαθεί ως αποτέλεσμα της παραβίασης ή δεν είναι εξαρχής γνωστά[37]. Για παράδειγμα, η αποθήκη μιας στατιστικής υπηρεσίας έχει πλημμυρίσει και τα έγγραφα που περιέχουν δεδομένα προσωπικού χαρακτήρα ήταν αποθηκευμένα μόνο σε έντυπη μορφή. Ο υπεύθυνος επεξεργασίας πρέπει να κάνει μια δημόσια ανακοίνωση ή να λάβει ένα παρεμφερές μέτρο με τα οποία τα πρόσωπα θα ενημερωθούν με εξίσου αποτελεσματικό τρόπο. Στην περίπτωση όπου απαιτούνται δυσανάλογες προσπάθειες, θα μπορούσε επίσης να εξετάζεται το ενδεχόμενο εφαρμογής τεχνικών ρυθμίσεων για τη διάθεση πληροφοριών σχετικά με την παραβίαση κατόπιν αιτήματος, οι οποίες θα μπορούσαν να αποδειχθούν χρήσιμες για τα πρόσωπα που ενδέχεται να έχουν επηρεαστεί από μια παραβίαση, ωστόσο ο υπεύθυνος επεξεργασίας δεν μπορεί να επικοινωνήσει με διαφορετικό τρόπο.

[37] Βλ. κατευθυντήριες γραμμές της ΟΕ29 σχετικά με τη διαφάνεια, οι οποίες εξετάζουν το ζήτημα της δυσανάλογης προσπάθειας και είναι διαθέσιμες στη διεύθυνση http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

Σύμφωνα με την αρχή της λογοδοσίας, οι υπεύθυνοι επεξεργασίας θα πρέπει να μπορούν να αποδεικνύουν στην εποπτική αρχή ότι πληρούν μία ή περισσότερες από αυτές τις προϋποθέσεις[38]. Θα πρέπει να λαμβάνεται υπόψη ότι, ενώ μπορεί αρχικά να μην απαιτείται γνωστοποίηση εάν δεν υπάρχει κανένας κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, αυτό το δεδομένο μπορεί να αλλάξει με την πάροδο του χρόνου και ο κίνδυνος θα πρέπει να αξιολογείται εκ νέου.

Εάν ένας υπεύθυνος επεξεργασίας αποφασίσει να μην ανακοινώσει μια παραβίαση στο πρόσωπο, το άρθρο 34 παράγραφος 4 εξηγεί ότι η εποπτική αρχή μπορεί να του ζητήσει να το πράξει, εάν θεωρεί ότι η παραβίαση είναι πιθανό να επιφέρει υψηλό κίνδυνο για τα πρόσωπα. Εναλλακτικά, ενδέχεται να θεωρήσει ότι οι προϋποθέσεις του άρθρου 34 παράγραφος 3 έχουν ικανοποιηθεί, περίπτωση στην οποία δεν απαιτείται ανακοίνωση στα πρόσωπα. Εάν η εποπτική αρχή αποφασίσει ότι η απόφαση για τη μη ανακοίνωση στα υποκείμενα των δεδομένων δεν είναι δεόντως αιτιολογημένη, ενδέχεται να εξετάσει το ενδεχόμενο να ασκήσει τις εξουσίες που έχει στη διάθεσή της και να επιβάλει κυρώσεις.

IV. **Αξιολόγηση κινδύνου και υψηλού κινδύνου**

ΙΑ. Ο κίνδυνος ως παράγοντας ενεργοποίησης της υποχρέωσης γνωστοποίησης

Παρότι ο ΓΚΠΔ θεσπίζει την υποχρέωση γνωστοποίησης/ανακοίνωσης μιας παραβίασης, αυτό δεν απαιτείται να γίνεται σε όλες τις περιστάσεις:

- Απαιτείται γνωστοποίηση στην αρμόδια εποπτική αρχή, εκτός εάν η παραβίαση δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων.
- Η ανακοίνωση μιας παραβίασης στο πρόσωπο πρέπει να γίνεται μόνο εάν η παραβίαση ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες του.

Αυτό σημαίνει ότι, αμέσως μόλις λάβει γνώση μιας παραβίασης, είναι ζωτικής σημασίας ο υπεύθυνος επεξεργασίας να επιδιώκει τον περιορισμό του συμβάντος, ωστόσο θα πρέπει επίσης να αξιολογεί τον κίνδυνο που θα μπορούσε να προκύψει από το συμβάν. Ο υπεύθυνος επεξεργασίας πρέπει να προβαίνει στις παραπάνω ενέργειες για δύο σημαντικούς λόγους: πρώτον, γνωρίζοντας τις πιθανότητες και τη δυνητική σοβαρότητα του αντικτύπου στο πρόσωπο, ο υπεύθυνος επεξεργασίας θα μπορέσει να προβεί σε αποτελεσματικές ενέργειες για τον περιορισμό και την αντιμετώπιση της παραβίασης· δεύτερον, θα βοηθηθεί ώστε να προσδιορίσει εάν απαιτείται γνωστοποίηση στην εποπτική αρχή και, εάν είναι απαραίτητο, ανακοίνωση στα ενδιαφερόμενα πρόσωπα.

Όπως επεξηγείται παραπάνω, η γνωστοποίηση μιας παραβίασης είναι αναγκαία, εκτός εάν δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων και ο βασικός παράγοντας που δημιουργεί την ανάγκη για ανακοίνωση μιας παραβίασης στα υποκείμενα των δεδομένων είναι η πιθανότητα αυτή η παραβίαση να επιφέρει *υψηλό* κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων. Αυτός ο κίνδυνος υφίσταται όταν η παραβίαση ενδέχεται να οδηγήσει σε σωματική, υλική ή ηθική βλάβη για τα πρόσωπα τα δεδομένων των οποίων έχουν παραβιαστεί. Παραδείγματα τέτοιας βλάβης είναι οι διακρίσεις, η κατάχρηση ή υποκλοπή ταυτότητας, η οικονομική απώλεια και η βλάβη φήμης. Όταν η παραβίαση αφορά δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα ή περιλαμβάνει δεδομένα που αφορούν την

[38] Βλ. άρθρο 5 παράγραφος 2.

υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας, αυτή η βλάβη θα πρέπει να θεωρείται πιθανό να επέλθει[39].

ΙΒ. Παράγοντες που πρέπει να λαμβάνονται υπόψη κατά την αξιολόγηση κινδύνου

Σύμφωνα με τις αιτιολογικές σκέψεις 75 και 76 του ΓΚΠΔ, εν γένει, κατά την αξιολόγηση του κινδύνου θα πρέπει να λαμβάνονται υπόψη η πιθανότητα και η σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Αναφέρεται επίσης ότι ο κίνδυνος θα πρέπει να αξιολογείται βάσει αντικειμενικής εκτίμησης.

Θα πρέπει να σημειωθεί ότι, κατά την αξιολόγηση του κινδύνου για τα δικαιώματα και τις ελευθερίες των προσώπων ως αποτέλεσμα μιας παραβίασης, η εστίαση στον κίνδυνο που εξετάζεται στο πλαίσιο μιας ΕΑΠΔ είναι διαφορετική[40]. Στο πλαίσιο μιας ΕΑΠΔ, εξετάζονται τόσο οι κίνδυνοι της επεξεργασίας των δεδομένων που πραγματοποιείται όπως έχει προβλεφθεί όσο και οι κίνδυνοι σε περίπτωση παραβίασης. Κατά τη διερεύνηση του ενδεχομένου παραβίασης, εξετάζονται σε γενικές γραμμές η πιθανότητα να σημειωθεί παραβίαση και η βλάβη που μπορεί να προκύψει για το υποκείμενο των δεδομένων. Δηλαδή, πρόκειται για την αξιολόγηση ενός υποθετικού συμβάντος. Όταν πρόκειται για πραγματική παραβίαση, το συμβάν έχει ήδη προκύψει και, συνεπώς, η προσοχή εστιάζεται αποκλειστικά στον κίνδυνο που απορρέει από τις συνέπειες της παραβίασης για τα πρόσωπα.

