Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR)

Κρυπτογράφηση και Ψευδωνυμοποίηση

Δρ. Νικόλαος Η. Λουκάς, *(CDPO, PRINCE2/P), Research Associate, Τμήμα Ψηφιακών Συστημάτων Πανεπιστημίου Πειραιά*

I. Εισαγωγή

Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) - *General Data Protection Regulation* (GDPR)][1], αποτελεί, στο πλαίσιο της Ε.Ε. για την τελευταία εικοσαετία, ένα από τα σημαντικότερα νομοθετικά εγχειρήματα, όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα. Παρότι ο νέος αυτός κανονισμός υιοθετεί αρκετές από τις βασικές αρχές (*principles*[2]) που εισάγει και περιγράφει η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[3], ωστόσο, η επερχόμενη εφαρμογή του (από τις 25 Μαΐου 2018) απαιτεί τρόπον τινά μια αναθεώρηση της αντίληψης ως προς την προστασία των προσωπικών δεδομένων και την ιδιωτικότητα (*privacy*) στους κόλπους της Ε.Ε.

Ο ΓΚΠΔ διαφοροποιείται σε σχέση με την Οδηγία 95/46/ΕΚ σε μια σειρά θεμάτων, όπως είναι, για παράδειγμα, το ρητά διευρυμένο εδαφικό πεδίο εφαρμογής (*extended territorial scope*), ο προσδιορισμός (του μέγιστου ορίου) των διοικητικών προστίμων που μπορούν να επιβληθούν στις περιπτώσεις παράβασης συγκεκριμένων διατάξεων του κανονισμού (συμπεριλαμβανομένων και αυτών που αφορούν την παραβίαση προσωπικών δεδομένων (*data breach*), η ενίσχυση του πλαισίου σχετικά με τη συγκατάθεση (*consent*) των υποκειμένων, ο καθορισμός των απαιτούμενων ενεργειών αντιμετώπισης περιστατικών παραβίασης προσωπικών δεδομένων, η εισαγωγή ενός νέου ρόλου, αυτού του υπεύθυνου προστασίας δεδομένων (*Data Protection Officer - DPO*), κ.ά.[4] Η λεπτομερής και πλήρης παρουσίαση όλων των νέων θεμάτων που εισάγει ο κανονισμός εκφεύγει του σκοπού του παρόντος άρθρου. Ωστόσο, η ανάλυση που ακολουθεί εστιάζει σε ένα ιδιαίτερα σημαντικό ζήτημα που αναδεικνύεται στον ΓΚΠΔ σε σχέση με την Οδηγία 95/46/ΕΚ και το οποίο αφορά στη συγκεκριμενοποίηση ορισμένων τεχνικών μέτρων (*technical measures*), που ο κανονισμός προτείνει, προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας των δεδομένων προσωπικού χαρακτήρα. Τα μέτρα αυτά αφορούν τις τεχνικές της Κρυπτογράφησης (*Encryption*) και της Ψευδωνυμοποίησης (*Pseudonymisation*[5]).

II. Αναφορές στα τεχνικά μέτρα στην Οδηγία 95/46/ΕΚ και στον ΓΚΠΔ

Το άρθρο 17 («Ασφάλεια της Επεξεργασίας») της Οδηγίας 95/46/ΕΚ, όσον αφορά την υιοθέτηση και εφαρμογή τεχνικών μέτρων, αναφέρει ότι *«τα κράτη-μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, ιδίως εάν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσω δικτύου, και από κάθε άλλη μορφή αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα»*[6]. Ωστόσο, τα τεχνικά αυτά μέτρα στην Οδηγία 95/46/ΕΚ δεν συγκεκριμενοποιούνται[7].

