Αθήνα, 28 Ιουλίου 2026
Αριθμ. Πρωτ. 3163

ΑΠΟΦΑΣΗ 15/2026

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής Αρχή), συνήλθε, μετά από πρόσκληση του εκτελούντος χρέη Προέδρου Αναπληρωτή Προέδρου της, Γεωργίου Μπατζαλέξη, σε συνεδρίαση μέσω τηλεδιάσκεψης στις 11-12-2025, μετά από αναβολή από τη διάσκεψη στις 2-12-2025, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο αναπληρωτής Πρόεδρος, Γεώργιος Μπατζαλέξης και τα τακτικά μέλη Σπύρος Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, Χαράλαμπος Ανθόπουλος, Χρήστος Καλλονιάτης και Κατερίνα Ηλιάδου, καθώς και τα αναπληρωματικά μέλη Δημοσθένης Βουγιούκας, ως εισηγητής, και Μαρία Ψάλλα, αντικαθιστώντας το τακτικό μέλος Γρηγόρη Τσόλια, ο οποίος αν και εκλήθη νομίμως εγγράφως δεν παρέστη λόγω κωλύματος. Παρόντες, με εντολή του Αν. Προέδρου, χωρίς δικαίωμα ψήφου, ήταν η Γεωργία Παναγοπούλου και ο Ιωάννης Λυκοτραφίτης, ειδικοί επιστήμονες-πληροφορικοί, ως βοηθοί εισηγητή και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών υποθέσεων της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα κατωτέρω:

Το Υπουργείο Κοινωνικής Συνοχής και Οικογένειας (εφεξής ΥΚΟΙΣΟ), υπέβαλε στην Αρχή, με βάση τον Κανονισμό (ΕΕ) 2016/679 (Γενικός Κανονισμός Προστασίας Δεδομένων – εφεξής ΓΚΠΔ), την με αρ. πρωτ. Γ/ΕΙΣ/1943/07-03-2025 γνωστοποίηση περιστατικού παραβίασης προσωπικών δεδομένων. Σχετικά υποβλήθηκε και από την Ελληνική Εταιρεία Τοπικής Ανάπτυξης και Αυτοδιοίκησης Α.Ε. (εφεξής ΕΕΤΑΑ) η με αρ. πρωτ. Γ/ΕΙΣ/1981/10-03-2025 γνωστοποίηση για το ίδιο περιστατικό παραβίασης προσωπικών δεδομένων. Οι γνωστοποιήσεις αφορούσαν σε παραβιάσεις Πληροφοριακών Συστημάτων που λειτουργεί η ΕΕΤΑΑ με την ιδιότητά του

εκτελούντος την επεξεργασία για λογαριασμό του υπευθύνου επεξεργασίας ΥΚΟΙΣΟ.

Στη συνέχεια, σε απάντηση μηνύματος ηλεκτρονικού ταχυδρομείου (με αρ. πρωτ. Γ/ΕΞΕ/846/10-03-2025) της Αρχής προς το ΥΚΟΙΣΟ, με το οποίο ζητήθηκαν διευκρινίσεις σχετικά με το είδος/κατηγορίες των δεδομένων που επηρεάστηκαν από το περιστατικό, το είδος/κατηγορίες και τον αριθμό των υποκειμένων που επηρεάστηκαν, τους ρόλους των εμπλεκόμενων φορέων ως προς την επεξεργασία και τα αρχεία που επηρεάστηκαν, το ΥΚΟΙΣΟ υπέβαλε το με αρ. πρωτ. Γ/ΕΙΣ/2201/17-03-2025 έγγραφο στο οποίο αναφέρονται, μεταξύ άλλων, τα εξής:

Η ΕΕΤΑΑ, σύμφωνα με την από 6-3-2025 αναφορά της προς το ΥΚΟΙΣΟ, δέχθηκε σειρά κυβερνοεπιθέσεων, οι οποίες έγιναν αρχικά αντιληπτές στις 3-3-2025 και συνέχιζαν να εκδηλώνονται μέχρι και στις 5-3-2025, οπότε και τεκμηριωμένα διαπιστώθηκαν από την ΕΕΤΑΑ. Οι εν λόγω κυβερνοεπιθέσεις αφορούσαν προσωπικά δεδομένα που τηρούνται από την ΕΕΤΑΑ για τις ανάγκες υλοποίησης της Δράσης (α) «Προώθηση και υποστήριξη παιδιών για την ένταξή τους στην προσχολική εκπαίδευση καθώς και για τη πρόσβαση παιδιών σχολικής ηλικίας, εφήβων και ατόμων με αναπηρία, σε υπηρεσίες δημιουργικής απασχόλησης» (πρόγραμμα «Βρεφονηπιακοί Σταθμοί») των περιόδων 2014-2015 έως και 2024-2025 και της πιλοτικής εφαρμογής της Δράσης (β) «Νταντάδες της Γειτονιάς».

Επισημαίνεται ότι στις ως άνω δράσεις, σύμφωνα με τα προβλεπόμενα στις ΚΥΑ υπ' αριθμ. 99310 ΕΞ 2024 της 10-7-2024 (ΦΕΚ Β 4056) και ΚΥΑ υπ' αριθμ. 6457 της 27-1-2022 (ΦΕΚ Β 205) αντίστοιχα. Ειδικότερα, στη μεν (α) ανωτέρω δράση, η ΕΕΤΑΑ αποτελεί τον μοναδικό εκτελούντα την επεξεργασία και έχει την ευθύνη για την υλοποίηση του συνόλου των επεξεργασιών που αφορούν στην υλοποίηση, παρακολούθηση και διαχείριση του φυσικού και οικονομικού αντικειμένου αυτής· στη δε (β) ανωτέρω δράση, η ΕΕΤΑΑ έχει την ιδιότητα του συνεκτελούντος την επεξεργασία, από κοινού με την «Εθνικό Δίκτυο Υποδομών Τεχνολογίας και Έρευνας Α.Ε.» (ΕΔΥΤΕ), με τον ρόλο της ΕΔΥΤΕ όμως να περιορίζεται κυρίως στις επεξεργασίες που αφορούν στη διεκπεραίωση των πληρωμών και τη διαχείριση του οικονομικού αντικειμένου του έργου.

Πιο συγκεκριμένα, ως προς τα εν λόγω περιστατικά ασφαλείας, σύμφωνα με τα αρμόδια στελέχη της Δ/νσης Πληροφορικής και Τεκμηρίωσης της ΕΕΤΑΑ, που διαπίστωσαν το γεγονός, η παραβίαση προήλθε από κυβερνοεπιθέσεις της κατηγορίας “Ransomware”, οι οποίες εκδηλώθηκαν σε δύο φάσεις και συνολικά διήρκεσε από τις πρώτες πρωινές ώρες της 1-3-2025 μέχρι και τις 14:00 της 5-3-2025, οπότε και ενημερώθηκε σχετικώς η Διοίκηση και ο ΥΠΔ της ΕΕΤΑΑ.

Ως αποτέλεσμα των εν λόγω επιθέσεων, κρυπτογραφήθηκαν και ενδεχομένως μεταφορτώθηκαν/υπεκλάπησαν (σύμφωνα με σχετικό σημείωμα που άφησαν οι επιτεθέντες) οι Βάσεις Δεδομένων των Πληροφοριακών Συστημάτων που υποστηρίζουν την υλοποίηση των δύο ανωτέρω αναφερόμενων Δράσεων. Τονίζεται, επίσης, ότι το πεδίο εφαρμογής της εν λόγω παραβίασης περιορίζεται στους διακομιστές και τις Βάσεις Δεδομένων που τηρούνται εντός των εγκαταστάσεων (on-site) της ΕΕΤΑΑ και δεν επεκτάθηκε σε Πληροφοριακά Συστήματα που φιλοξενούνται από άλλους παρόχους στο νέφος.