Παράδειγμα

Σύμφωνα με μια ΕΑΠΔ, η προτεινόμενη χρήση ενός συγκεκριμένου λογισμικού ασφάλειας για την προστασία των δεδομένων είναι ένα κατάλληλο μέτρο προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων που θα επέφερε η επεξεργασία για τα πρόσωπα σε διαφορετική περίπτωση. Ωστόσο, εάν σε μεταγενέστερο στάδιο καταστεί γνωστό ένα τρωτό σημείο, το γεγονός αυτό θα έχει επίπτωση στην καταλληλότητα του λογισμικού όσον αφορά τον περιορισμό του κινδύνου για τα δεδομένα προσωπικού χαρακτήρα που προστατεύονται και, συνεπώς, θα χρήζει εκ νέου αξιολόγησης στο πλαίσιο μιας συνεχούς ΕΑΠΔ.

Κάποιος εκμεταλλεύεται στη συνέχεια ένα τρωτό σημείο του προϊόντος και προκύπτει μια παραβίαση. Ο υπεύθυνος επεξεργασίας θα πρέπει να αξιολογεί τις ειδικές περιστάσεις της παραβίασης, τα επηρεαζόμενα δεδομένα και το ενδεχόμενο επίπεδο αντικτύπου στα πρόσωπα, καθώς και πόσο πιθανό είναι ο αυτός ο κίνδυνος να προκύψει.

Συνεπώς, κατά την αξιολόγηση του κινδύνου για τα πρόσωπα ως αποτέλεσμα μιας παραβίασης, ο υπεύθυνος επεξεργασίας θα πρέπει να εξετάζει τις ειδικές περιστάσεις της παραβίασης, συμπεριλαμβανομένων της σοβαρότητας του πιθανού αντικτύπου και της πιθανότητας να προκύψει. Συνεπώς, η ΟΕ29 συνιστά κατά την αξιολόγηση να λαμβάνονται υπόψη τα ακόλουθα κριτήρια[41]:

- Το είδος της παραβίασης

[39] Βλ. αιτιολογική σκέψη 75 και αιτιολογική σκέψη 85.

[40] Βλ. κατευθυντήριες γραμμές της ΟΕ για τις ΕΑΠΔ εδώ: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[41] Το άρθρο 3.2 του κανονισμού (ΕΕ) αριθ. 611/2013 παρέχει καθοδήγηση όσον αφορά τους παράγοντες που θα πρέπει να λαμβάνονται υπόψη σε σχέση με την κοινοποίηση παραβιάσεων στον τομέα των υπηρεσιών ηλεκτρονικών επικοινωνιών, η οποία μπορεί να είναι χρήσιμη στο πλαίσιο της γνωστοποίησης δυνάμει του ΓΚΠΔ. Βλ. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:el:PDF

Το είδος της παραβίασης που έχει προκύψει μπορεί να επηρεάζει το επίπεδου του κινδύνου για τα πρόσωπα. Για παράδειγμα, μια παραβίαση της εμπιστευτικότητας όπου ιατρικές πληροφορίες έχουν κοινοποιηθεί σε μη εξουσιοδοτημένα μέρη ενδέχεται να έχει διάφορες συνέπειες για ένα πρόσωπο σε σύγκριση με μια παραβίαση όπου τα ιατρικά στοιχεία ενός προσώπου έχουν χαθεί και δεν είναι πλέον διαθέσιμα.

- Η φύση, η ευαισθησία και ο όγκος των δεδομένων προσωπικού χαρακτήρα

Εξυπακούεται ότι, κατά την αξιολόγηση του κινδύνου, ένας βασικός παράγοντας είναι το είδος και η ευαισθησία των δεδομένων προσωπικού χαρακτήρα που έχουν τεθεί σε κίνδυνο λόγω της παραβίασης. Συνήθως, όσο μεγαλύτερος είναι ο βαθμός ευαισθησίας των δεδομένων, τόσο υψηλότερος θα είναι ο κίνδυνος βλάβης για τα επηρεαζόμενα πρόσωπα, ωστόσο θα πρέπει να λαμβάνονται επίσης υπόψη άλλα δεδομένα προσωπικού χαρακτήρα που ενδέχεται να είναι διαθέσιμα σχετικά με το υποκείμενο των δεδομένων. Για παράδειγμα, η κοινοποίηση του ονόματος και της διεύθυνσης ενός προσώπου υπό συνήθεις περιστάσεις είναι απίθανο να προκαλέσει σοβαρή βλάβη. Ωστόσο, εάν το όνομα και η διεύθυνση ενός θετού γονέα κοινοποιηθεί σε έναν βιολογικό γονέα, οι συνέπειες θα μπορούσαν να είναι πολύ σοβαρές τόσο για τον θετό γονέα όσο και το παιδί.

Οι παραβιάσεις που αφορούν δεδομένα υγείας, έγγραφα ταυτότητας ή οικονομικά δεδομένα, όπως στοιχεία πιστωτικών καρτών, μπορούν να προκαλέσουν βλάβη από μόνες τους, αλλά, εάν χρησιμοποιηθούν συνδυαστικά, θα μπορούσαν να χρησιμοποιηθούν για την υποκλοπή ταυτότητας. Ένας συνδυασμός δεδομένων προσωπικού χαρακτήρα παρουσιάζει συνήθως μεγαλύτερη ευαισθησία από ένα μόνο δεδομένο προσωπικού χαρακτήρα.

Ορισμένα είδη δεδομένων προσωπικού χαρακτήρα ενδέχεται να φαίνονται εκ πρώτης όψεως σχετικά αθώα, ωστόσο θα πρέπει να εξετάζεται προσεκτικά τι θα μπορούσαν αυτά τα δεδομένα να αποκαλύψουν σχετικά με το επηρεαζόμενο πρόσωπο. Ένας κατάλογος πελατών που λαμβάνουν τακτικά παραδόσεις ενδέχεται να μην παρουσιάζει ιδιαίτερη ευαισθησία, ωστόσο τα ίδια δεδομένα σχετικά με πελάτες που έχουν ζητήσει τη διακοπή των παραδόσεών τους ενόσω βρίσκονται σε διακοπές θα αποτελούσαν πληροφορίες χρήσιμες για εγκληματίες.

Αντίστοιχα, ένας μικρός όγκος πολύ ευαίσθητων δεδομένων προσωπικού χαρακτήρα μπορεί να έχει μεγάλο αντίκτυπο σε ένα πρόσωπο και ένα μεγάλο φάσμα λεπτομερειών μπορεί να αποκαλύψει ένα μεγαλύτερο φάσμα πληροφοριών σχετικά με το συγκεκριμένο πρόσωπο. Επίσης, μια παραβίαση που επηρεάζει μεγάλους όγκους δεδομένων προσωπικού χαρακτήρα τα οποία αφορούν μεγάλο αριθμό υποκειμένων των δεδομένων μπορεί να έχει επιπτώσεις σε ένα αντίστοιχα μεγάλο αριθμό προσώπων.