Το 2014 η ομάδα εργασίας του άρθρου 29 (WP 29[8]) επιχειρεί να εισάγει και να αναλύσει την αποτελεσματικότητα και τα όρια των τεχνικών μέτρων (*Opinion on Anonymisation Techniques*[9]), και συγκεκριμένα των υφιστάμενων τεχνικών Ανωνυμοποίησης (*Anonymization*) για την προστασία των δεδομένων και παρέχει συστάσεις για τη διαχείριση αυτών των τεχνικών, λαμβάνοντας υπόψη τον υπολειπόμενο κίνδυνο (*residual risk*) ταυτοποίησης των υποκειμένων των δεδομένων, που είναι εγγενής σε καθεμία από αυτές τις τεχνικές. Παράλληλα, το ίδιο κείμενο αναλύει λεπτομερώς και την τεχνική της ψευδωνυμοποίησης και αποσαφηνίζει ορισμένες παρανοήσεις, ειδικά όσον αφορά στις διαφορές μεταξύ της ψευδωνυμοποίησης και της ανωνυμοποίησης.

Το 2016, ο ΓΚΠΔ, σε αντίθεση με την Οδηγία 95/46/ΕΚ, επιχειρεί πλέον επίσημα τον προσδιορισμό κάποιων εκ των απαιτούμενων τεχνικών μέτρων για την προστασία των δεδομένων, με αναφορά σε συνολικά δεκαπέντε σημεία εντός του κειμένου του κανονισμού (εκ των οποίων εννέα φορές στις αιτιολογικές σκέψεις) στην ψευδωνυμοποίηση, και σε τέσσερα σημεία εντός του κειμένου του κανονισμού (εκ των οποίων μία φορά στις αιτιολογικές σκέψεις) στην κρυπτογράφηση. Δεν αποτελεί, φυσικά, αντικείμενο υψηλού ενδιαφέροντος αυτός καθαυτός ο συνολικός αριθμός αναφορών στα μέτρα αυτά, αλλά, όπως θα παρουσιαστεί στη συνέχεια, η ιδιαίτερη σημασία και βαρύτητα των διατάξεων του κανονισμού όπου αναφέρονται τα μέτρα αυτά.

III. Ορισμοί

Στον ΓΚΠΔ δεν περιλαμβάνεται ένας ακριβής ορισμός της κρυπτογράφησης[10]. Ωστόσο, ο όρος αυτός θα μπορούσε να περιγραφεί ως η εφαρμογή μιας διαδικασίας μετασχηματισμού μέσω κάποιου αλγορίθμου με τη χρήση «κλειδιών κρυπτογράφησης» (*encryption keys*), ενός συνόλου προσωπικών δεδομένων σε μία ακατανόητη (ακατάληπτη) μορφή ώστε να μην μπορούν να αναγνωσθούν από κανέναν εκτός του(ων) νόμιμου(ων) ιδιοκτήτη(τών) των κλειδιών κρυπτογράφησης[11, 12].

Αντιθέτως, ο ΓΚΠΔ ορίζει επαρκώς την τεχνική της ψευδωνυμοποίησης. Σύμφωνα με το άρθρο 4 παρ. 5: *«ψευδωνυμοποίηση είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τέτοιο τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρω-*

ματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο».

Ωστόσο, όπως εμμέσως υποδηλώθηκε παραπάνω (Ενότητα ΙΙ), ένας όρος που συχνά συγχέεται με την ψευδωνυποποίηση στο πεδίο της ασφάλειας και της προστασίας των προσωπικών δεδομένων είναι η ανωνυμοποίηση[13]. Ουσιαστικά πρόκειται για δύο διαφορετικές τεχνικές που θα πρέπει να διαχωρίζονται μεταξύ τους, πολύ περισσότερο μάλιστα στο πλαίσιο του ΓΚΠΔ, δεδομένου ότι τα «ανωνυμοποιημένα δεδομένα» και τα «ψευδωνυποιημένα δεδομένα» αντιμετωπίζονται ως δύο εντελώς διαφορετικές κατηγορίες.

