ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 01-10-2021
Αριθ. Πρωτ.: 2198

ΑΠΟΦΑΣΗ 43/2021

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε, μετά από πρόσκληση του Προέδρου της, σε έκτακτη συνεδρίαση μέσω τηλεδιάσκεψης την 19-07-2021, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Κωνσταντίνος Μενουδάκος, Πρόεδρος της Αρχής, τα τακτικά μέλη Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, ως εισηγητής, και Χαράλαμπος Ανθόπουλος. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν, με εντολή του Προέδρου, οι ελεγκτές Κωνσταντίνος Λιμνιώτης και Σπύρος Παπαστεργίου, ειδικοί επιστήμονες πληροφορικής, ως βοηθοί εισηγητή, και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Υποβλήθηκε στην Αρχή, η με αριθμ. πρωτ. Γ/ΕΙΣ/7897/17-11-2020 έγγραφη αναφορά του Α, στην οποία αναφέρονται τα εξής:

α) Στις …/2020 απέστειλε μήνυμα ηλεκτρονικού ταχυδρομείου στην Ελληνική Αστυνομία, και ειδικότερα στη διεύθυνση …@astynomia.gr, το οποίο περιελάμβανε προσωπικά του δεδομένα όπως, πέραν της ηλεκτρονικής του διεύθυνσης, το ονοματεπώνυμο και τον προσωπικό του κωδικό για την υπηρεσία Passenger Location Form, αναφορικά με την επίσκεψή του στην Ελλάδα τον … του 2020.

β) Ακολούθως, χωρίς να λάβει απάντηση από την Ελληνική Αστυνομία, έλαβε τέσσερα διαφορετικά ηλεκτρονικά μηνύματα τα οποία «υποδύονται» ότι προέρχονται από την Ελληνική Αστυνομία και είτε έφεραν κακόβουλο λογισμικό είτε συνδέσμους οι οποίοι παρέπεμπαν σε κακόβουλο λογισμικό (τα μηνύματα

Λεωφ. Κηφισίας 1-3, 11523 Αθήνα
T: 210 6475 600 • E: contact@dpa.gr • www.dpa.gr

επισυνάπτονται στην ως άνω αναφορά του). Όπως προσδιορίζει ο καταγγέλλων, οι διευθύνσεις διαδικτύου (διευθύνσεις IP) από τις οποίες φέρεται να προέρχονται τα εν λόγω μηνύματα αντιστοιχούν σε διάφορες χώρες του εξωτερικού (συγκεκριμένα, στο Υ, στη Φ, στο Χ και στο Ψ). Από τα εν λόγω μηνύματα φαίνεται ότι το αρχικό μήνυμα του καταγγέλλοντος προς την Ελληνική Αστυνομία έχει διαρρεύσει εξ ολοκλήρου σε άγνωστους τρίτους.

γ) Σε τηλεφωνική επικοινωνία που είχε με την Ελληνική Αστυνομία στις …/2020, εκπρόσωπος της Υπηρεσίας τον ενημέρωσε ότι υπήρχε πρόβλημα ασφάλειας στο ηλεκτρονικό της ταχυδρομείο.

δ) Τα ανωτέρω περιγράφονται από τον καταγγέλλοντα σε μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο έστειλε προς την Ελληνική Αστυνομία στις …/2020, με το οποίο επίσης ζητά τη θέση της Ελληνικής Αστυνομίας επί των εν λόγω συμβάντων (και το οποίο κοινοποιήθηκε στην Αρχή με την ως άνω αναφορά του).

Ακολούθως, με το υπ’ αριθμ. πρωτ. Γ/ΕΙΣ/8192/30-11-2020 έγγραφό του, ο καταγγέλλων ενημέρωσε για επώνυμη ανάρτηση στο Διαδίκτυο άλλου ατόμου στο οποίο, κατά τους ισχυρισμούς του, συνέβη ακριβώς το ίδιο (ο σύνδεσμος είναι ο: …).