- Η ευκολία ταυτοποίησης των προσώπων

Ένας σημαντικός παράγοντας που πρέπει να εξετάζεται είναι ο βαθμός ευκολίας για ένα πρόσωπο έχει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που έχουν τεθεί σε κίνδυνο να εξακριβώσει την ταυτότητα συγκεκριμένων προσώπων ή να αντιστοιχίσει τα δεδομένα με άλλες πληροφορίες για να εξακριβώσει την ταυτότητα προσώπων. Ανάλογα με τις περιστάσεις, η εξακρίβωση της ταυτότητας θα μπορούσε να είναι δυνατή απευθείας από τα δεδομένα προσωπικού χαρακτήρα χωρίς να απαιτείται ειδική έρευνα για την ανακάλυψη της ταυτότητας του προσώπου ή ενδέχεται τα δεδομένα προσωπικού χαρακτήρα να είναι εξαιρετικά δύσκολο να αντιστοιχιστούν σε ένα συγκεκριμένο πρόσωπο, ωστόσο η εν λόγω αντιστοίχιση εξακολουθεί να είναι δυνατή υπό ορισμένες συνθήκες. Η εξακρίβωση της ταυτότητας ενδέχεται να είναι άμεσα ή έμμεσα δυνατή από τα δεδομένα που έχουν παραβιαστεί, ωστόσο ενδέχεται επίσης να εξαρτάται από το ειδικό πλαίσιο της παραβίασης και τη διαθεσιμότητα των σχετικών προσωπικών στοιχείων στο κοινό. Αυτό μπορεί να αφορά περισσότερο τις παραβιάσεις εμπιστευτικότητας και διαθεσιμότητας.

Όπως αναφέρεται παραπάνω, τα δεδομένα προσωπικού χαρακτήρα που προστατεύονται με κατάλληλο επίπεδο κρυπτογράφησης θα είναι μη κατανοητά σε μη εξουσιοδοτημένα άτομα που δεν διαθέτουν το κλειδί αποκρυπτογράφησης. Επιπλέον, η ψευδωνυμοποίηση που εφαρμόζεται με τον

κατάλληλο τρόπο [ορίζεται στο άρθρο 4 σημείο 5) ως «η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο»] μπορεί επίσης να μειώσει τις πιθανότητες εξακρίβωσης της ταυτότητας προσώπων σε περίπτωση παραβίασης. Ωστόσο, οι τεχνικές ψευδωνυμοποίησης από μόνες τους δεν μπορούν να θεωρείται ότι καθιστούν τα δεδομένα μη κατανοητά.

- Η σοβαρότητα των συνεπειών για τα πρόσωπα

Ανάλογα με τη φύση των δεδομένων προσωπικού χαρακτήρα που αφορά η παραβίαση, για παράδειγμα, ειδικές κατηγορίες δεδομένων, η ενδεχόμενη βλάβη για τα πρόσωπα που θα μπορούσε να προκύψει μπορεί να είναι ιδιαίτερα σοβαρή, ιδίως όταν η παραβίαση θα μπορούσε να οδηγήσει σε κατάχρηση ή υποκλοπή ταυτότητας, σωματική βλάβη, ψυχολογική οδύνη, εξευτελισμό ή βλάβη φήμης. Εάν η παραβίαση αφορά δεδομένα προσωπικού χαρακτήρα σχετικά με ευάλωτα πρόσωπα, αυτά τα πρόσωπα θα μπορούσαν να διατρέχουν μεγαλύτερο κίνδυνο βλάβης.

Το εάν ο υπεύθυνος επεξεργασίας γνωρίζει ότι τα δεδομένα προσωπικού χαρακτήρα βρίσκονται στα χέρια ατόμων με άγνωστες ή πιθανώς κακόβουλες προθέσεις μπορεί να επηρεάζει το επίπεδο του ενδεχόμενου κινδύνου. Ενδέχεται να πρόκειται για παραβίαση της εμπιστευτικότητας, όπου δεδομένα προσωπικού χαρακτήρα έχουν κοινοποιηθεί σε τρίτον, όπως αυτός ορίζεται στο άρθρο 4 σημείο 10), ή σε άλλον εσφαλμένο αποδέκτη. Αυτό μπορεί να συμβεί, για παράδειγμα, όταν δεδομένα προσωπικού χαρακτήρα αποσταλούν τυχαία σε εσφαλμένο τμήμα ενός οργανισμού ή σε έναν οργανισμό-προμηθευτή που χρησιμοποιείται ευρέως. Ο υπεύθυνος επεξεργασίας δύναται να ζητήσει από τον αποδέκτη είτε να επιστρέψει είτε να καταστρέψει με ασφάλεια τα δεδομένα που έχει λάβει. Σε αμφότερες τις περιπτώσεις, δεδομένου ότι ο υπεύθυνος επεξεργασίας έχει μια συνεχή σχέση μαζί του και μπορεί να γνωρίζει τις διαδικασίες και το ιστορικό του, καθώς και άλλες σχετικές λεπτομέρειες, ο αποδέκτης μπορεί να θεωρηθεί «έμπιστος». Με άλλα λόγια, μπορεί να υπάρχει ένα επίπεδο εμπιστοσύνης μεταξύ του υπευθύνου επεξεργασίας και του αποδέκτη, ώστε να μπορεί να αναμένεται ευλόγως ότι αυτό το μέρος δεν θα διαβάσει ούτε θα προσπελάσει τα δεδομένα που απεστάλησαν εκ παραδρομής και θα συμμορφωθεί με τις οδηγίες για την επιστροφή τους. Ακόμη και αν τα δεδομένα έχουν προσπελαστεί, ο υπεύθυνος επεξεργασίας θα μπορούσε πιθανώς να εξακολουθήσει να έχει εμπιστοσύνη στον αποδέκτη και να θεωρεί ότι δεν θα προβεί σε καμία άλλη ενέργεια μ' αυτά, θα επιστρέψει άμεσα τα δεδομένα στον υπεύθυνο επεξεργασίας και θα συνεργαστεί για την ανάκτησή τους. Σε τέτοιες περιπτώσεις, αυτό μπορεί να συνεκτιμάται στην αξιολόγηση κινδύνου που διενεργεί ο υπεύθυνος επεξεργασίας μετά την παραβίαση – το γεγονός ότι ο αποδέκτης είναι έμπιστος ενδέχεται να εξαλείψει τη σοβαρότητα των συνεπειών της παραβίασης, αλλά δεν σημαίνει ότι δεν έχει σημειωθεί παραβίαση. Ωστόσο, αυτό με τη σειρά του μπορεί να εξαλείψει την πιθανότητα κινδύνου για τα πρόσωπα και, συνακόλουθα, να μην απαιτηθεί η γνωστοποίηση στην εποπτική αρχή ή η ανακοίνωση στα επηρεαζόμενα πρόσωπα. Ωστόσο, αυτό εξαρτάται από την εκάστοτε περίπτωση. Εντούτοις, ο υπεύθυνος επεξεργασίας εξακολουθεί να πρέπει να τηρεί τις πληροφορίες σχετικά με την παραβίαση στο πλαίσιο του γενικού καθήκοντος να τηρεί αρχεία των παραβιάσεων (βλ. ενότητα V παρακάτω).

Θα πρέπει να λαμβάνεται επίσης υπόψη ο μόνιμος χαρακτήρας των συνεπειών για τα πρόσωπα στις περιπτώσεις όπου ο αντίκτυπος μπορεί να θεωρείται μεγαλύτερος εάν οι συνέπειες είναι μακροχρόνιες.