Ως ανωνυμοποίηση ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην είναι πλέον εφικτό τα ανωνυμοποιημένα δεδομένα να συσχετιστούν με το υποκείμενο των δεδομένων[14]. Κατά συνέπεια από τους δύο αυτούς ορισμούς (δηλαδή αυτούς της ψευδωνυμοποίησης και της ανωνυμοποίησης) προκύπτει ότι η χρήση της ανωνυμοποίησης έχει ως αποτέλεσμα την αδυναμία προσδιορισμού του υποκειμένου των δεδομένων, ενώ η ψευδωνυμοποίηση αντικαθιστά την ταυτότητα του υποκειμένου των δεδομένων με τέτοιο τρόπο, ώστε να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώριση του υποκειμένου των δεδομένων.

Βάσει του κανονισμού [Αιτ. Σκέψη υπ' αριθμ. (26)], οι βασικές αρχές της προστασίας δεδομένων δεν θα πρέπει να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή σε πληροφορίες που δεν μπορούν να συσχετιστούν με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί. Ως εκ τούτου, ο ΓΚΠΔ δεν αφορά την επεξεργασία τέτοιων ανώνυμων πληροφοριών[15]. Αντιθέτως, τα δεδομένα προσωπικού χαρακτήρα, που έχουν υποστεί ψευδωνυμοποίηση, συνεχίζουν να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο και κατά συνέπεια συνεχίζουν να εμπίπτουν στις διατάξεις και στους περιορισμούς του ΓΚΠΔ.

IV. Η κρυπτογράφηση και η ψευδωνυμοποίηση ως προτεινόμενα τεχνικά μέτρα στον ΓΚΠΔ

Η κρυπτογράφηση και η ψευδωνυμοποίηση μπορούν να μειώσουν σημαντικά τους κινδύνους που σχετίζονται με την επεξεργασία δεδομένων. Για τον λόγο αυτόν, ο ΓΚΠΔ παροτρύνει και δημιουργεί κίνητρα για τους υπεύθυνους επεξεργασίας να εφαρμόζουν τις τεχνικές αυτές στα προσωπικά δεδομένα που συλλέγουν, μέσω μάλιστα και της ελαστικοποίησης ορισμένων απαιτήσεων που τους αφορούν σε ορισμένα σημαντικά άρθρα του κανονισμού.

Ήδη από το άρθρο 6 («Νομιμότητα της επεξεργασίας»), όταν *«η επεξεργασία για σκοπό άλλον από αυτόν για τον οποίο έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση»*.

Η «Προστασία των Δεδομένων ήδη από τον Σχεδιασμό και εξ' Ορισμού» *(data protection by design and by default)*, που περιγράφεται στο άρθρο 25, προβλέπει ότι ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση[16].

Το άρθρο 32 («Ασφάλεια Επεξεργασίας»), θεωρεί ότι η κρυπτογράφηση και η ψευδωνυμοποίηση δύνανται να διασφαλίσουν το κατάλληλο επίπεδο ασφάλειας στα δεδομένα προσωπικού χαρακτήρα έναντι των κινδύνων. Παράλληλα, στο άρθρο 34 («Ανακοίνωση Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα στο Υποκείμενο των Δεδομένων») καθορίζεται ότι δεν απαιτείται ενημέρωση του υποκειμένου των δεδομένων σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον τα δεδομένα αυτά (μεταξύ και άλλων προϋποθέσεων) είναι κρυπτογραφημένα.

Βάσει του άρθρου 40 («Κώδικες Δεοντολογίας»), ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας παροτρύνονται να εκπονούν κώδικες δεοντολογίας, προκειμένου να προσδιορίσουν την εφαρμογή του κανονισμού ΓΚΠΔ όσον αφορά μεταξύ άλλων και την ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα.