Δεδομένου ότι στις 14:00 την 5-3-2025 το περιστατικό βρισκόταν ακόμα σε εξέλιξη, χωρίς να είναι δυνατός ο περιορισμός του, τα αρμόδια στελέχη της ΕΕΤΑΑ προχώρησαν στον τερματισμό των διεργασιών του συνόλου των εμπλεκόμενων Πληροφοριακών Συστημάτων και τη θέση τους σε κατάσταση «εκτός λειτουργίας». Τούτο κατέστησε αδύνατη την εξ οικείων διερεύνηση της προέλευσης της κυβερνοεπίθεσης, καθώς και της ευαλωτότητας που της επέτρεψε να εκδηλωθεί.

Από την έρευνα των αρμοδίων στελεχών της ΕΕΤΑΑ, εντοπίστηκε η ευαλωτότητα, την οποία εκμεταλλεύτηκε το κακόβουλο λογισμικό, και η οποία περιγράφεται στο Εμπιστευτικό Παράρτημα, Σημείο 1.

Επίσης, περιγράφονται στην από 6-3-2025 αναφορά της ΕΕΤΑΑ προς το ΥΚΟΙΣΟ τα μέτρα τα οποία είχαν ληφθεί πριν το περιστατικό, τα οποία περιλαμβάνονται στο Εμπιστευτικό Παράρτημα, Σημείο 2, καθώς και τα μέτρα που ελήφθησαν αμέσως μετά το περιστατικό, τα οποία περιλαμβάνονται στο Εμπιστευτικό Παράρτημα, Σημείο 3 της παρούσας.

Δεδομένου ότι στην προκειμένη περίπτωση, η κυβερνοεπίθεση ενδέχεται να επέτρεψε σε μη εξουσιοδοτημένα πρόσωπα να αποκτήσουν πρόσβαση σε

προσωπικά δεδομένα που τηρεί η ΕΕΤΑΑ, το εν λόγω περιστατικό συνιστά παραβίαση της εμπιστευτικότητας των εν λόγω προσωπικών δεδομένων. Ταυτόχρονα, η θέση εκτός λειτουργίας των εμπλεκόμενων Πληροφοριακών Συστημάτων συνιστά παραβίαση και της διαθεσιμότητας των προσωπικών δεδομένων. Τέλος, δεδομένου ότι στην παρούσα φάση εκτιμάται ότι υπάρχει η δυνατότητα επαναφοράς και ανασύστασης των Βάσεων Δεδομένων που επλήγησαν, δεν διαπιστώνεται παραβίαση της ακεραιότητας των παρ' αυτών τηρούμενων προσωπικών δεδομένων.

Στην ίδια συμπληρωματική αναφορά περιστατικού το ΥΚΟΙΣΟ αναφέρει ως προς τα επηρεαζόμενα υποκείμενα και τα αντίστοιχα προσωπικά δεδομένα:

Όσον αφορά στη Δράση «Προώθηση και υποστήριξη παιδιών για την ένταξή τους στην προσχολική εκπαίδευση καθώς και για την πρόσβαση παιδιών σχολικής ηλικίας, εφήβων και ατόμων με αναπηρία, σε υπηρεσίες δημιουργικής απασχόλησης», η παραβίαση αφορά ιδίως στα προσωπικά δεδομένα των αιτούντων συμμετοχή στο Πρόγραμμα, των ετέρων μελών (συζύγους/συντρόφους) καθώς και των ανηλίκων τέκνων αυτών. Πιο συγκεκριμένα, τα στοιχεία αφορούν:

α) Στο ωφελούμενο πρόσωπο (βρέφος, νήπιο και παιδί προσχολικής εκπαίδευσης, καθώς και το παιδί σχολικής ηλικίας, ο έφηβος και το άτομο με αναπηρία, που εμπίπτει στις κατηγορίες και πληρούν τις προϋποθέσεις της εκάστοτε ΚΥΑ προκειμένου να λάβουν «αξία τοποθέτησης» (voucher). Τα προσωπικά δεδομένα αυτής της κατηγορίας περιλαμβάνουν: α. Ονοματεπώνυμο, πατρώνυμο, β. Ημ/νία γέννησης, γ. Φύλο, δ. ΑΦΜ ε. ΑΜΚΑ, στ. Ένδειξη ΑμεΑ και σχετικά πιστοποιητικά, η. Ένδειξη αναδοχής/επιμέλειας/επιτροπείας, ζ. Στοιχεία εισοδήματος (εισόδημα και αναλογών φόρος), η. Στοιχεία ημερήσιας παρουσίας στις Δομές της Δράσης (χρόνος εισόδου και εξόδου)

β) Στον νόμιμο εκπρόσωπο/αιτούντα (γονέας ή πρόσωπο που έχει τη γονική μέριμνα ή την επιμέλεια, ο ανάδοχος γονέας, ο επίτροπος ή ο συμπαραστάτης του ωφελούμενου). Τα προσωπικά δεδομένα αυτής της κατηγορίας περιλαμβάνουν: α. Ονοματεπώνυμο, πατρώνυμο, μητρώνυμο, β. Ημερομηνία γέννησης, γ. Ιθαγένεια και στην περίπτωση αλλοδαπών από χώρες εκτός ΕΕ, Άδεια Διαμονής ή σχετικής αίτησης ανανέωσης, δ. Στοιχεία διεύθυνσης και επικοινωνίας, ε. Οικογενειακή κατάσταση, στ. Εργασιακή κατάσταση ιδίου και συζύγου/συντρόφου, ζ. ΑΦΜ και ΔΟΥ ιδίου και

συζύγου/συντρόφου, η. ΑΜΚΑ ιδίου και συζύγου/συντρόφου, θ. Φύλο, ι. Ένδειξη ΑμεΑ ιδίου ή/και συζύγου/συντρόφου ή/και τέκνου, ια. Στοιχεία τέκνων κ.λπ. εξαρτώμενων μελών (ονοματεπώνυμο, ημ/νία γέννησης, ένδειξη ΑμεΑ), ιβ. Στοιχεία εισοδήματος ιδίου και συζύγου/συντρόφου (εισόδημα και αναλογών φόρος)

γ) Στον νόμιμο εκπρόσωπο Φορέα/Δομής (νόμιμος εκπρόσωπος του Φορέα που παρέχει θέσεις προσχολικής αγωγής και φροντίδας και δημιουργικής απασχόλησης παιδιών ή και ατόμων με αναπηρία, στο πλαίσιο της Δράσης). Τα προσωπικά δεδομένα αυτής της κατηγορίας περιλαμβάνουν: α. Ονοματεπώνυμο, όνομα πατρός και μητρός, β. Ημ/νία γέννησης, γ. Στοιχεία διεύθυνσης και επικοινωνίας, δ. ΑΜΦ, ε. Ένδειξη ασφαλιστικής και φορολογικής ενημερότητας, στ. IBAN Τραπεζικού λογαριασμού, ζ. Αμοιβή για παροχή υπηρεσιών στο πλαίσιο της δράσης.