- Τα ειδικά χαρακτηριστικά του προσώπου

Μια παραβίαση μπορεί να επηρεάσει δεδομένα προσωπικού χαρακτήρα που αφορούν παιδιά ή άλλα ευάλωτα πρόσωπα, τα οποία ενδέχεται να διατρέχουν μεγαλύτερο κίνδυνο. Ενδέχεται να υπάρχουν

άλλοι παράγοντες σχετικά με το πρόσωπο που να επηρεάζουν το επίπεδο του αντικτύπου μιας παραβίασης γι' αυτό.

- Τα ειδικά χαρακτηριστικά του υπευθύνου επεξεργασίας δεδομένων

Η φύση και ο ρόλος του υπευθύνου επεξεργασίας και οι δραστηριότητές του ενδέχεται να επηρεάζουν το επίπεδο κινδύνου για τα πρόσωπα ως αποτέλεσμα μιας παραβίασης. Για παράδειγμα, ένας ιατρικός οργανισμός επεξεργάζεται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, γεγονός που σημαίνει ότι υπάρχει μεγαλύτερη απειλή για τα πρόσωπα σε περίπτωση παραβίασης των δεδομένων προσωπικού χαρακτήρα τους, σε σύγκριση με έναν κατάλογο ηλεκτρονικών διευθύνσεων μιας εφημερίδας.

- Ο αριθμός των επηρεαζόμενων προσώπων

Μια παραβίαση μπορεί να επηρεάζει μόνο ένα πρόσωπο ή μικρό αριθμό προσώπων ή και μερικές χιλιάδες, εάν όχι περισσότερα. Σε γενικές γραμμές, όσο υψηλότερος είναι ο αριθμός των επηρεαζόμενων προσώπων, τόσο μεγαλύτερο αντίκτυπο μπορεί να έχει μια παραβίαση. Ωστόσο, μια παραβίαση μπορεί να έχει σοβαρό αντίκτυπο ακόμη και σε ένα πρόσωπο, ανάλογα με τη φύση των δεδομένων προσωπικού χαρακτήρα και το πλαίσιο εντός του οποίου έχουν τεθεί σε κίνδυνο. Και πάλι, το βασικό είναι να εξετάζονται η πιθανότητα και η σοβαρότητα του αντικτύπου σ' αυτά τα επηρεαζόμενα πρόσωπα.

- Γενικές παρατηρήσεις

Ως εκ τούτου, κατά την αξιολόγηση του κινδύνου που είναι πιθανό να επιφέρει μια παραβίαση, ο υπεύθυνος επεξεργασίας θα πρέπει να εξετάζει συνδυαστικά τη σοβαρότητα του πιθανού αντικτύπου στα δικαιώματα και στις ελευθερίες των προσώπων και την πιθανότητα επέλευσής του. Σαφώς, όταν οι συνέπειες μιας παραβίασης είναι πιο σοβαρές, ο κίνδυνος είναι υψηλότερος και, αντίστοιχα, όταν η πιθανότητα αυτές οι συνέπειες να προκύψουν είναι μεγαλύτερη, ο κίνδυνος είναι επίσης υψηλότερος. Εάν έχει αμφιβολία, ο υπεύθυνος επεξεργασίας θα πρέπει να επιδείξει ιδιαίτερη προσοχή και να προβεί σε γνωστοποίηση. Το παράρτημα Β παρέχει ορισμένα χρήσιμα παραδείγματα διαφόρων ειδών παραβιάσεων που συνεπάγονται κίνδυνο ή υψηλό κίνδυνο για τα πρόσωπα.

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) έχει διατυπώσει συστάσεις για μια μεθοδολογία αξιολόγησης της σοβαρότητας μιας παραβίασης, η οποία ενδέχεται να φανεί χρήσιμη στους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία κατά τον σχεδιασμό των σχεδίων διαχείρισης παραβιάσεων[42].

V. **Λογοδοσία και τήρηση αρχείων**

ΙΓ. Τεκμηρίωση των παραβιάσεων

Ανεξάρτητα από το εάν μια παραβίαση πρέπει να γνωστοποιηθεί στην εποπτική αρχή ή όχι, ο υπεύθυνος επεξεργασίας πρέπει να τηρεί αρχεία τεκμηρίωσης όλων των παραβιάσεων, όπως εξηγείται στο άρθρο 33 παράγραφος 5:

«Ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού

[42] ENISA, Συστάσεις για μια μεθοδολογία αξιολόγησης της σοβαρότητας των παραβιάσεων δεδομένων προσωπικού χαρακτήρα, https://www.enisa.europa.eu/publications/dbn-severity

χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην εποπτική αρχή να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο.»

Αυτό συνδέεται με την αρχή της λογοδοσίας του ΓΚΠΔ που προβλέπεται στο άρθρο 5 παράγραφος 2. Ο σκοπός της καταγραφής μη γνωστοποιήσιμων αλλά και γνωστοποιήσιμων παραβιάσεων συνδέεται επίσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας δυνάμει του άρθρου 24 και η εποπτική αρχή μπορεί να ζητήσει να δει αυτά τα αρχεία. Οι υπεύθυνοι επεξεργασίας ενθαρρύνονται, συνεπώς, να δημιουργούν ένα εσωτερικό μητρώο παραβιάσεων, ανεξάρτητα από το εάν απαιτείται να τις γνωστοποιήσουν ή όχι[43].

Παρότι εναπόκειται στον υπεύθυνο επεξεργασίας να καθορίζει τη μέθοδο και τη δομή που θα χρησιμοποιεί κατά την τεκμηρίωση μιας παραβίασης, υπάρχουν ορισμένα βασικά στοιχεία που θα πρέπει να περιλαμβάνονται σε κάθε περίπτωση όσον αφορά τις πληροφορίες που πρέπει να καταγράφονται. Όπως απαιτείται από το άρθρο 33 παράγραφος 5, ο υπεύθυνος επεξεργασίας πρέπει να καταγράφει λεπτομέρειες σχετικά με την παραβίαση, οι οποίες θα πρέπει να περιλαμβάνουν τις αιτίες της, τι συνέβη και τα δεδομένα προσωπικού χαρακτήρα που επηρεάζονται. Θα πρέπει να περιλαμβάνουν επίσης τα αποτελέσματα και τις συνέπειες της παραβίασης, μαζί με τα διορθωτικά μέτρα που έλαβε ο υπεύθυνος επεξεργασίας.

Ο ΓΚΠΔ δεν προσδιορίζει κάποιο χρονικό διάστημα διατήρησης αυτής της τεκμηρίωσης. Όταν αυτά τα αρχεία περιέχουν δεδομένα προσωπικού χαρακτήρα, θα εναπόκειται στον υπεύθυνο επεξεργασίας να καθορίζει το κατάλληλο χρονικό διάστημα διατήρησης σύμφωνα με τις αρχές που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα[44] και να προβαίνει στην επεξεργασία επί νόμιμης βάσης[45]. Θα πρέπει να τηρεί τεκμηρίωση σύμφωνα με το άρθρο 33 παράγραφος 5 στον βαθμό που ενδέχεται να κληθεί να παράσχει στην εποπτική αρχή στοιχεία συμμόρφωσης με το εν λόγω άρθρο ή με την αρχή λογοδοσίας γενικότερα. Είναι σαφές ότι, εάν τα ίδια τα αρχεία δεν περιέχουν δεδομένα προσωπικού χαρακτήρα, η αρχή περιορισμού της περιόδου αποθήκευσης[46] του ΓΚΠΔ δεν ισχύει.