Τέλος, στο άρθρο 89 («Διασφαλίσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς») η ψευδωνυμοποίηση περιλαμβάνεται μεταξύ των εγγυήσεων ότι έχουν θεσπιστεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε (περαιτέρω) επεξεργασία για λόγους αρχειοθέτησης για λόγους γενικού συμφέροντος, επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

V. Σχόλια - Συμπεράσματα

Η κρυπτογράφηση και η ψευδωνυμοποίηση προτείνονται ως κάποιες από τις βασικές τεχνικές[17] για την ενίσχυση του επιπέδου προστασίας των προσωπικών δεδομένων, συμπεριλαμβανομένων και των προσωπικών δεδομένων ειδικών κατηγοριών.

Η κρυπτογράφηση, θεωρούμενη ως ασφαλής τεχνική (ειδικά με τη χρήση εξελιγμένων μηχανισμών κρυπτογράφησης[18]) δύναται να αποτρέψει την πρόσβαση σε τρίτους, ακόμη και σε περιπτώσεις που μη εξουσιοδοτημένα πρόσωπα αποκτούν πρόσβαση σε αυτά. Ωστόσο, τα κρυπτογραφημένα δεδομένα δεν θεωρούνται «εύχρηστα», καθώς η επεξεργασία τους (π.χ., αναζήτηση, ανάλυση, κ.λπ.) απαιτεί πρώτα την αποκρυπτογράφησή τους - διαδικασία που απαιτεί επιπρόσθετο χρόνο και υπολογιστικούς πόρους[19]. Ως εκ τούτου, ένα από τα κύρια ζητήματα της κρυπτογράφησης είναι η εξισορρόπηση μεταξύ του επιπέδου ασφάλειας των προσωπικών δεδομένων και της χρηστικότητας τους. Παράλληλα ως ιδιαίτερα σημαντική χαρακτηρίζεται και η απαίτηση για διαχείριση και προστασία των «κλειδιών κρυπτογράφησης» - απώλεια των κλειδιών σημαίνει και απώλεια δεδομένων. Όλα τα παραπάνω καθιστούν την κρυπτογράφηση ίσως όχι την πρακτικότερη επιλογή προστασίας των προσωπικών δεδομένων από έναν υπεύθυνο επεξεργασίας, ιδιαίτερα σε περιπτώσεις επεξεργασίας μεγάλου όγκου δεδομένων σε συχνή (π.χ. καθημερινή) βάση[20].

>

Τεχνικά Μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) *(συνέχεια)*

Η ψευδωνυμοποίηση μπορεί να θεωρηθεί ως μία εναλλακτική λύση αντί της κρυπτογράφησης[21], ιδιαίτερα ως προς το θέμα της «χρηστικότητας» των δεδομένων, επιτρέποντας την αντικατάσταση μόνο των προσωπικών αναγνωριστικών (*personal identifiers*) από τα δεδομένα, έτσι ώστε αυτά να περιέχουν μόνο ψευδή αναγνωριστικά. Τα δεδομένα δεν δύνανται να αποδοθούν σε κάποιο υποκείμενο, και ταυτόχρονα δεν περιορίζεται η ευκολία της επεξεργασίας τους. Ωστόσο, τα ψευδωνυμοποιημένα δεδομένα αντιμετωπίζουν τον κίνδυνο ταυτοποίησης του υποκειμένου όταν σε μία παραβίαση δεδομένων, ένας τρίτος ενδεχομένως αποκτήσει το μηχανισμό ψευδωνυμοποίησης, ή συνδέσει με άλλο τρόπο το ψευδοανωνυμοποιημένο σύνολο δεδομένων με τα υποκείμενα. Για τον λόγο αυτόν ο ΓΚΠΔ θέτει ως απαίτηση οι «πρόσθετες πληροφορίες», που χρησιμοποιούνται για την υλοποίηση της ψευδωνυμοποίησης, να διατηρούνται σε ξεχωριστή τοποθεσία, και να «υπόκεινται στα κατάλληλα τεχνικά και οργανωτικά μέτρα», προκειμένου να καταστεί δυνατή η διασφάλιση και προστασία των προσωπικών δεδομένων.