δ) Στο στέλεχος Φορέα/Δομής (εργαζόμενος σε φορέα της παρ. γ ανωτέρω). Τα προσωπικά δεδομένα αυτής της κατηγορίας περιλαμβάνουν: α. Ονοματεπώνυμο, β. ΑΦΜ, γ. Ιδιότητα

Σύμφωνα με την ίδια αναφορά, δεδομένου του εύρους που καλύπτει η περίοδος τήρησης των δεδομένων που παραβιάστηκαν (συνολικά 10 έτη), αδρομερώς υπολογίζεται ότι το πλήθος των αιτήσεων μπορεί να ανέρχεται σε 700.000 και αφορά σε 2.500.000 υποκείμενα περίπου. Όσον αφορά στην πιλοτική εφαρμογή της Δράσης *«Νταντάδες της Γειτονιάς»*, η παραβίαση αφορά στα προσωπικά δεδομένα του ωφελούμενου προσώπου (άτομο που έχει την επιμέλεια βρέφους ή νηπίου). Λόγω της πιλοτικής φύσης του έργου, ο συνολικός αριθμός των ως άνω υποκειμένων ανέρχεται στα 700 άτομα περίπου. Τα προσωπικά δεδομένα αυτής της Δράσης περιλαμβάνουν: α. Ονοματεπώνυμο και πατρώνυμο, β. ΑΦΜ, γ. Ημερομηνία γέννησης, δ. Στοιχεία διεύθυνσης και επικοινωνίας, ε. IBAN Τραπεζικού λογαριασμού.

Στη συνέχεια, με το με αρ. πρωτ. Γ/ΕΙΣ/2687/01-04-2025 μήνυμα ηλεκτρονικού ταχυδρομείου, το ΥΚΟΙΣΟ ενημέρωσε την Αρχή ότι εξέδωσε δελτίο τύπου στις 31-3-2025 σχετικά με το περιστατικό παραβίασης, το οποίο αναρτήθηκε και στην

ιστοσελίδα του ΥΚΟΙΣΟ[1]. Επίσης, στο εν λόγω μήνυμα ανέφερε ότι, σε συνέχεια των ενεργειών του, το ΥΚΟΙΣΟ προτίθεται να ενημερώσει κατ' ιδίαν τα υποκείμενα των δεδομένων και ότι μόλις ολοκληρωθεί η σχετική ενέργεια θα ενημερωθεί η Αρχή.

Ακολούθως, με το με αρ. πρωτ. Γ/ΕΙΣ/5253/12-06-2025 έγγραφο το ΥΚΟΙΣΟ ενημέρωσε την Αρχή ότι η κατ' ιδίαν ενημέρωση των υποκειμένων, των οποίων τα δεδομένα περιλαμβάνονταν στα Πληροφοριακά Συστήματα που παραβιάστηκαν, ολοκληρώθηκε την 10-6-2025 μέσω της αποστολής μηνυμάτων στις διευθύνσεις επικοινωνίας που είχαν δηλώσει (e-mails / sms). Τα μηνύματα εστάλησαν από το ΥΚΟΙΣΟ και το λεκτικό είχε ως εξής:

«*Το ΥΚΟΙΣΟ σας ενημερώνει ότι την Τετάρτη 5-3-2025 έγινε κυβερνοεπίθεση στο πληροφοριακό σύστημα της Ελληνικής Εταιρείας Τοπικής Ανάπτυξης και Αυτοδιοίκησης Α.Ε. (ΕΕΤΑΑ) που διαχειρίζεται τις δράσεις Παιδικών Σταθμών και «Νταντάδες της Γειτονιάς» για λογαριασμό του Υπουργείου. Το πληροφοριακό σύστημα του Υπουργείου δεν παραβιάστηκε. Παρ' όλα αυτά το ΥΚΟΙΣΟ ως Υπεύθυνος επεξεργασίας προέβη άμεσα σε γνωστοποίηση του περιστατικού στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και έδωσε εντολή στην ΕΕΤΑΑ να προβεί σε όλες τις απαραίτητες ενέργειες για την άμεση αποκατάσταση του πληροφοριακού συστήματος ώστε να είναι σε θέση να ανταποκριθεί στις υποχρεώσεις του που απορρέουν από τις παραπάνω δράσεις. Δεδομένου ότι η κυβερνοεπίθεση ενδέχεται να επέτρεψε σε μη εξουσιοδοτημένα πρόσωπα να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα σας, το Υπουργείο εφιστά την προσοχή των αιτούντων, δικαιούχων και απασχολούμενων στις πιο πάνω δράσεις να είναι ιδιαιτέρως προσεκτικοί και να μην ανταποκρίνονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, sms ή τηλεφωνικές κλήσεις με τις οποίες καλούνται να παράσχουν προσωπικά δεδομένα τους (ιδίως δεδομένα οικονομικής φύσεως, όπως αριθμούς τραπεζικών λογαριασμών ή πιστωτικών καρτών κλπ) ή να προβούν σε ενέργειες σχετικές με τις ανωτέρω δράσεις, καθώς μπορεί να συνιστούν κακόβουλες* ενέργειες.»

Για κανένα από τα αποσταλέντα μηνύματα δεν επέστρεψε συστημικά ενημέρωση ότι

[1] https://minscfa.gov.gr/enimerosi-ypokeimenon-vasei-tou-arthrou-34-tou-genikou-kanonismou-prostasias-dedomenon-ee-2016-679-gkpd/

δεν παρελήφθη ή ότι ήταν ανεπιτυχής η αποστολή του.

Στη συνέχεια, η Αρχή κάλεσε το ΥΚΟΙΣΟ και την ΕΕΤΑΑ με τις υπ' αρ. πρωτ. Γ/ΕΞΕ/3025/01-09-2025 και Γ/ΕΞΕ/3030/01-09-2025 κλήσεις, αντίστοιχα, σε ακρόαση, μέσω τηλεδιάσκεψης. Στην τηλεδιάσκεψη της 09-09-2025 συνδέθηκαν οι: Γρηγόρης Λαζαράκος, δικηγόρος-εκπρόσωπος της ΕΕΤΑΑ με ΑΜ ΔΣ…, Α, ΥΠΔ του ΥΚΟΙΣΟ με ΑΜ ΔΣ…, Ιωάννης Γκόλνας, δικηγόρος με ΑΜ ΔΣ…, Γεωργία Κορμά, δικηγόρος-συνεργάτης στο Γραφείο Υπουργού Κοινωνικής Κοινωνικής Συνοχής και Οικογένειας με ΑΜΔΣ…, Γεωργία Δρεμέτσικα, δικηγόρος-συνεργάτης στο Γραφείο Υπουργού Κοινωνικής Κοινωνικής Συνοχής και Οικογένειας με ΑΜ ΔΣ…, Χρύσα Παπαϊακώβου, δικηγόρος-συνεργάτης Υφυπουργού Κοινωνικής Συνοχής και Οικογένειας με ΑΜ ΔΣ…, Β, Διευθύντρια στο Γραφείο Γενικής Γραμματέως Ισότητας και Ανθρωπίνων Δικαιωμάτων, Σταυρούλα Γεωργουλέα, δικηγόρος-συνεργάτης στο Γραφείο του Γενικού Γραμματέα Δημογραφικής και Στεγαστικής Πολιτικής με ΑΜ .. ΔΣ …, Γ, Προϊσταμένη του τμήματος Ενίσχυσης Οικογενειακής Συνοχής της Δ/νσης Προστασίας Παιδιού και Οικογένειας, Δ, Προϊσταμένη του Τμήματος Διοίκησης Ανθρώπινου Δυναμικού της Δ/νσης Υποστήριξης Ανθρώπινου Δυναμικού και Υπηρεσιών του ΥΚΟΙΣΟ και Ε, Αν. προϊστάμενος Δ/νσης Ηλ. Διακυβέρνησης ΥΚΟΙΣΟ. Ο εκπρόσωπος της ΕΕΤΑΑ αιτήθηκε την αναβολή εξέτασης της υπόθεσης λόγω Γενικής Συνέλευσης της εταιρείας. Στη συνέχεια, δόθηκε η 21/10/2025 και ώρα 10:45 ως νέα ημερομηνία εξέτασης της υπόθεσης, χωρίς την αποστολή νέας κλήσης.