Κατόπιν των ανωτέρω, η Ελληνική Αστυνομία διαβίβασε στην Αρχή με το υπ’ αριθμ. πρωτ. … από …2020 έγγραφό της (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/8783/22-12-2020), την απάντηση που έστειλε προς τον καταγγέλλοντα στο ως άνω αίτημά του. Συγκεκριμένα, στην εν λόγω απάντηση (με αρ. πρωτ. … και ημερομηνία …2020) περιγράφεται ότι κατά τις ημερομηνίες λήψης των προαναφερόμενων τεσσάρων μηνυμάτων ηλεκτρονικού ταχυδρομείου από υποτιθέμενο αποστολέα της Ελληνικής Αστυνομίας, ήταν σε πλήρη εξέλιξη κυβερνοεπίθεση με κωδικό όνομα «EMOTET» η οποία εκδηλώθηκε σε παγκόσμιο επίπεδο. Περαιτέρω, από τη μελέτη του κώδικα των εν λόγω μηνυμάτων (ο οποίος εξάλλου είχε συμπεριληφθεί στην αρχική επιστολή του καταγγέλλοντα), προκύπτει ότι τα μηνύματα δεν έχουν αποσταλεί από υποδομές της Ελληνικής Αστυνομίας αλλά από ηλεκτρονικούς λογαριασμούς που δεν έχουν καμία σχέση με την Ελληνική Αστυνομία (και οι οποίοι παρατίθενται στο εν λόγω έγγραφο). Στη συνέχεια, ο καταγγέλλων διαβίβασε στην Αρχή, με το υπ’ αριθμ. πρωτ. Γ/ΕΙΣ/487/19-01-2021 έγγραφό του, το υπ’ αριθμ. πρωτ. … και από …2020 έγγραφο

της Ελληνικής Αστυνομίας, με το οποίο είχε ενημερωθεί, από την Υπεύθυνο Προστασίας Δεδομένων της Ελληνικής Αστυνομίας, ότι το αίτημά του έχει προωθηθεί στο Τμήμα Ασφάλειας Πληροφορικών και Προστασίας Προσωπικών Δεδομένων της Διεύθυνσης Πληροφορικής της Ελληνικής Αστυνομίας (το εν λόγω έγγραφο αποτελούσε την αρχική ανταπόκριση, από την πλευρά της Ελληνικής Αστυνομίας, στο αίτημά του, πριν την τελική απάντηση με την προαναφερθείσα επιστολή ημερομηνίας …2020).

Σε συνέχεια των ανωτέρω, η Αρχή απέστειλε στην Ελληνική Αστυνομία το υπ' αριθμ. πρωτ. Γ/ΕΞΕ/482/27-01-2021 έγγραφο, με το οποίο την κάλεσε να περιγράψει τις ακριβείς ενέργειες στις οποίες προέβη για τον εξακρίβωση της ασφάλειας των συστημάτων της σε σχέση με το εν λόγω ζήτημα, λαμβάνοντας υπόψη ότι, καίτοι καθίσταται σαφές ότι τα εν λόγω μηνύματα δεν εστάλησαν από την Ελληνική Αστυνομία, δεν προέκυψε εν τούτοις από την απάντησή της προς τον καταγγέλλοντα ότι πραγματοποιήθηκε έλεγχος από την πλευρά της ως προς το αν κάποιο υποσύστημά της (π.χ. σταθμός εργασίας) έχει «μολυνθεί» από κακόβουλο λογισμικό ή αν έχει παραβιαστεί καθ' οιονδήποτε άλλον τρόπο η ασφάλειά του, έτσι ώστε να «διευκολυνθεί» η εξάπλωση της ανωτέρω κυβερνο-επίθεσης. Στο ίδιο έγγραφο η Αρχή επισήμανε ότι ένας τέτοιος έλεγχος αποτελεί υποχρέωση της Ελληνικής Αστυνομίας, δεδομένου ότι αφενός τα προαναφερθέντα κακόβουλα μηνύματα εμπεριείχαν αυτούσιο κείμενο το οποίο είχε ήδη τύχει επεξεργασίας από εφαρμογές ηλεκτρονικού ταχυδρομείου της Αστυνομίας, και αφετέρου ότι η ως άνω κυβερνο-επίθεση βασίζεται, για την εξάπλωσή της, σε κακόβουλο λογισμικό το οποίο εγκαθίσταται σε προγράμματα ηλεκτρονικού ταχυδρομείου (παραπέμποντας σχετικά σε κείμενο του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA)[1]), καθώς επίσης ότι, σε περίπτωση κατά την οποία για το εν λόγω ζήτημα έχει υπάρξει παραβίαση ασφάλειας υπο-συστήματος της Ελληνικής Αστυνομίας, τότε – πέραν των υποχρεώσεων για αμελλητί αντιμετώπισή του και αποκατάσταση της ασφάλειας – τυγχάνουν κατ' αρχήν εφαρμογής και οι διατάξεις των άρθρων 33 και 34 του Γενικού