Τέλος, πέραν της κρυπτογράφησης και της ψευδωνυμοποίησης δεν θα πρέπει να εξαιρεθεί από τα μέτρα προστασίας και η εφαρμογή της τεχνικής ανωνυμοποίησης[22] στα προσωπικά δεδομένα που διατηρεί ένας υπεύθυνος επεξεργασίας[23]. Ως εκ τούτου, η ανωνυμοποίηση μπορεί να θεωρηθεί ως μια στρατηγική επιλογή ενός υπεύθυνου επεξεργασίας για την κατά κάποιο τρόπο «αποδέσμευσή» του από τις διατάξεις του ΓΚΠΔ και από το αντίστοιχο νομοθετικό καθεστώς που προδιαγράφεται. Τα πλεονεκτήματα από μια τέτοια επιλογή μπορεί να είναι πολλαπλά[24], παρέχοντας τρόπον τινά ένα σαφές κίνητρο για τους υπεύθυνους επεξεργασίας προσωπικών δεδομένων να υιοθετούν και να εφαρμόζουν σε ορισμένες περιπτώσεις τεχνικές και μεθόδους που ανωνυμοποιούν τα δεδομένα που έχουν στη διάθεσή τους. Ωστόσο, η ανωνυμοποίηση, δεδομένου ότι είναι μια μη αναστρέψιμη διαδικασία που καταργεί την ικανότητα αναγνώρισης των υποκειμένων των δεδομένων, μπορεί να έχει ως αποτέλεσμα την υποβάθμιση της χρησιμότητας και χρηστικότητας των ανωνυμοποιημένων δεδομένων και σε πολλές περιπτώσεις να τα καταστήσει μη εκμεταλλεύσιμα για σκοπούς επεξεργασίας. Επομένως, η ανωνυμοποίηση δεν μπορεί να θεωρηθεί ότι αποτελεί μια τυπική επιλογή για όλους τους υπεύθυνους και για όλες τις περιπτώσεις επεξεργασίας. Σ