Στην τηλεδιάσκεψη της 21-10-2025 συνδέθηκαν οι: Εκ μέρους του ΥΚΟΙΣΟ:Α, DPO, δικηγόρος με ΑΜ ΔΣ…, Σταύρος Ζουμπουλίδης, δικηγόρος με ΑΜ ΔΣ…, Γεωργία Κορμά, συνεργάτης στο Γραφείο Υπουργού Κοινωνικής Συνοχής και Οικογένειας, δικηγόρος με ΑΜ ΔΣ…, Γεωργία Δρεμέτσικα, συνεργάτης στο Γραφείο Υπουργού Κοινωνικής Συνοχής και Οικογένειας, δικηγόρος με ΑΜ ΔΣ…, Χρύσα Παπαϊακώβου, συνεργάτης Υφυπουργού Κοινωνικής Συνοχής και Οικογένειας, δικηγόρος με ΑΜ ΔΣ…, Β, διευθύντρια στο Γραφείο Γενικής Γραμματέως Ισότητας και Ανθρωπίνων Δικαιωμάτων, Σταυρούλα Γεωργουλέα, συνεργάτης στο Γραφείο του Γενικού Γραμματέα Δημογραφικής και Στεγαστικής Πολιτικής, δικηγόρος με ΑΜ ΔΣ…, Γ, προϊσταμένη του τμήματος Ενίσχυσης Οικογενειακής Συνοχής της Δ/νσης Προστασίας Παιδιού και Οικογένειας, Δ, προϊσταμένη του Τμήματος Διοίκησης

Ανθρώπινου Δυναμικού της Δ/νσης Υποστήριξης Ανθρώπινου Δυναμικού και Υπηρεσιών του ΥΚΟΙΣΟ, και Ε, Στέλεχος Δ/νσης Ηλ. Διακυβέρνησης του ΥΚΟΙΣΟ. Εκ μέρους της ΕΕΤΑΑ: ΣΤ, διευθύνων σύμβουλος της ΕΕΤΑΑ, Ευάγγελος Μπαρμπούρης, προϊστάμενος της Δ/νσης Νομικής Υποστήριξης της ΕΕΤΑΑ, δικηγόρος με ΑΜ ΔΣ…, Ζ, προϊστάμενος του Αυτοτελούς Τμήματος Διαχείρισης Ποιότητας και Προστασίας Προσωπικών Δεδομένων της ΕΕΤΑΑ, Η, ασκών καθήκοντα προϊσταμένου του Τμήματος Τεκμηρίωσης και Πληροφόρησης της ΕΕΤΑΑ και Γρηγόρης Λαζαράκος, δικηγόρος με ΑΜ ΔΣ ….

Ακολούθως, το ΥΚΟΙΣΟ υπέβαλε εμπροθέσμως το υπ' αρ. πρωτ. Γ/ΕΙΣ/11578/10-11-2025 υπόμνημα μετά των σχετικών αυτού εγγράφων. Αντιστοίχως, η ΕΕΤΑΑ υπέβαλε εμπροθέσμως το υπ' αρ. πρωτ. Γ/ΕΙΣ/11477/07-11-2025 υπόμνημα.

Ειδικότερα, στο ανωτέρω υπόμνημά του, το ΥΚΟΙΣΟ αναφέρει συνοπτικά, μεταξύ άλλων, τα ακόλουθα:

Το ΥΚΟΙΣΟ δεν είχε καμία ευθύνη ως προς το γεγονός της κρινόμενης παραβίασης, καθώς τα πληγέντα συστήματα ανήκουν αποκλειστικά στην ΕΕΤΑΑ. Το πληροφοριακό σύστημα του ΥΚΟΙΣΟ δεν παραβιάσθηκε. Το ΥΚΟΙΣΟ ενεργεί υπό την ιδιότητά του ως υπευθύνου επεξεργασίας στο πλαίσιο των ανωτέρω προγραμμάτων η αρμοδιότητα των οποίων του μεταβιβάσθηκε από το Υπουργείο Εργασίας. Η ανάθεση της υλοποίησης των ως άνω προγραμμάτων στην ΕΕΤΑΑ είναι απολύτως σύννομη και βασίζεται στο νομικό και συμβατικό πλαίσιο.

Το ΥΚΟΙΣΟ μόλις έλαβε γνώση του περιστατικού παραβίασης προέβη αμέσως στις προβλεπόμενες από τα άρθρα 33 και 34 του ΓΚΠΔ ενέργειες γνωστοποίησης του περιστατικού στην Αρχή και ενημέρωσης των υποκειμένων των δεδομένων αμέσως μόλις αυτό κατέστη τεχνικά δυνατόν. Περαιτέρω, επικοινώνησε αμέσως με την ΕΕΤΑΑ ως εκτελούσα την επεξεργασία προκειμένου να λάβει όλα τα απαραίτητα μέτρα για την αντιμετώπιση του περιστατικού ώστε να επιτευχθεί το συντομότερο δυνατόν η διαθεσιμότητα των συστημάτων και να ελαχιστοποιηθούν τυχόν συνέπειες για τα υποκείμενα των δεδομένων. Ως εκ τούτου το ΥΚΟΙΣΟ ενήργησε απολύτως στο πλαίσιο των νόμιμων υποχρεώσεών του.

Ως προς το ισχύον νομικό και συμβατικό πλαίσιο ανάθεσης υλοποίησης των

εν λόγω προγραμμάτων, το ΥΚΟΙΣΟ αναφέρει:

Το πρόγραμμα «Βρεφονηπιακοί Σταθμοί» προβλέπεται στο άρθρο 104 του ν.4941/2022 «Αναμόρφωση του θεσμικού πλαισίου λειτουργίας του Ταμείου Χρηματοπιστωτικής Σταθερότητας και του Συνεγγυητικού Κεφαλαίου Εξασφάλισης Επενδυτικών Υπηρεσιών, εκσυγχρονισμός Οργανισμού Διαχείρισης Δημοσίου Χρέους και άλλες επείγουσες διατάξεις» και υλοποιείται στο πλαίσιο της Προγραμματικής Περιόδου ΕΣΠΑ 2021-2027.

Αρμόδιος φορέας για την υλοποίηση των προγραμμάτων αυτών είναι σύμφωνα με τη διάταξη του άρθρου 104 Ν. 4941/2022 η ΕΕΤΑΑ. Ειδικότερα, για την επιλογή της ΕΕΤΑΑ ως φορέα υλοποίησης των προγραμμάτων αυτών εφαρμόζεται η διαδικασία επιλογής που προβλέπεται από τις οικείες διατάξεις του ΕΣΠΑ 2021-2027 με το Νόμο 4914/2022 και τις σε αυτόν προβλεπόμενες κανονιστικές διαδικασίες σε συνδυασμό με το άρθρο 104 Ν. 4941/2022. Πιο συγκεκριμένα, για την υλοποίηση του προγράμματος εκδίδεται ετησίως μία Κοινή Υπουργική Απόφαση που τιτλοφορείται Σύστημα Διαχείρισης, Αξιολόγησης, Παρακολούθησης και Ελέγχου - Διαδικασία Εφαρμογής της Δράσης «Προώθηση και υποστήριξη παιδιών για την ένταξή τους στην προσχολική εκπαίδευση καθώς και για τη πρόσβαση παιδιών σχολικής ηλικίας, εφήβων και ατόμων με αναπηρία, σε υπηρεσίες δημιουργικής απασχόλησης». Σε κάθε σχετική ΚΥΑ προβλέπεται ότι η ΕΕΤΑΑ ενεργεί την υλοποίηση του προγράμματος ως δικαιούχος του προγράμματος, καθώς και ότι για τους σκοπούς υλοποίησης του προγράμματος η ΕΕΤΑΑ αποτελεί τον εκτελούντα την επεξεργασία των δεδομένων του προγράμματος, με Κυρίους των δεδομένων αυτών το ΥΚΟΙΣΟ και το Υπουργείο Εθνικής Οικονομίας και Οικονομικών. Για την υλοποίηση του προγράμματος έχουν εκδοθεί οι αντίστοιχες ΚΥΑ[2].