[1] Βλ. τη σχετική αναφορά του ENISA για το 2020: https://www.enisa.europa.eu/publications/malware αλλά και τις εκεί σχετικές αναφορές.

Κανονισμού Προστασίας Δεδομένων αναφορικά με περιστατικά παραβίασης προσωπικών δεδομένων.

Σε απάντηση αυτού, η Ελληνική Αστυνομία (Τμήμα Ασφάλειας Πληροφοριών και Προστασίας Προσωπικών Δεδομένων της Διεύθυνσης Πληροφορικής) υπέβαλε στην Αρχή την υπ΄αριθμ. πρωτ. … και από …/2021 απάντησή της (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/1162/17-2-2021), στην οποία αναφέρει τα εξής σχετικά με τις ενέργειες στις οποίες προέβη για το εν λόγω περιστατικό:

α) Πρωταρχικά διερευνήθηκε από στελέχη της Υπηρεσίας, σε συνεργασία με τους αναδόχους υποστήριξης των συγκεκριμένων συστημάτων, το ενδεχόμενο διείσδυσης ή μόλυνσης των εξυπηρετητών του φορέα, χωρίς να διαπιστωθεί η οποιαδήποτε παράβαση.

β) Επιπλέον, για τον περιορισμό της μετάδοσης του EMOTET, ο φορέας προέβη στα εξής οργανωτικά και τεχνικά μέτρα:

i) για τους ενδιάμεσους mail relays: ισχυροποιήθηκαν οι κανόνες φιλτραρίσματος αντιβιοτικού, spam και κακόφημου περιεχομένου, καταχωρήθηκαν σε «μαύρη λίστα» κάποια mail domains και αποστολείς, δημιουργήθηκαν επιπλέον φίλτρα με λέξεις-κλειδιά στο περιεχόμενο των μηνυμάτων, ενώ εγκαταστάθηκαν οι τελευταίες ενημερώσεις λογισμικού του συστήματος,

ii) για τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου: ισχυροποιήθηκαν οι κανόνες φιλτραρίσματος αντιβιοτικού, spam και κακόφημου περιεχομένου, παρότι προκαλούν περισσότερες εσφαλμένες αναγνωρίσεις,

iii) για τους σταθμούς εργασίας: έγινε διαμόρφωση (format) σε τέσσερις μεμονωμένες περιπτώσεις όπου ευρέθησαν μολύνσεις, αναβαθμίστηκαν οι παλαιότερες εκδόσεις του MS Outlook (όπου χρησιμοποιούνταν), οι περιφερειακοί διαχειριστές έλεγξαν για περίπτωση μη ενημερωμένου αντιβιοτικού λογισμικού και μερίμνησαν για την ενημέρωσή του, ελέγχθηκαν όλοι οι σταθμοί εργασίας του φορέα για τυχόν ανεύρεση επιβλαβών μηνυμάτων, άλλαξε το συνθηματικό (password) ορισμένων χρηστών και ζητήθηκε η χρήση webmail αντί του MS Outlook,