Εκτός από αυτές τις λεπτομέρειες, η ΟΕ29 συνιστά ο υπεύθυνος επεξεργασίας να καταγράφει επίσης το σκεπτικό του για τις αποφάσεις που λαμβάνει για την αντιμετώπιση μιας παραβίασης. Πιο συγκεκριμένα, εάν μια παραβίαση δεν γνωστοποιηθεί, θα πρέπει να καταγράφεται μια τεκμηριωμένη αιτιολόγηση γι' αυτή την απόφαση. Αυτή η αιτιολόγηση θα πρέπει να περιλαμβάνει τους λόγους για τους οποίους ο υπεύθυνος επεξεργασίας θεωρεί ότι η παραβίαση δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων[47]. Εναλλακτικά, εάν ο υπεύθυνος επεξεργασίας θεωρεί ότι πληρούται οποιαδήποτε από τις προϋποθέσεις του άρθρου 34 παράγραφος 3, θα πρέπει να είναι σε θέση να παράσχει τα κατάλληλα αποδεικτικά στοιχεία.

Όταν ο υπεύθυνος επεξεργασίας γνωστοποιεί μια παραβίαση στην εποπτική αρχή αλλά η γνωστοποίηση είναι καθυστερημένη, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να παράσχει τους λόγους αυτής της καθυστέρησης· η σχετική τεκμηρίωση θα μπορούσε να συμβάλει ώστε να αποδειχθεί ότι η καθυστέρηση στην αναφορά είναι αιτιολογημένη και όχι υπερβολική.

[43] Ο υπεύθυνος επεξεργασίας μπορεί να επιλέξει να καταγράφει τις παραβιάσεις στο αρχείο των δραστηριοτήτων επεξεργασίας που τηρεί σύμφωνα με το άρθρο 30. Δεν απαιτείται η τήρηση ξεχωριστού μητρώου, υπό την προϋπόθεση ότι οι πληροφορίες που αφορούν την παραβίαση είναι σαφώς αναγνωρίσιμες και μπορούν να εξαχθούν κατόπιν αιτήματος.

[44] Βλ. άρθρο 5.

[45] Βλ. άρθρο 6 και επίσης άρθρο 9.

[46] Βλ. άρθρο 5 παράγραφος 1 στοιχείο ε).

[47] Βλ. αιτιολογική σκέψη 85.

Όταν ο υπεύθυνος επεξεργασίας ανακοινώνει μια παραβίαση στα επηρεαζόμενα πρόσωπα, θα πρέπει να σαφής όσον αφορά την παραβίαση και να την ανακοινώνει κατά τρόπο αποτελεσματικό και εγκαίρως. Συνεπώς, η τήρηση στοιχείων αυτής της ανακοίνωσης θα βοηθούσε τον υπεύθυνο επεξεργασίας να καταδεικνύει τη λογοδοσία και τη συμμόρφωση.

Για τη διευκόλυνση της συμμόρφωσης με τα άρθρα 33 και 34, θα ήταν επωφελές τόσο για τους υπευθύνους επεξεργασίας όσο και για τους εκτελούντες την επεξεργασία να διαθέτουν διαδικασία τεκμηριωμένης γνωστοποίησης, η οποία θα περιγράφει τα βήματα που πρέπει να γίνονται μετά τον εντοπισμό μιας παραβίασης και, μεταξύ άλλων, τον τρόπο περιορισμού, διαχείρισης και αποκατάστασης του συμβάντος, καθώς και τον τρόπο αξιολόγησης του κινδύνου και γνωστοποίησης της παραβίασης. Προς αυτό τον σκοπό, για να καταδεικνύεται η συμμόρφωση με τον ΓΚΠΔ, μπορεί να είναι χρήσιμο να αποδεικνύεται ότι οι εργαζόμενοι έχουν ενημερωθεί σχετικά την ύπαρξη αυτών των διαδικασιών και μηχανισμών και ότι γνωρίζουν πώς να διαχειρίζονται παραβιάσεις.

Θα πρέπει να σημειωθεί ότι η μη κατάλληλη τεκμηρίωση μιας παραβίασης μπορεί να οδηγήσει στην άσκηση από τον εποπτική αρχή των εξουσιών της δυνάμει του άρθρου 58 ή στην επιβολή από αυτήν διοικητικού προστίμου σύμφωνα με το άρθρο 83.

ΙΔ. Ο ρόλος του υπευθύνου προστασίας δεδομένων

Ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία μπορεί να έχει έναν υπεύθυνο προστασίας δεδομένων[48], είτε όπως απαιτείται από το άρθρο 37 είτε οικειοθελώς ως ορθή πρακτική. Το άρθρο 39 του ΓΚΠΔ ορίζει μια σειρά υποχρεωτικών καθηκόντων για τον υπεύθυνο προστασίας δεδομένων, ωστόσο δεν αποτρέπει την ανάθεση περαιτέρω καθηκόντων από τον υπεύθυνο επεξεργασίας, κατά περίπτωση.

Τα υποχρεωτικά καθήκοντα του υπευθύνου προστασίας δεδομένων, που έχουν ιδιαίτερη συνάφεια με τη γνωστοποίηση της παραβίασης, περιλαμβάνουν, μεταξύ άλλων, την παροχή συμβουλών και πληροφοριών για την προστασία των δεδομένων στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία, την παρακολούθηση της συμμόρφωσης με τον ΓΚΠΔ και την παροχή συμβουλών όσον αφορά τις ΕΑΠΔ. Ο υπεύθυνος προστασίας δεδομένων πρέπει επίσης να συνεργάζεται με την εποπτική αρχή και να λειτουργεί ως σημείο επαφής για την εποπτική αρχή και τα υποκείμενα των δεδομένων. Θα πρέπει να σημειωθεί επίσης ότι, κατά τη γνωστοποίηση της παραβίασης στην εποπτική αρχή, το άρθρο 33 παράγραφος 3 στοιχείο β) απαιτεί από τον υπεύθυνο επεξεργασίας να παρέχει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων του ή άλλου σημείου επικοινωνίας.

Όσον αφορά την τεκμηρίωση των παραβιάσεων, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί να επιθυμεί να λάβει τη γνώμη του υπευθύνου προστασίας δεδομένων του όσον αφορά τη δομή, την ανάπτυξη και τη διαχείριση αυτής της τεκμηρίωσης. Ο υπεύθυνος προστασίας δεδομένων θα μπορούσε να αναλαμβάνει επιπροσθέτως την τήρηση τέτοιων αρχείων.

Αυτοί οι παράγοντες σημαίνουν ότι ο υπεύθυνος προστασίας δεδομένων μπορεί να διαδραματίζει σημαντικό ρόλο ως προς την αποτροπή μιας παραβίασης ή την προετοιμασία για την αντιμετώπιση μιας παραβίασης, παρέχοντας συμβουλές και παρακολουθώντας τη συμμόρφωση, καθώς και κατά τη διάρκεια μιας παραβίασης (δηλαδή κατά τη γνωστοποίηση στην εποπτική αρχή) και κατά τη διάρκεια οποιασδήποτε μεταγενέστερης έρευνας από την εποπτική αρχή. Υπό το πρίσμα των ανωτέρω, η ΟΕ29 συνιστά ο υπεύθυνος προστασίας δεδομένων να ενημερώνεται άμεσα σχετικά με την ύπαρξη παραβίασης και να συμμετέχει στη διαδικασία διαχείρισης και γνωστοποίησης της παραβίασης.