Όσον αφορά τα προσωπικά δεδομένα, στην παράγραφο 2 του άρθρου 17 εκάστης ΚΥΑ προβλέπεται ότι κατά την υλοποίηση του Προγράμματος πρέπει να τηρούνται οι απαιτήσεις του ΓΚΠΔ, του ν. 4624/2019 καθώς και τα όσα ορίζονται από τις αποφάσεις της Αρχής Προστασίας Δεδομένων, προκειμένου να διασφαλίζονται όλες οι σχετικές προβλέψεις για την επεξεργασία των προσωπικών δεδομένων και

[2] Για την περίοδο 2022-2023 εκδόθηκε η ΚΥΑ 77094/1.8.2022 [Β 4049]. Για την περίοδο 2023-2024 εκδόθηκε η ΚΥΑ 47217/20.05.2023 [Β 3418]. Για τη περίοδο 2024-2025 εκδόθηκε η ΚΥΑ 99310/10.07.2024 [Β 4056. Για τις περιόδους 2025-2027 έχει ήδη εκδοθεί η ΚΥΑ 134974/ΕΞ 2025/29.07.2025 [Β 4127] με διετή διάρκεια ισχύος, ως έχει τροποποιηθεί και ισχύει, με την ΚΥΑ 15670/2025 (ΦΕΚ Β΄5646).

την προστασία τόσο των εν λόγω δεδομένων όσο και των δικαιωμάτων των υποκειμένων τους. Περαιτέρω είχε υπογραφεί η με αρ. πρωτ. 15321/2022 σχετική σύμβαση για την επεξεργασία δεδομένων την 4/11/2022 «*που λόγω της ανά έτος διαδοχικής, συνεχούς και αδιάλειπτης εφαρμογής του προγράμματος αυτού με αντίστοιχες και παρόμοιες κατά περιεχόμενο Κοινές Υπουργικές Αποφάσεις 11μηνης τυπικής ισχύος καλύπτει τις εκατέρωθεν υποχρεώσεις Υπουργείων και ΕΕΤΑΑ αναφορικά με τη προστασία των προσωπικών δεδομένων. Σημειώνεται ότι η ανάγκη ετήσιας έκδοσης των ΚΥΑ αυτών κάλυψε αποκλειστικά και μόνο διοικητικές υποχρεώσεις διαχείρισης του προγράμματος βρεφονηπιακών σταθμών αναφορικά με τη χρηματοδότησή του και, στο πλαίσιο της χρηματοδότησης αυτής, τον τρόπο χειρισμού κυρίως των συμβάσεων εργασίας του προσωπικού που απασχολείται στις δημοτικές δομές βρεφονηπιακών σταθμών που συμμετέχουν στο πρόγραμμα καθώς πρόκειται για προσωπικό το οποίο απασχολείται στις δομές αυτές με ανανεούμενες συμβάσεις εργασίας ισόχρονες προς την διάρκεια του σχολικού έτους.*» Με άλλα λόγια το περιεχόμενο της υποχρέωσης εμπιστευτικότητας και προστασίας των προσωπικών δεδομένων παραμένει διαρκώς ίδιο, ενώ και το σύστημα της ΕΕΤΑΑ παρέμενε το ίδιο ανά έτος και ανά ΚΥΑ.

Στο πλαίσιο της υλοποίησης του ως άνω έργου, και ειδικά για την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί η ΕΕΤΑΑ για την παροχή των υπηρεσιών που αναφέρονται στην υπ' αριθμ. ΚΥΑ 77094/1.8.2022, υπεγράφη στις 4-11-2022 Σύμφωνο για την επεξεργασία δεδομένων μεταξύ του ΥΚΟΙΣΟ και της ΕΕΤΑΑ. Μεταξύ άλλων, στο εν λόγω Σύμφωνο αναφέρεται, σχετικά με την ασφάλεια της επεξεργασίας, ότι η ΕΕΤΑΑ εφαρμόζει τουλάχιστον τα τεχνικά και οργανωτικά μέτρα που καθορίζονται στο Παράρτημα ΙΙ του Συμφώνου προκειμένου να διασφαλίζει τα προσωπικά δεδομένα, συμπεριλαμβανομένης της προστασίας από παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων. Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, οι συμβαλλόμενοι λαμβάνουν δεόντως υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους που συντρέχουν για τα υποκείμενα των δεδομένων. Επίσης, αναφέρεται ότι, σε περίπτωση που η ΕΕΤΑΑ

παραβιάζει τις υποχρεώσεις της από το Σύμφωνο, το ΥΚΟΙΣΟ μπορεί να δώσει εντολή στην ΕΕΤΑΑ να αναστείλει την επεξεργασία έως ότου η ΕΕΤΑΑ συμμορφωθεί με το Σύμφωνο. Η ΕΕΤΑΑ, επιπρόσθετα, ενημερώνει αμέσως το ΥΚΟΙΣΟ σε περίπτωση που αδυνατεί να συμμορφωθεί με το Σύμφωνο, για οποιονδήποτε λόγο. Στο Παράρτημα ΙΙ του εν λόγω Συμφώνου, αναφέρεται μεταξύ άλλων, ότι εφαρμόζεται από την ΕΕΤΑΑ ολοκληρωμένη Πολιτική Προστασίας Προσωπικών Δεδομένων, ιδίως στους τομείς της διασφάλισης της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των πληροφοριακών πόρων της ΕΕΤΑΑ, όπως του εξοπλισμού και των συστημάτων ΤΠΕ (συμπεριλαμβανομένης της προστασίας των συστημάτων από ιούς και άλλο κακόβουλο λογισμικό, της λήψης αντιγράφων ασφαλείας, κ.λπ.) και του δικτύου και των Πληροφοριακών Συστημάτων (συμπεριλαμβανομένης της ασφάλειας περιμέτρου, παρακολούθησης και ελέγχου συστημάτων, ενημέρωσης λογισμικού, χρήσης VPN για απομακρυσμένη πρόσβαση, κ.λπ.).

Σχετικά με το πρόγραμμα «Νταντάδες της Γειτονιάς», αυτό προβλέπεται στη διάταξη του άρθρου 44 του Ν4837/2021 [Α 178], ενώ με τις υπ΄ αριθμ. 6457/2022 [Β 205] και 26460/2022 [Β. 1328] ΚΥΑ, αντιστοίχως, ρυθμίστηκαν τα θέματα λειτουργίας του μητρώου επιμελητών και του πληροφοριακού συστήματος επιλογής ωφελουμένων.