εφαρμόστηκαν αλλαγές στις πολιτικές τομέα για τον περιορισμό δικαιωμάτων εκτέλεσης εφαρμογών, μακροεντολών και powershell,

iv) για την ενημέρωση τελικών χρηστών: διακινήθηκε έγγραφο ενημέρωσης μέσω εσωτερικής εφαρμογής αλληλογραφίας, ενημερώνοντας τους χρήστες για το κύμα κακόβουλων μηνυμάτων spam, πώς να τα χειριστούν και ποιον να ενημερώσουν,

v) για την ενημέρωση αρμόδιων αρχών: ενημερώθηκε το εθνικό CERT, η Δίωξη Ηλεκτρονικού Εγκλήματος, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και επηρεαζόμενοι οργανισμοί λόγω των αποστολέων τους.

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου και αφού άκουσε τον εισηγητή και τους βοηθούς εισηγητές, οι οποίοι (βοηθοί) αποχώρησαν μετά τη συζήτηση της υπόθεσης και πριν από τη διάσκεψη, μετά από διεξοδική συζήτηση

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Σύμφωνα με τις διατάξεις των άρθρων 51 και 55 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 (εφεξής, ΓΚΠΔ) και του άρθρου 9 του ν. 4624/2019 (ΦΕΚ Α΄ 137), η Αρχή έχει αρμοδιότητα να εποπτεύει την εφαρμογή των διατάξεων του ΓΚΠΔ, του νόμου αυτού και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων.
2. Σύμφωνα με το άρθρο 4 του ΓΚΠΔ, ως υπεύθυνος επεξεργασίας ορίζεται «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους*», ενώ ως εκτελών την επεξεργασία ορίζεται «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα*

για λογαριασμό του υπευθύνου της επεξεργασίας». Στη συγκεκριμένη περίπτωση, υπεύθυνος επεξεργασίας κατά την έννοια του άρθρου 4 του ΓΚΠΔ είναι η Ελληνική Αστυνομία.

3. Στο ίδιο άρθρο 4 ορίζεται η παραβίαση δεδομένων προσωπικού χαρακτήρα ως «*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*».
4. Σύμφωνα με το άρθρο 5 παρ. 3 του ΓΚΠΔ ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τις αρχές της επεξεργασίας που καθιερώνονται στην παράγραφο 1 του ιδίου άρθρου (συμπεριλαμβανομένης της εμπιστευτικότητας και ακεραιότητας των δεδομένων σύμφωνα με το άρθρο άρθρο 5 παρ. 1 στοιχ. στ'). Με άλλα λόγια, με τον ΓΚΠΔ υιοθετήθηκε ένα μοντέλο συμμόρφωσης με κεντρικό πυλώνα την εν λόγω αρχή της λογοδοσίας, ήτοι ο υπεύθυνος επεξεργασίας υποχρεούται να σχεδιάζει, εφαρμόζει και εν γένει λαμβάνει τα αναγκαία μέτρα και πολιτικές, προκειμένου η επεξεργασία των δεδομένων να είναι σύμφωνη με τις σχετικές νομοθετικές προβλέψεις και, επιπλέον, οφείλει να αποδεικνύει ο ίδιος και ανά πάσα στιγμή τη συμμόρφωσή του με τις αρχές του άρθρου 5 παρ. 1 ΓΚΠΔ.
5. Σύμφωνα με το άρθρο 24 παρ. 1 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με το ΓΚΠΔ, ενώ επίσης τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο. Περαιτέρω, σύμφωνα με το άρθρο 32 του ΓΚΠΔ, «*λαμβάνοντας 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, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να*

διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: (…) δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας». Εξάλλου, στην παράγραφο 2 αυτού, αναφέρεται ότι «*κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία*».