[48] Βλ. κατευθυντήριες γραμμές της ΟΕ σχετικά με τους υπεύθυνους προστασίας δεδομένων εδώ: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

VI. Υποχρεώσεις γνωστοποίησης βάσει άλλων νομικών πράξεων

Εκτός από τη γνωστοποίηση και την ανακοίνωση παραβιάσεων δυνάμει του ΓΚΠΔ, και ξεχωριστά από αυτές, οι υπεύθυνοι επεξεργασίας θα πρέπει να γνωρίζουν επίσης οποιαδήποτε απαίτηση γνωστοποίησης συμβάντων ασφάλειας βάσει άλλης σχετικής νομοθεσίας στην οποία υπόκεινται, καθώς και εάν, σύμφωνα με την εν λόγω νομοθεσία, υποχρεούνται να γνωστοποιούν στην εποπτική αρχή μια παραβίαση δεδομένων προσωπικού χαρακτήρα. Αυτές οι απαιτήσεις μπορούν να διαφέρουν μεταξύ των κρατών μελών, ωστόσο παραδείγματα απαιτήσεων γνωστοποίησης που προβλέπονται σε άλλες νομικές πράξεις και του τρόπου με τον οποίο συνδέονται με τον ΓΚΠΔ περιλαμβάνουν τα εξής:

- Κανονισμός (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (κανονισμός eIDAS)[49].

Το άρθρο 19 παράγραφος 2 του κανονισμού eIDAS απαιτεί από τους παρόχους υπηρεσιών εμπιστοσύνης να ενημερώνουν τον εποπτικό φορέα για οποιαδήποτε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας που έχει σημαντικό αντίκτυπο στην παρεχόμενη υπηρεσία εμπιστοσύνης ή στα σχετικά δεδομένα προσωπικού χαρακτήρα. Κατά περίπτωση –δηλαδή όταν αυτή η παραβίαση ή απώλεια συνιστά επίσης παραβίαση δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον ΓΚΠΔ–, ο πάροχος υπηρεσιών εμπιστοσύνης θα πρέπει επίσης να ενημερώνει την εποπτική αρχή.

- Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (οδηγία ΑΔΠ)[50].

Τα άρθρα 14 και 16 της οδηγίας ΑΔΠ απαιτούν από τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών να κοινοποιούν στην αρμόδια αρχή τα συμβάντα ασφάλειας. Όπως αναγνωρίζεται από την αιτιολογική σκέψη 63 της οδηγίας ΑΔΠ[51], τα συμβάντα ασφάλειας μπορούν συχνά να περιλαμβάνουν την έκθεση δεδομένων προσωπικού χαρακτήρα σε κίνδυνο. Παρότι η οδηγία ΑΔΠ απαιτεί από τις αρμόδιες αρχές και τις εποπτικές αρχές να συνεργάζονται και να ανταλλάσσουν πληροφορίες, όταν αυτά τα συμβάντα είναι ή καθίστανται παραβιάσεις δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον ΓΚΠΔ, αυτοί οι φορείς εκμετάλλευσης και/ή πάροχοι εξακολουθούν να πρέπει να ενημερώνουν την εποπτική αρχή ξεχωριστά από τις απαιτήσεις γνωστοποίησης συμβάντων της οδηγίας ΑΔΠ.

Παράδειγμα

Ένας πάροχος υπηρεσιών υπολογιστικού νέφους που γνωστοποιεί μια παραβίαση σύμφωνα με την οδηγία ΑΔΠ μπορεί επίσης να οφείλει να ενημερώσει έναν υπεύθυνο επεξεργασίας, εάν η παραβίαση περιλαμβάνει και παραβίαση δεδομένων προσωπικού χαρακτήρα. Ομοίως, ένας πάροχος υπηρεσιών εμπιστοσύνης που προβαίνει σε γνωστοποίηση σύμφωνα με τον κανονισμό eIDAS ενδέχεται επίσης να πρέπει να ενημερώσει την αρμόδια αρχή προστασίας δεδομένων σε περίπτωση παραβίασης.

- Οδηγία 2009/136/ΕΚ (οδηγία για τα δικαιώματα των πολιτών) και κανονισμός (ΕΕ) αριθ. 611/2013 (κανονισμός για την κοινοποίηση παραβιάσεων).

[49] Βλ. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32014R0910

[50] Βλ. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016L1148

51 Αιτιολογική σκέψη 63: *«Ως αποτέλεσμα συμβάντων, σε πολλές περιπτώσεις διακυβεύονται δεδομένα προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, οι αρμόδιες αρχές και οι αρχές προστασίας δεδομένων πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες για όλα τα συναφή θέματα με σκοπό την αντιμετώπιση των παραβιάσεων δεδομένων προσωπικού χαρακτήρα οι οποίες οφείλονται σε συμβάντα.»*

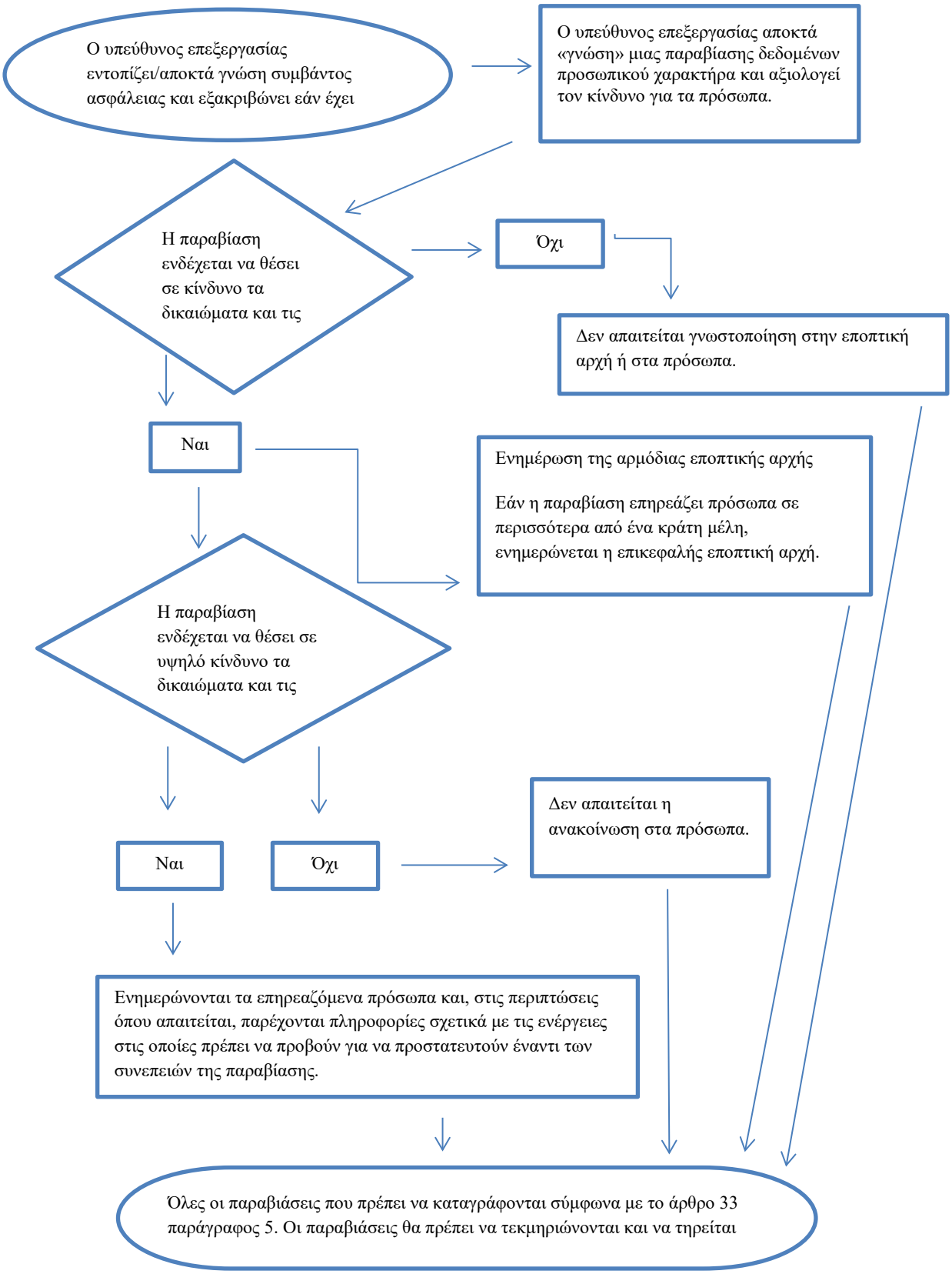
Οι πάροχοι υπηρεσιών διαθέσιμων στο κοινό ηλεκτρονικών επικοινωνιών υπό την έννοια της οδηγίας 2002/58/ΕΚ[52] πρέπει να γνωστοποιούν τις παραβιάσεις στις αρμόδιες εθνικές αρχές.