Για τη χρηματοδότηση του πιλοτικού προγράμματος εκδόθηκε η υπ΄αριθμ. 76042 ΕΞ2024/30.05.2024 Πράξη της Γενικής Γραμματέα Διαχείρισης Προγραμμάτων του Ευρωπαϊκού Κοινωνικού Ταμείου για τη χρηματοδότηση της Πράξης «Πιλοτική Εφαρμογή της δράσης «Νταντάδες της Γειτονιάς» από το Πρόγραμμα Ανθρώπινο Δυναμικό και Κοινωνική Συνοχή με Δικαιούχους την Γενική Γραμματεία Ισότητας και Ανθρωπίνων Δικαιωμάτων, το Εθνικό Δίκτυο Υποδομών Τεχνολογίας και Έρευνας ΑΕ και την ΕΕΤΑΑ». Η διάρκεια της πράξης ορίστηκε από την 01.02.2022 ως 31.03.2025. Ειδικότερα, στο πλαίσιο του προγράμματος αυτού, η ΕΕΤΑΑ ανέλαβε την υλοποίηση του Υποέργου 5 και επιπλέον, για τον σκοπό αυτόν, υπογράφηκε και η από 12.05.2022 προγραμματική σύμβαση μεταξύ της Γενικής Γραμματεία Ισότητας του Υπουργείου Εργασίας και Κοινωνικών Υποθέσεων [από 27.6.2023 ΥΚΟΙΣΟ], όπου και ρυθμίζονται θέματα εμπιστευτικότητας για την προστασία προσωπικών δεδομένων.

Σημειώνεται ότι η ευαλωτότητα, την οποία εκμεταλλεύτηκε το κακόβουλο

λογισμικό που διεξήγαγε την επίθεση, και η οποία περιγράφεται στο Εμπιστευτικό Παράρτημα, Σημείο 1, αφορά σύστημα που χρησιμοποιείτο για την υποστήριξη ληξιπρόθεσμων εφαρμογών που υποστήριζαν το Πρόγραμμα «Βάση Δεδομένων Κακοποιημένων Γυναικών». Το πρόγραμμα αυτό υλοποιήθηκε και χρηματοδοτήθηκε από το ΕΣΠΑ 2014-2020 με πόρους του Ευρωπαϊκού Κοινωνικού Ταμείου από το Επιχειρησιακό Πρόγραμμα Διοικητική Μεταρρύθμιση. Ειδικότερα, με την υπ΄ αριθμ. 1522/12.08.2016 απόφαση του Ειδικού Γραμματέα Διαχείρισης Τομεακών Προγραμμάτων του Ευρωπαϊκού Κοινωνικού Ταμείου της Προγραμματικής Περιόδου ΕΣΠΑ 2014-2020 εντάχθηκε και χρηματοδοτήθηκε από το Επιχειρησιακό Πρόγραμμα Διοικητική Μεταρρύθμιση. Δικαιούχος του Προγράμματος ήταν η ΕΕΤΑΑ και φορέας χρηματοδότησης – αρμόδιο υπουργείο ήταν το Υπουργείο Εσωτερικών. Η πράξη αυτή χρηματοδοτήθηκε αρχικά για την περίοδο από 01.01.2016 – 31.12.20218 και κατόπιν διαδοχικών τροποποιήσεων ως την 31.12.2023 και τελικό χρόνο λήξης την 16.04.2024. Για το χρονικό διάστημα μετά την ολοκλήρωση της πράξης και δεδομένης της μεταφοράς της καθ΄ ύλην αρμοδιότητας της Γενικής Γραμματείας Ισότητας στο ΥΚΟΙΣΟ (το οποίο συστάθηκε από 27.6.2023) και προκειμένης της περαιτέρω λειτουργίας του συστήματος αυτού, αποφασίστηκε η ανάληψη της δαπάνης της εν λόγω προγραμματικής συμφωνίας από τον τακτικό προϋπολογισμό του ΥΚΟΙΣΟ για 2 οικονομικά έτη (2024- 2025). Τελικώς, την 19.12.2024 υπογράφηκε μεταξύ της Γενικής Γραμματείας Ισότητας και Ανθρωπίνων Δικαιωμάτων του ΥΚΟΙΣΟ και της ΕΕΤΑΑ η υπ΄αριθμ. 7883/14.12.2024 προγραμματική σύμβαση, όπου τα θέματα εμπιστευτικότητας που αφορούν στο εν λόγω σύστημα περιλαμβάνονται στο άρθρο 10 αυτής, σύμφωνα με το οποίο, στο εδ. δ΄ «Η Ε.Ε.Τ.Α.Α. τηρεί τις υποχρεώσεις που απορρέουν από τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠ), την κείμενη εθνική και ενωσιακή νομοθεσία και διαθέτει εν ισχύ όλες τις απαιτούμενες άδειες σχετικά με την προστασία των προσωπικών δεδομένων», ενώ στο εδ. ε’ αναφέρεται ότι «Η Ε.Ε.Τ.Α.Α. υποχρεούται να λαμβάνει όλα τα απαραίτητα μέτρα για την προστασία της βάσης δεδομένων και των πληροφοριών και των δεδομένων αυτής από τυχόν κυβερνοαπειλές και κυβερνοεπιθέσεις σύμφωνα με την εθνική και ενωσιακή νομοθεσία.»

Τέλος, το ΥΚΟΙΣΟ αναφέρει ότι ως προς τον ισχυρισμό της ΕΕΤΑΑ, κατά την ακρόαση της 21/10/2025, ότι είχε ενημερώσει το ΥΚΟΙΣΟ για την ανάγκη αναβάθμισης των συστημάτων της προκειμένου να καταστούν ασφαλέστερα και περισσότερο λειτουργικά, παρ' όλο που η σχετική αρμοδιότητα εκφεύγει του ΥΚΟΙΣΟ και ανήκει στα Υπουργεία Εσωτερικών και Εθνικής Οικονομίας και Οικονομικών, ουδεμία τέτοια επικοινωνία ή ενημέρωση προκύπτει ότι έλαβε χώρα από τη μεταβίβαση της αρμοδιότητας επί των προγραμμάτων «Βρεφονηπιακοί σταθμοί» και «Νταντάδες της Γειτονιάς» στο ΥΚΟΙΣΟ.

Αντιστοίχως, στο ανωτέρω υπόμνημά της, η ΕΕΤΑΑ αναφέρει συνοπτικά, μεταξύ άλλων, τα ακόλουθα:

Πρωταρχική αιτία του εν λόγω περιστατικού εκτιμάται ότι αποτελεί η ύπαρξη παρωχημένου λογισμικού σε αρκετούς διακομιστές της υποδομής πληροφορικής της ΕΕΤΑΑ. Τα εν λόγω συστήματα υποστήριζαν προγράμματα που λειτουργούσαν προς το δημόσιο συμφέρον (όπως ήταν ο server που φιλοξενούσε το πρόγραμμα για την υποστήριξη κακοποιημένων γυναικών), τα οποία (Προγράμματα) η ΕΕΤΑΑ δεν μπορούσε να διακόψει αφενός διότι αυτά υπήρχαν για την εξυπηρέτηση του δημοσίου συμφέροντος και υπήρχε πολιτική απόφαση για τη συνέχισή τους και, αφετέρου, διότι η διακοπή τους ανήκε στην αποκλειστική αρμοδιότητα του υπεύθυνου επεξεργασίας, του ΥΚΟΙΣΟ, και όχι της ΕΕΤΑΑ, η οποία είχε απλώς το ρόλο του «εκτελούντος την επεξεργασία».

Μετά το περιστατικό, η ΕΕΤΑΑ ανέθεσε σε εξειδικευμένη εταιρεία να διενεργήσει ενδελεχή έλεγχο και καθαρισμό του συνόλου των Πληροφοριακών Συστημάτων της από κακόβουλο λογισμικό που ενδεχομένως έχει εγκατασταθεί σε αυτά κατά την κυβερνοεπίθεση, αποκατάσταση των υπολογιστικών συστημάτων της και ενίσχυση της ασφάλειας των Πληροφοριακών Συστημάτων της.