6. Αναφορικά με τη περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα, ο ΓΚΠΔ ορίζει συγκεκριμένες υποχρεώσεις για τους υπευθύνους επεξεργασίας. Συγκεκριμένα, στο άρθρο 33 αυτού, ορίζεται 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 αρμόδια εποπτική αρχή[2], εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.
7. Στην παράγραφο 3 του άρθρου 33 ορίζεται η πληροφορία που πρέπει κατ' ελάχιστο να περιέχεται σε μία τέτοια γνωστοποίηση, στην οποία συμπεριλαμβάνονται - μεταξύ άλλων - οι ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς επίσης και 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. Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.

[2] Λαμβάνοντας υπόψη το άρθρο 55 του ΓΚΔΠ περί των αρμοδιοτήτων των εποπτικών αρχών, αρμόδια για το εν λόγω περιστατικό είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

8. Περαιτέρω, σύμφωνα με το άρθρο 34 του ΓΚΠΔ, όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων. Σε αυτήν την ανακοίνωση 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). Η ανακοίνωση στο υποκείμενο των δεδομένων δεν απαιτείται, εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις: α) ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση, β) ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, γ) προϋποθέτει δυσανάλογες προσπάθειες (οπότε, στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο).
9. Σύμφωνα με το άρθρο 12 παρ. 1 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία που αναφέρεται στα άρθρα 13 και 14 (τα οποία αφορούν τις πληροφορίες που παρέχονται στα υποκείμενα των δεδομένων είτε τα δεδομένα συλλέγονται από τα ίδια τα υποκείμενα είτε όχι) και κάθε ανακοίνωση στο πλαίσιο των άρθρων 15 έως 22 (τα οποία αφορούν τα δικαιώματα των υποκειμένων των δεδομένων, συμπεριλαμβανομένου του δικαιώματος πρόσβασης του άρθρου 15) αλλά και του προαναφερθέντος άρθρου 34 σχετικά με την επεξεργασία, σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή. Ειδικά ως προς το δικαίωμα πρόσβασης του άρθρου 15 του ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, πρόσβαση σε κάθε πληροφορία σχετικά με την επεξεργασία.

10. Στη συγκεκριμένη περίπτωση, πρόκειται για περιστατικό κυβερνοασφάλειας το οποίο έλαβε χώρα σε παγκόσμιο επίπεδο και έχει ονομαστεί ως EMOTET[3] πλήττοντας πλήθος φορέων. Το περιστατικό αυτό συνδέεται με διάχυση κακόβουλου λογισμικού. Σύμφωνα με ανακοίνωση της Ευρωπόλ στις 27/1/2021[4], το εν λόγω κακόβουλο λογισμικό εγκαθίσταται στους σταθμούς εργασίας των θυμάτων μέσω «μολυσμένων» συνημμένων αρχείων σε μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία για να παραπλανήσουν τους αποδέκτες τους εμφανιζόντουσαν με διάφορους τρόπους, όπως ως δήθεν απόδειξη πληρωμής ή πληροφορίες περί του COVID-19. Τα συνημμένα μολυσμένα αρχεία ήταν τύπου Word, με τα οποία ο χρήστης, εφόσον τα «ανοίγει», προτρέπεται να ενεργοποιήσει μακροντολές, το οποίο με τη σειρά του επιτρέπει την εγκατάσταση του κακόβουλου λογισμικού στο σταθμό εργασίας του θύματος. Στην ίδια ανακοίνωση της Ευρωπόλ αναφέρονται τρόποι με τους οποίους γενικά μπορεί κανείς να αντιμετωπίσει τέτοιου τύπου επιθέσεις όπως αυτής του EMOTET, οι οποίοι βασίζονται σε συνδυασμό εργαλείων κυβερνοασφάλειας (αντιβιοτικά λογισμικά και επικαιροποιημένα λειτουργικά συστήματα) και επαγρύπνησης των χρηστών ώστε να μην «ανοίγουν» ύποπτα συνημμένα αρχεία.
11. Εφόσον από μία επίθεση κυβερνοασφάλειας έχει επέλθει παραβίαση δεδομένων προσωπικού χαρακτήρα, τότε πρόκειται – σύμφωνα με το άρθρο 4 του ΓΚΠΔ - και για περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα. Αυτό φαίνεται ότι ισχύει στην εν λόγω περίπτωση, σύμφωνα και με την αρχική αναφορά του καταγγέλλοντα αλλά και με τη φύση και τα χαρακτηριστικά της επίθεσης[5].
12. Για τη συγκεκριμένη περίπτωση, δεν υπήρξε γνωστοποίηση του εν λόγω περιστατικού στην Αρχή όπως επιτάσσει το άρθρο 33 του ΓΚΠΔ. Σημειώνεται ότι σαφώς υπάρχουν κίνδυνοι - και μάλιστα υψηλοί - για τα επηρεαζόμενα πρόσωπα και, άρα, το εν λόγω περιστατικό δεν εμπίπτει στην εξαίρεση από την υποχρέωση