ΥΠΟΣΗΜΕΙΩΣΕΙΣ

1. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
2. Στους βασικούς όρους που αναφέρεται το παρόν άρθρο χρησιμοποιείται και η Αγγλική ορολογία μέσα σε παρένθεση.
3. Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
4. "Comparison of General Data Protection Regulation and Data Protection Directive", The Centre for Internet & Society (https://cisindia.org/).
5. Για την πληρέστερη παρουσίαση των υπόψη τεχνικών μέτρων θεωρήθηκε ως αναγκαία η ανάλυση και του όρου της Ανωνυμοποίησης (Anonymisation), ο οποίος παρότι ως όρος δεν αναφέρεται ρητά στις διατάξεις του ΓΚΠΔ, εμμέσως σχετίζεται με την εφαρμογή του.
6. Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
7. Αντίστοιχα και ο Ν 2472/1997 που ουσιαστικά ενσωματώνει την Οδηγία 95/46/ΕΚ στην ελληνική νομοθεσία δεν προσδιορίζει τα αντίστοιχα, τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους.
8. Η ομάδα εργασίας συστάθηκε βάσει του άρθρου 29 της Οδηγίας 95/46/ΕΚ. Αποτελεί ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για την προστασία των δεδομένων και την προστασία της ιδιωτικής ζωής.
9. "Opinion 05/2014 on Anonymisation Techniques", ARTICLE 29 DATA PROTECTION WORKING PARTY, 0829/14/EN WP216, Adopted on 10 April 2014.
10. Σε αντίθεση με την πρόταση του Ευρωπαϊκού Κοινοβουλίου κατά τη φάση επεξεργασίας του ΓΚΠΔ, η οποία είχε προτείνει την ενσωμάτωση του ορισμού «Κρυπτογραφημένα Δεδομένα» (Encrypted Data) στο κείμενο του κανονισμού.
11. Η αντίστροφη διαδικασία με την εφαρμογή της οποίας από τα κρυπτογραφημένα δεδομένα παράγεται το αρχικό σύνολο δεδομένων ονομάζεται αποκρυπτογράφηση (decryption).
12. «Κρυπτογραφία», Βικιπαίδεια, αναθ. 4.5.2017.
13. "Opinion 05/2014 on Anonymisation Techniques", ARTICLE 29 DATA PROTECTION WORKING PARTY, 0829/14/EN WP216, Adopted on 10 April 2014.
14. *Κ. Λαμπρινουδάκης, Σ. Γκρίτζαλης, Λ. Μήτρου, Σ. Κάτσικας,* «Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών», εκδ. Παπασωτηρίου, Αθήνα, 2010.
15. Η ίδια προσέγγιση έχει ακολουθηθεί και στην Οδηγία 95/46/ΕΚ [Αιτ. Σκ. υπ' αριθμ. (26)].
16. Στο άρθρο 25 η ψευδωνυμοποίηση θεωρείται και ως μέθοδος που εξασφαλίζει την τήρηση της αρχής της ελαχιστοποίησης των δεδομένων (data minimisation): «ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων». Αντίστοιχη διατύπωση συναντάται και στο άρθρο 89.
17. Η λεπτομερής παρουσίαση του συνόλου των τεχνικών μέτρων που μπορούν να υιοθετηθούν για την προστασία των δεδομένων προσωπικού χαρακτήρα είναι εκτός του σκοπού του παρόντος άρθρου.
18. Υπάρχουν τρεις βασικοί παράγοντες που λαμβάνονται υπόψη κατά την αξιολόγηση του επιπέδου ασφάλειας της κρυπτογράφησης: η δύναμη του χρησιμοποιούμενου αλγόριθμου κρυπτογράφησης (strength of the encryption algorithm), το μήκος του κλειδιού κρυπτογράφησης (length of the encryption key) -όσο μεγαλύτερο είναι το κλειδί, τόσο ασφαλέστερη θα είναι η κρυπτογράφηση- και η ασφάλεια της διαχείρισης των κλειδιών.
19. Οι εξελίξεις στον τομέα της κρυπτογράφησης στοχεύουν μεταξύ άλλων και στην επιτυχή αντιμετώπιση και εξάλειψη αυτών των προβλημάτων (βλ. για παράδειγμα ομομορφική κρυπτογράφηση).
20. Τα πλεονεκτήματα, ωστόσο, της κρυπτογράφησης αναδεικνύονται καλύτερα στις περιπτώσεις αποθήκευσης δεδομένων για μεσοπρόθεσμη ή μακροπρόθεσμη χρήση, ή στις περιπτώσεις που απαιτείται ασφαλής μετάδοση δεδομένων μεταξύ δύο ή περισσοτέρων τελικών χρηστών (end users) μέσω ενός επικοινωνιακού συστήματος.
21. Θα πρέπει σε αυτό το σημείο να σημειωθεί ότι είναι εφικτή (και σε αρκετές περιπτώσεις προτείνεται) ως λύση και η παράλληλη εφαρμογή και χρήση και των δύο αυτών τεχνικών .
22. Στο πλαίσιο του αυστηρού ορισμού της όπως παρουσιάστηκε στην Ενότητα ΙΙΙ (Ορισμοί).
23. "Anonymisation: managing data protection risk code of practice", Information Commissioner's Office (ICO), Nov 2012, UK.
24. Στην περίπτωση ανωνυμοποίησης των δεδομένων, τα θέματα της συναίνεσης των υποκειμένων των δεδομένων παύουν να ισχύουν, διευκολύνεται η διεθνής διακίνηση των ανωνυμοποιημένων δεδομένων, και παράλληλα αίρονται οι περιορισμοί σχετικά με τον χρόνο διατήρησης των δεδομένων στη διάθεση του υπεύθυνου επεξεργασίας.