Οι υπεύθυνοι επεξεργασίας θα πρέπει να είναι ενήμεροι για οποιαδήποτε πρόσθετα καθήκοντα γνωστοποίησης νομικής, ιατρικής ή επαγγελματικής φύσεως βάσει άλλων εφαρμοστέων καθεστώτων.

[52] Στις 10 Ιανουαρίου 2017, η Ευρωπαϊκή Επιτροπή πρότεινε έναν κανονισμό για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες, ο οποίος θα αντικαταστήσει την οδηγία 2009/136/ΕΚ και θα καταργήσει τις απαιτήσεις γνωστοποίησης. Ωστόσο, μέχρι η πρόταση να εγκριθεί από το Ευρωπαϊκό Κοινοβούλιο, η ισχύουσα απαίτηση γνωστοποίησης παραμένει σε ισχύ, βλ. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Παράρτημα**

ΙΕ. Διάγραμμα ροής που απεικονίζει τις απαιτήσεις γνωστοποίησης



Β. Παραδείγματα παραβιάσεων δεδομένων προσωπικού χαρακτήρα και σε ποιον πρέπει να γίνεται γνωστοποίηση

Τα ακόλουθα ενδεικτικά παραδείγματα θα βοηθήσουν τους υπευθύνους επεξεργασίας ώστε να αποφασίζουν εάν πρέπει να προβαίνουν σε γνωστοποίηση σε διάφορα σενάρια παραβίασης δεδομένων προσωπικού χαρακτήρα. Αυτά τα παραδείγματα μπορεί επίσης να είναι βοηθητικά για τη διάκριση μεταξύ του κινδύνου και του υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των προσώπων.

Παράδειγμα	**Γνωστοποίηση στην εποπτική αρχή;**	**Ανακοίνωση στο υποκείμενο των δεδομένων;**	**Σημειώσεις/συστάσεις**
i. Ένας υπεύθυνος επεξεργασίας αποθήκευσε αντίγραφο ασφαλείας αρχείου δεδομένων προσωπικού χαρακτήρα σε κρυπτογραφημένη μορφή σε κλειδί USB. Το κλειδί εκλάπη κατά τη διάρκεια διάρρηξης.	Όχι.	Όχι.	Εφόσον τα δεδομένα έχουν κρυπτογραφηθεί με αλγόριθμο προηγμένης τεχνολογίας, υπάρχουν αντίγραφα ασφαλείας των δεδομένων, το μοναδικό κλειδί δεν έχει τεθεί σε κίνδυνο και είναι δυνατή η επαναφορά των δεδομένων εγκαίρως, αυτό ενδέχεται να μην συνιστά παραβίαση που πρέπει να αναφερθεί. Ωστόσο, εάν τεθεί σε κίνδυνο σε μεταγενέστερο στάδιο, απαιτείται γνωστοποίηση.
ii. Ένας υπεύθυνος επεξεργασίας διατηρεί μια ηλεκτρονική υπηρεσία. Ως αποτέλεσμα επίθεσης στον κυβερνοχώρο σ' αυτή την υπηρεσία, αποσπώνται δεδομένα προσωπικού χαρακτήρα προσώπων. Ο υπεύθυνος επεξεργασίας έχει πελάτες σε ένα μόνο κράτος μέλος.	Ναι, ενημερώνεται η εποπτική αρχή εάν είναι πιθανό να υπάρχουν συνέπειες για πρόσωπα.	Ναι, ενημερώνονται τα πρόσωπα ανάλογα με τη φύση των δεδομένων προσωπικού χαρακτήρα που επηρεάζονται και εάν η σοβαρότητα των ενδεχόμενων συνεπειών για τα πρόσωπα είναι μεγάλη.	
iii. Σύντομη διακοπή ρεύματος διάρκειας αρκετών λεπτών στο τηλεφωνικό κέντρο υπευθύνου επεξεργασίας έχει ως	Όχι.	Όχι.	Δεν πρόκειται για παραβίαση που πρέπει να γνωστοποιηθεί, ωστόσο δεν παύει να είναι ένα συμβάν που πρέπει να καταγραφεί σύμφωνα με

αποτέλεσμα οι πελάτες να μην μπορούν να καλέσουν τον υπεύθυνο επεξεργασίας και να προσπελάσουν τα αρχεία τους.			το άρθρο 33 παράγραφος 5. Ο υπεύθυνος επεξεργασίας θα πρέπει να τηρεί κατάλληλα αρχεία.
iv. Ένας υπεύθυνος επεξεργασίας έχει υποστεί επίθεση από λυτρισμικό, η οποία είχε ως αποτέλεσμα την κρυπτογράφηση όλων των δεδομένων. Δεν υπάρχουν διαθέσιμα αντίγραφα ασφαλείας και δεν είναι δυνατή η ανάκτηση των δεδομένων. Από την έρευνα κατέστη σαφές ότι η μοναδική λειτουργία του λυτρισμικού ήταν η κρυπτογράφηση των δεδομένων και ότι δεν υπήρχε άλλο κακόβουλο λογισμικό στο σύστημα.	Ναι, το συμβάν αναφέρεται στην εποπτική αρχή, εάν υπάρχουν ενδεχόμενες συνέπειες για τα πρόσωπα, δεδομένου ότι πρόκειται για απώλεια της διαθεσιμότητας.	Ναι, το συμβάν αναφέρεται στα πρόσωπα, ανάλογα με τη φύση των δεδομένων προσωπικού χαρακτήρα που επηρεάζονται και τις ενδεχόμενες συνέπειες της έλλειψης διαθεσιμότητας των δεδομένων, καθώς και άλλες ενδεχόμενες συνέπειες.	Αν υπήρχε διαθέσιμο αντίγραφο ασφαλείας και ήταν δυνατή η έγκαιρη επαναφορά των δεδομένων, δεν θα απαιτούταν η αναφορά στην εποπτική αρχή ή στα πρόσωπα, καθώς δεν θα επρόκειτο για μόνιμη απώλεια της διαθεσιμότητας ή της εμπιστευτικότητας. Ωστόσο, εάν η εποπτική αρχή έλαβε γνώση του συμβάντος με άλλα μέσα, μπορεί να εξετάσει το ενδεχόμενο να διεξαγάγει έρευνα για την αξιολόγηση της συμμόρφωσης με τις απαιτήσεις του άρθρου 32 για την ευρύτερη ασφάλεια.
v. Ένα πρόσωπο καλεί στο τηλεφωνικό κέντρο μιας τράπεζας για να αναφέρει μια παραβίαση δεδομένων. Το πρόσωπο έχει λάβει μια μηνιαία κατάσταση η οποία αφορά άλλο πρόσωπο. Ο υπεύθυνος επεξεργασίας προβαίνει σε σύντομη έρευνα (δηλαδή η έρευνα ολοκληρώνεται εντός 24 ωρών) και διαπιστώνει με εύλογη βεβαιότητα ότι έχει σημειωθεί παραβίαση δεδομένων προσωπικού χαρακτήρα και	Ναι.	Τα επηρεαζόμενα πρόσωπα ενημερώνονται μόνο εάν υπάρχει υψηλός κίνδυνος και είναι σαφές ότι δεν επηρεάστηκαν άλλα πρόσωπα.	Εάν, έπειτα από περαιτέρω διερεύνηση, διαπιστωθεί ότι επηρεάζονται περισσότερα πρόσωπα, πρέπει να ενημερώνεται η εποπτική αρχή και ο υπεύθυνος επεξεργασίας ενημερώνει επιπλέον τα υπόλοιπα πρόσωπα εάν υπάρχει υψηλός κίνδυνος γι' αυτά.