Εδώ και χρόνια, η ΕΕΤΑΑ αναλαμβάνει την υλοποίηση έργων και δράσεις με εξαιρετικά μεγάλες απαιτήσεις σε τεχνολογικές υποδομές και ακόμη μεγαλύτερες σε θέματα ασφάλειας των πληροφοριών που διακινούνται στα Πληροφοριακά Συστήματα. Τα έργα και οι δράσεις αυτές περιλαμβάνουν μεγάλης κλίμακας επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία ενέχει σοβαρούς κινδύνους σε σχέση με τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και

διαθεσιμότητας των δεδομένων, καθώς και της επιχειρησιακής συνέχειας (Business Continuity), την εγγενή δηλαδή ικανότητα του οργανισμού να παρέχει με συνέπεια τις υπηρεσίες του, σε αποδεκτά προκαθορισμένα ποιοτικά και ποσοτικά επίπεδα, ακόμα και μετά την εμφάνιση γεγονότων που προκαλούν διακοπή της λειτουργίας βασικών τεχνολογικών του υποδομών.

Δυστυχώς, η ικανότητα της ΕΕΤΑΑ να παρέχει τις υπηρεσίες που απορρέουν από το θεσμικό της ρόλο, με σεβασμό και, προπάντων, με ασφάλεια στην προστασία των προσωπικών δεδομένων των ωφελουμένων του κάθε προγράμματος, μειώνεται περαιτέρω εξαιτίας της συνεχιζόμενης μείωσης του τακτικού προσωπικού, ιδίως μετά το 2020, του υψηλού μέσου όρου ηλικίας, γεγονότα που δημιούργησαν σημαντικές ελλείψεις σε πολλούς τομείς τόσο ως προς την απαιτούμενη στελέχωση όσο και ως προς την επάρκεια δεξιοτήτων.

Η ΕΕΤΑΑ, αντιλαμβανόμενη τον κίνδυνο που διατρέχουν τα υλοποιούμενα, αλλά και μελλοντικά προγράμματα, κυρίως, όμως, τα προσωπικά δεδομένα των ωφελούμενων προσώπων που διακινούνται στα πληροφοριακά της συστήματα, ανέθεσε, προ τριετίας, σε εταιρεία που ειδικεύεται στον τομέα της κυβερνοασφάλειας, τη διενέργεια σειράς ελέγχων για την αξιολόγηση της ευαλωτότητας (vulnerability assessment) των συστημάτων της από κυβερνοεπιθέσεις, καθώς και την παροχή, προς την ΕΕΤΑΑ, σχετικών συμβουλευτικών υπηρεσιών. Τα πρώτα πορίσματα, που προφορικά έλαβε η ΕΕΤΑΑ περί τα τέλη του 2022, ήταν ανησυχητικά και εδραίωσαν την πεποίθηση ότι ήταν απαραίτητη η άμεση βελτίωση των υποδομών Τεχνολογιών Πληροφορικής και Επικοινωνιών της ΕΕΤΑΑ, με παράλληλη ενίσχυση της ασφάλειας των συστημάτων και των δεδομένων, καθώς και η ενσωμάτωση της χρήσης των ΤΠΕ σε όλα τα επίπεδα λειτουργίας της ΕΕΤΑΑ, με απώτερο στόχο την αποτελεσματικότητα και την αποδοτικότητα στην παροχή των υπηρεσιών και την υλοποίηση των στόχων της, με σεβασμό στους ωφελούμενους και, ιδίως στα προσωπικά δεδομένα τους, τα οποία διακινούντο στα συστήματά της.

Η ΕΕΤΑΑ δηλώνει στο υπόμνημά της ότι κατόπιν των ανωτέρω, τα αρμόδια στελέχη Πληροφορικής, ο Υπεύθυνος Προστασίας Δεδομένων και, κυρίως, η Διοίκηση

της ΕΕΤΑΑ, άρχισαν σειρά επαφών με τα τρία αρμόδια Υπουργεία (Εσωτερικών, Ψηφιακής Διακυβέρνησης και ΥΚΟΙΣΟ), προκειμένου να εξασφαλιστούν οι απαραίτητοι οικονομικοί πόροι που θα επέτρεπαν στην ΕΕΤΑΑ να αντιμετωπίσει και να θεραπεύσει τα παραπάνω προβλήματα, δηλ. να εκσυγχρονιστούν τα πληροφοριακά της συστήματα και να ενισχυθούν τα μέτρα ασφαλείας για τη διασφάλιση των προσωπικών ιδίως δεδομένων που τηρούντο και διακινούντο σε αυτά.

Μάλιστα, η ΕΕΤΑΑ σημειώνει ότι οι εν λόγω επαφές είχαν αποτέλεσμα, καθώς ένα χρόνο αργότερα, στις 21/10/2024, υπεγράφη Προγραμματική Συμφωνία της ΕΕΤΑΑ με την ΚτΠ Μ.Α.Ε. για την αναβάθμιση των Πληροφοριακών Συστημάτων της ΕΕΤΑΑ (συγκεκριμένα ο τίτλος της συμφωνίας είναι «Ψηφιακός Μετασχηματισμός της ΕΕΤΑΑ Α.Ε.»). Η εν λόγω συμφωνία δεν πρόλαβε να υλοποιηθεί καθώς το σχετικό Τεχνικό Δελτίο υπεβλήθη στις 21/1/2025 περίπου ένα μήνα πριν το περιστατικό παραβίασης. Τα μέτρα τα οποία προγραμματίζεται να ληφθούν περιγράφονται στο Εμπιστευτικό Παράρτημα, Σημείο 4.

Η ΕΕΤΑΑ, τέλος, επισημαίνει ότι δεν θα μπορούσε να διακόψει την υλοποίηση των προγραμμάτων, όταν αντελήφθη τα υποκείμενα ζητήματα ασφαλείας, ή να αρνηθεί την παροχή υπηρεσιών και την υλοποίηση των Προγραμμάτων τις επόμενες χρονιές, αλλά όφειλε να παρέχει -και τότε και στο μέλλον- τις υπηρεσίες της με τα διαθέσιμα μέσα και με τον καλύτερο δυνατό τρόπο, προσπαθώντας ταυτόχρονα να ενημερώνει συνεχώς τους αρμόδιους φορείς (Υπουργεία) για την κατάσταση που βρίσκονταν τα Π.Σ. της και για τις συνθήκες ασφαλείας.

Επιπρόσθετα, η ίδια η ΕΕΤΑΑ δεν διέθετε τους υψηλότατους οικονομικούς πόρους που χρειαζόταν προκειμένου να εκσυγχρονίσει τα πληροφοριακά της συστήματα, καθώς εξαρτάτο δε απολύτως από κρατική χρηματοδότηση.

Η Αρχή, μετά από εξέταση των στοιχείων του φακέλου, αφού άκουσε τον εισηγητή και τις διευκρινίσεις από τους βοηθούς εισηγητή, οι οποίοι παρέστησαν χωρίς δικαίωμα ψήφου, κατόπιν διεξοδικής συζητήσεως,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Από τις διατάξεις των άρθρων 51 και 55 του ΓΚΠΔ και του άρθρου 9 του νόμου 4624/2019 (ΦΕΚ Α΄ 137) προκύπτει ότι 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 σημείο 12 του άρθρου 4 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».*

3. Σύμφωνα με το άρθρο 4 στοιχ. 1 του ΓΚΠΔ δεδομένα προσωπικού χαρακτήρα είναι «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου*».