[3] Είναι το όνομα του σχετικού botnet.
[4] Βλ. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
[5] Προς τούτο, πρέπει να σημειωθεί ότι, στην προαναφερθείσα ανακοίνωση της Ευρωπόλ, αναφέρεται ειδικότερα ότι κατόπιν ενεργειών της Αστυνομίας της Ολλανδίας, έχει εντοπιστεί βάση δεδομένων με στοιχεία όπως ηλεκτρονικές διευθύνσεις, ονόματα χρηστών (user names) και συνθηματικά, τα οποία διέρρευσαν στο πλαίσιο της επίθεσης EMOTET, όπου και μπορεί κανείς να δει αν τα στοιχεία του έχουν διαρρεύσει.

γνωστοποίησής του, ακριβώς λόγω του γεγονότος ότι μηνύματα ηλεκτρονικού ταχυδρομείου «υποδύονται» ότι έχουν ως αποστολέα την Ελληνική Αστυνομία (και άρα, ένας καλόπιστος παραλήπτης τους χωρίς εμπειρία σε θέματα ασφάλειας, θα μπορούσε να τα «ανοίξει»), ενώ εξάλλου το περιεχόμενο των μηνυμάτων εμπεριέχει πληροφορίες – συμπεριλαμβανομένων προσωπικών δεδομένων - που υπήρχαν σε προηγούμενα νόμιμα ηλεκτρονικά μηνύματα, οπότε και γεννάται ζήτημα μη εξουσιοδοτημένης πρόσβασης και διάδοσης σε δεδομένα τα οποία πολίτες υπέβαλαν στην Ελληνική Αστυνομία. Μάλιστα, στη συγκεκριμένη περίπτωση ενδέχεται να γεννάται και ζήτημα παραβίασης του απορρήτου της επικοινωνίας, που είναι θεμελιώδες δικαίωμα κατά το άρθρο 19 του Συντάγματος και το άρθρο 7 του ΧΘΔ της ΕΕ, γεγονός που ενισχύει τον ισχυρισμό περί υψηλών κινδύνων από το εν λόγω περιστατικό. Ακόμα και αν θεωρηθεί ότι, αφού η επίθεση EMOTET έγινε ευρέως γνωστή, χρειαζόταν χρόνος για να διερευνηθεί και να αποσαφηνιστεί αν πράγματι πρόκειται για περιστατικό παραβίασης προσωπικών δεδομένων για το φορέα, το περιεχόμενο της σχετικής αναφοράς του καταγγέλλοντα καταδεικνύει υψηλή πιθανότητα για μία τέτοια περίπτωση και άρα, η Ελληνική Αστυνομία ως υπεύθυνος επεξεργασίας όφειλε να διερευνήσει αμέσως το περιστατικό. Εξάλλου, όπως αποδείχτηκε, υπήρξαν πράγματι «μολυσμένοι» σταθμοί εργασίας εντός του υπευθύνου επεξεργασίας, η ύπαρξη των οποίων συνετέλεσε στην επιτυχή επίθεση (διότι διαφορετικά, αν δεν είχε πληγεί κανένα υποσύστημα της Ελληνικής Αστυνομίας, το εν λόγω περιστατικό δεν θα αφορούσε την Ελληνική Αστυνομία ως υπεύθυνο επεξεργασίας[6]).