εξετάζει κατά πόσο υπάρχει συστημική έλλειψη η οποία μπορεί να συνεπάγεται ότι επηρεάζονται ή ενδέχεται να επηρεαστούν και άλλα πρόσωπα.			
vi. Ένας υπεύθυνος επεξεργασίας διαχειρίζεται μια διαδικτυακή αγορά και έχει πελάτες σε περισσότερα από ένα κράτη μέλη. Η αγορά δέχεται κυβερνοεπίθεση και τα ονόματα χρηστών, οι κωδικοί πρόσβασης και το ιστορικό αγορών δημοσιεύονται στο διαδίκτυο από το άτομο που κάνει την επίθεση.	Ναι, το συμβάν αναφέρεται στην επικεφαλής εποπτική αρχή εάν αφορά διασυνοριακή επεξεργασία.	Ναι, καθώς θα μπορούσε να επιφέρει υψηλό κίνδυνο.	Ο υπεύθυνος επεξεργασίας θα πρέπει να αναλάβει δράση, π.χ., να επιβάλει την επαναφορά των κωδικών πρόσβασης των λογαριασμών που έχουν επηρεαστεί, καθώς και άλλες ενέργειες για τον μετριασμό του κινδύνου. Ο υπεύθυνος επεξεργασίας θα πρέπει επίσης να λάβει υπόψη τυχόν άλλες υποχρεώσεις γνωστοποίησης, π.χ., σύμφωνα με την οδηγία ΑΔΠ δεδομένου ότι είναι πάροχος ψηφιακών υπηρεσιών.
vii. Μια εταιρεία φιλοξενίας δικτυακών τόπων που λειτουργεί ως εκτελών την επεξεργασία δεδομένων εντοπίζει ένα σφάλμα στον κώδικα που ελέγχει την εξουσιοδότηση χρήστη. Αυτό το σφάλμα σημαίνει ότι οποιοσδήποτε χρήστης μπορεί να προσπελάσει τα στοιχεία λογαριασμού οποιουδήποτε άλλου χρήστη.	Ως εκτελών την επεξεργασία, η εταιρεία φιλοξενίας δικτυακών τόπων πρέπει να ενημερώσει αμελλητί τους πελάτες (τους υπευθύνους επεξεργασίας). Εάν υποθέσουμε ότι η εταιρεία φιλοξενίας δικτυακών τόπων έχει διεξαγάγει τη δική της έρευνα, οι επηρεαζόμενοι υπεύθυνοι επεξεργασίας θα πρέπει να έχουν εύλογη βεβαιότητα ως προς το εάν καθένας εξ αυτών έχει υποστεί παραβίαση και,	Εάν δεν ενδέχεται να δημιουργηθεί υψηλός κίνδυνος για τα πρόσωπα, δεν απαιτείται η ενημέρωσή τους.	Η εταιρεία φιλοξενίας δικτυακών τόπων (δηλαδή ο εκτελών την επεξεργασία) θα πρέπει να λάβει υπόψη τυχόν άλλες υποχρεώσεις γνωστοποίησης (π.χ., σύμφωνα με την οδηγία ΑΔΠ δεδομένου ότι είναι πάροχος ψηφιακών υπηρεσιών). Εάν δεν υπάρχουν στοιχεία για εκμετάλλευση αυτού του τρωτού σημείου για οποιονδήποτε από τους υπευθύνους επεξεργασίας της, ενδέχεται να μην έχει σημειωθεί παραβίαση που χρήζει γνωστοποίησης, αλλά

	συνεπώς, είναι πιθανό να θεωρείται ότι έχει «αποκτήσει γνώση» μετά τη γνωστοποίηση από την εταιρεία φιλοξενίας (τον εκτελούντα την επεξεργασία). Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει στη συνέχεια την εποπτική αρχή.		είναι πιθανό να πρόκειται για παραβίαση που πρέπει να καταγραφεί ή, διαφορετικά, δεν θα υπάρχει συμμόρφωση με το άρθρο 32.
viii. Ιατρικά αρχεία σε ένα νοσοκομείο δεν είναι διαθέσιμα για χρονικό διάστημα 30 ωρών λόγω κυβερνοεπίθεσης.	Ναι, το νοσοκομείο υποχρεούται να προβεί σε γνωστοποίηση, καθώς ενδέχεται να προκύψει υψηλός κίνδυνος για την ευημερία και την προστασία της ιδιωτικής ζωής των ασθενών.	Ναι, το συμβάν αναφέρεται στα επηρεαζόμενα πρόσωπα.	
ix. Δεδομένα προσωπικού χαρακτήρα μεγάλου αριθμού σπουδαστών εστάλησαν εκ παραδρομής σε εσφαλμένο κατάλογο ηλεκτρονικών διευθύνσεων με περισσότερους από 1 000 αποδέκτες.	Ναι, το συμβάν αναφέρεται στην εποπτική αρχή.	Ναι, το συμβάν αναφέρεται στα πρόσωπα ανάλογα με την έκταση και το είδος των δεδομένων προσωπικού χαρακτήρα που επηρεάζονται και τη σοβαρότητα των ενδεχόμενων συνεπειών.	
x. Ένα μήνυμα ηλεκτρονικού ταχυδρομείου άμεσης εμπορικής προώθησης αποστέλλεται σε αποδέκτες με συμπληρωμένα τα πεδία «προς:» ή «κοιν.:», με αποτέλεσμα κάθε αποδέκτης να μπορεί να δει τη διεύθυνση ηλεκτρονικού ταχυδρομείου άλλων	Ναι, η ενημέρωση της εποπτικής αρχής ενδέχεται να είναι υποχρεωτική εάν επηρεάζεται μεγάλος αριθμός προσώπων, εάν αποκαλύπτονται ευαίσθητα δεδομένα (π.χ., ο κατάλογος ηλεκτρονικών διευθύνσεων ενός ψυχοθεραπευτή) ή εάν άλλοι παράγοντες παρουσιάζουν υψηλούς κινδύνους	Ναι, το συμβάν αναφέρεται στα πρόσωπα ανάλογα με την έκταση και το είδος των δεδομένων προσωπικού χαρακτήρα που επηρεάζονται και τη σοβαρότητα των ενδεχόμενων συνεπειών.	Η γνωστοποίηση ενδέχεται να μην είναι απαραίτητη εάν δεν αποκαλύπτονται ευαίσθητα δεδομένα και εάν αποκαλύπτεται μόνο ένας μικρός αριθμός ηλεκτρονικών διευθύνσεων.

αποδεκτών.	(π.χ., το μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει τους αρχικούς κωδικούς πρόσβασης).		