Καίτοι η Ελληνική Αστυνομία, στο τελευταίο έγγραφό της προς την Αρχή, αναφέρει ότι, στο πλαίσιο αντιμετώπισης του περιστατικού ενημέρωσε την Αρχή, τέτοια ενημέρωση κατ' ουσίαν δεν υπήρξε (αφού η μόνη ενημέρωση ήταν η διαβίβαση της απάντησής της προς τον καταγγέλλοντα, η οποία απάντηση μάλιστα – όπως αναλύεται και στη συνέχεια – δεν είχε πλήρεις πληροφορίες).

[6] Π.χ. μία γενική αποστολή μη γνήσιων ηλεκτρονικών μηνυμάτων που υποδύονται ως αποστολέα τους την Ελληνική Αστυνομία, δεν συνιστά συμβάν ασφάλειας για την Ελληνική Αστυνομία αν η αποστολή αυτή δεν βασίζεται σε πλήγμα οποιουδήποτε υποσυστήματος της Ελληνικής Αστυνομίας.

13. Πέραν της μη γνωστοποίησης του περιστατικού στην Αρχή, δεν υπήρξε επίσης ενημέρωση των θιγόμενων προσώπων, σύμφωνα με το άρθρο 34 του ΓΚΠΔ. Λόγω των υψηλών κινδύνων που απορρέουν από το εν λόγω περιστατικό, όπως αναλύθηκαν ανωτέρω, προκύπτει ότι μία τέτοια ενημέρωση ήταν υποχρεωτική. Εξάλλου, σύμφωνα με την παρ. 3 του ιδίου άρθρου, εάν η ενημέρωση των θιγόμενων προσώπων δεν μπορεί να πραγματοποιηθεί διότι προϋποθέτει δυσανάλογες προσπάθειες (κάτι το οποίο πιθανότατα θα μπορούσε να τεκμηριωθεί για την εν λόγω περίπτωση, λόγω της ιδιάζουσας φύσης του περιστατικού), τότε γίνεται αντ' αυτής δημόσια ανακοίνωση ή λαμβάνεται παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο. Δεν προκύπτει στη συγκεκριμένη περίπτωση ότι έλαβε χώρα μία τέτοια γενικού χαρακτήρα ενημέρωση.
14. Επισημαίνεται επίσης ότι οι πληροφορίες που παρείχε η Ελληνική Αστυνομία στον καταγγέλλοντα (βλ. ανωτέρω), στο πλαίσιο του αιτήματός του το οποίο αποτελεί ειδική έκφανση του δικαιώματος πρόσβασης, δεν μπορούν να θεωρηθούν ως πλήρεις, αφού περιορίζονται στο να αναφέρουν ότι τα μηνύματα, τα οποία ο ίδιος έλαβε, δεν προέρχονται από την Ελληνική Αστυνομία και εντάσσονται στο πλαίσιο της κυβερνοεπίθεσης με την επωνυμία ΕΜΟΤΕΤ, χωρίς να περιγράφεται ότι η Ελληνική Αστυνομία έχει προβεί σε κατάλληλες ενέργειες για την αντιμετώπισή του. Ουσιαστικά, από την απάντηση της Ελληνικής Αστυνομίας προς τον καταγγέλλοντα δεν προκύπτει με σαφήνεια ότι υπήρξε περιστατικό ασφάλειας για την Ελληνική Αστυνομία, εκ του οποίου επήλθε παραβίαση προσωπικών δεδομένων του.
15. Στο τελευταίο της έγγραφο προς την Αρχή, η Ελληνική Αστυνομία περιγράφει σύνολο ενεργειών στις οποίες προέβη για τη διερεύνηση του περιστατικού. Καίτοι οι ενέργειες αυτές φαίνεται να είναι καταρχήν στη σωστή κατεύθυνση, εν τούτοις δεν προκύπτει ότι διερευνήθηκαν ενδελεχώς οι τυχόν συνέπειες του περιστατικού (π.χ. δεν διερευνήθηκε για πόσα πρόσωπα υπήρξε διαρροή δεδομένων, καθώς επίσης και τι είδους ήταν τα δεδομένα αυτά), με αποτέλεσμα να μην έχει γίνει η σχετική αξιολόγηση των συνεπειών - η οποία ήταν υποχρεωτική σύμφωνα με τα όσα ορίζονται στα άρθρα 33 και 34 του ΓΚΠΔ. Περαιτέρω, δεν προκύπτει με σαφήνεια ότι τα εν λόγω μέτρα – αν και, όπως προαναφέρθηκε, είναι σαφώς στη σωστή κατεύθυνση - υιοθετήθηκαν κατόπιν ανάλυσης των κινδύνων για τη

συγκεκριμένη περίπτωση (δηλαδή δεν παρατίθεται ειδική τεκμηρίωση της καταλληλότητας και πληρότητας των μέτρων εν όψει των κινδύνων που καλούνται να αντιμετωπίσουν). Τέλος, από τις ενέργειες αυτές προκύπτει ότι υπήρχαν περιπτώσεις όπου δεν είχαν επικαιροποιηθεί λειτουργικά συστήματα ή αντιβιοτικά λογισμικά, η παράλειψη δε αυτή καταδεικνύει μία εν γένει σημαντική έλλειψη διαδικασιών για επικαιροποίηση και επανεξέταση μέτρων ασφάλειας (τούτο ισχύει ανεξαρτήτως αν η εν λόγω μη επικαιροποίηση συνετέλεσε στο εν λόγω συμβάν παραβίασης δεδομένων ή όχι).

16. Η Αρχή, λαμβάνοντας υπόψη τις ανωτέρω διαπιστωθείσες παραβάσεις των άρθρων 32, 33 και 34 του ΓΚΠΔ αναφορικά με την ασφάλεια της επεξεργασίας, αλλά και του άρθρου 15 του ΓΚΠΔ ως προς την πληρότητα της ανταπόκρισης σε δικαίωμα πρόσβασης, και συνυπολογίζοντας αφενός το μέγεθος της κυβερνοεπίθεσης EMOTET για την οποία είναι γνωστό ότι έπληξε πολύ μεγάλο αριθμό συστημάτων ανά τον κόσμο και αφετέρου ότι ο υπεύθυνος επεξεργασίας προέβη σε ενέργειες για την αντιμετώπισή της και για αποτροπή αντίστοιχης μελλοντικής επίθεσης, κρίνει ότι συντρέχουν οι προϋποθέσεις επιβολής σε βάρος του της κατ' άρθρο 58 παρ. 2 β΄ του ΓΚΠΔ διοικητικής κύρωσης, όπως αναφέρεται στο διατακτικό της παρούσας, η οποία κρίνεται ανάλογη με τη βαρύτητα των παραβάσεων.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή,

Απευθύνει στην Ελληνική Αστυνομία, ως υπεύθυνο επεξεργασίας, επίπληξη για τις ως άνω διαπιστωθείσες παραβιάσεις των άρθρων 32-34 και 15 του ΓΚΠΔ.

Ο Πρόεδρος	**Η Γραμματέας**
Κωνσταντίνος Μενουδάκος	**Ειρήνη Παπαγεωργοπούλου**