4. Σύμφωνα με το άρθρο 4 στοιχ. 8 του ΓΚΠΔ εκτελών την επεξεργασία είναι «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας*».

5. Στο άρθρο 5 παρ. 1 του ΓΚΠΔ ορίζονται οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σε αυτές περιλαμβάνεται η αρχή της ακεραιότητας και εμπιστευτικότητας (εδαφ. στ'), σύμφωνα με την οποία τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και

τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

6. Σύμφωνα δε με την αρχή της λογοδοσίας που εισάγεται με τη δεύτερη παράγραφο του αυτού ως άνω άρθρου 5, ορίζεται ρητώς ότι ο υπεύθυνος επεξεργασίας «φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»)». Η αρχή αυτή, η οποία συνιστά ακρογωνιαίο λίθο του ΓΚΠΔ, συνεπάγεται την υποχρέωση του υπευθύνου επεξεργασίας 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, να είναι σε θέση να αποδεικνύει ο ίδιος και ανά πάσα στιγμή τη συμμόρφωσή του με τις αρχές του άρθρου 5 παρ. 1 ΓΚΠΔ.

7. Σύμφωνα με τους ορισμούς του άρθρου 25 του ΓΚΠΔ: «*1. 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 από την επεξεργασία, ο υπεύθυνος επεξεργασίας 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, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.».*

8. Στο άρθρο 28 παρ. 3 του ΓΚΠΔ ορίζεται ότι: « *Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας. Η εν λόγω σύμβαση ή άλλη νομική πράξη προβλέπει ειδικότερα ότι ο εκτελών την επεξεργασία:*

α) επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας (…)

γ) λαμβάνει όλα τα απαιτούμενα μέτρα δυνάμει του άρθρου 32 (…)

στ) 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 (…)

η) θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που θεσπίζονται στο παρόν άρθρο και επιτρέπει και διευκολύνει τους ελέγχους, περιλαμβανομένων των επιθεωρήσεων, που διενεργούνται από τον υπεύθυνο επεξεργασίας ή από άλλον ελεγκτή εντεταλμένο από τον υπεύθυνο επεξεργασίας.»

9. Στο άρθρο 32 παρ. 1 και 2 του ΓΚΠΔ ορίζεται ότι: «*1. 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 (…) 2. 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*».

10. Σύμφωνα με το άρθρο 33 του ΓΚΠΔ: «*1. 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. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση. (...) 3. Η γνωστοποίηση που αναφέρεται στην παράγραφο 1 κατ' ελάχιστο: 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. 4. Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση. 5. Ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα που συνίστανται στα πραγματικά περιστατικά που αφορούν στην παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην εποπτική αρχή να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο.».

11. Σύμφωνα με το άρθρο 34 του ΓΚΠΔ: «*1. 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. 2. 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). 3. Η ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 1 δεν απαιτείται, εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις: α) ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη 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 ο αναφερόμενος στην παράγραφο 1 υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, γ) προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο. 4. Εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, η εποπτική αρχή μπορεί, έχοντας εξετάσει την πιθανότητα επέλευσης υψηλού κινδύνου από την παραβίαση των δεδομένων προσωπικού χαρακτήρα, να του ζητήσει να το πράξει ή μπορεί να αποφασίσει ότι πληρούνται οποιαδήποτε από τις προϋποθέσεις που αναφέρονται στην παράγραφο 3.»

12. Η Αρχή υπενθυμίζει ότι η υποχρέωση ασφάλειας που προβλέπεται στο άρθρο 32 του ΓΚΠΔ συνιστά υποχρέωση μέσων και όχι αποτελέσματος και επιβάλλει στον υπεύθυνο επεξεργασίας την υποχρέωση λήψης κατάλληλων τεχνικών και οργανωτικών μέτρων, τα οποία, λαμβανομένων υπόψη των χαρακτηριστικών της συγκεκριμένης επεξεργασίας, αποσκοπούν τόσο στη μείωση της πιθανότητας επέλευσης παραβίασης δεδομένων προσωπικού χαρακτήρα όσο και, ενδεχομένως, στον περιορισμό της σοβαρότητάς της. Ως εκ τούτου, δεν απαιτείται τα μέτρα ασφάλειας να εξαλείφουν κάθε μορφή κινδύνου και η απλή επέλευση παραβίασης δεδομένων προσωπικού χαρακτήρα δεν συνιστά, αυτή καθαυτή, παράβαση του άρθρου 32 του ΓΚΠΔ. Η ανωτέρω ερμηνεία έχει

επιβεβαιωθεί από το Δικαστήριο της Ευρωπαϊκής Ένωσης με την απόφασή του Agence nationale des recettes publiques de Bulgarie (14.12.2023, C-340/21, σκέψεις 29-31), με την οποία κρίθηκε ότι η αναφορά, στο άρθρο 32 παρ. 1 και 2 ΓΚΠΔ, σε «επίπεδο ασφάλειας κατάλληλο προς τον κίνδυνο» και σε «κατάλληλο επίπεδο ασφάλειας» καταδεικνύει ότι ο ΓΚΠΔ θεσπίζει καθεστώς διαχείρισης κινδύνων και δεν αποσκοπεί στην εξάλειψη των κινδύνων παραβίασης δεδομένων προσωπικού χαρακτήρα. Από τη διατύπωση των άρθρων 24 και 32 ΓΚΠΔ προκύπτει ότι οι διατάξεις αυτές επιβάλλουν στον υπεύθυνο επεξεργασίας την υποχρέωση υιοθέτησης τεχνικών και οργανωτικών μέτρων με σκοπό την αποτροπή, στο μέτρο του δυνατού, παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Η καταλληλότητα των μέτρων αυτών πρέπει να αξιολογείται κατά περίπτωση, λαμβανομένων υπόψη των κριτηρίων που προβλέπονται στα ανωτέρω άρθρα, καθώς και των ειδικών αναγκών προστασίας των δεδομένων και των κινδύνων που απορρέουν από τη συγκεκριμένη επεξεργασία.

13. Στην προκειμένη περίπτωση, από τα στοιχεία του φακέλου της υπόθεσης προκύπτει ότι η ΕΕΤΑΑ, ως φορέας υλοποίησης των προγραμμάτων κοινωνικής πολιτικής, λειτουργεί ως εκτελούσα την επεξεργασία μεγάλης κλίμακας δεδομένων για λογαριασμό του ΥΚΟΙΣΟ, ως υπευθύνου επεξεργασίας, και άλλων φορέων, κατά την έννοια του άρθρου 4 σημ. 8 ΓΚΠΔ. Συνολικά, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία φαίνεται ότι συμμορφώθηκαν με τις έννομες υποχρεώσεις τους, οι οποίες απορρέουν από τα προαναφερθέντα άρθρα 33 και 34 του ΓΚΠΔ αναφορικά με τη διαχείριση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα, δεδομένου ότι:

α) ο εκτελών την επεξεργασία ενημέρωσε τον υπεύθυνο επεξεργασίας όταν αντελήφθη το περιστατικό παραβίασης,

β) ο υπεύθυνος επεξεργασίας υπέβαλε τη σχετική γνωστοποίηση στην Αρχή, εντός εβδομήντα δύο (72) ωρών από τη στιγμή που έλαβε γνώση του περιστατικού,

γ) η γνωστοποίηση συνολικά, όπως αυτή συμπληρώθηκε, παρέχει όλες τις πληροφορίες που απαιτούνται βάσει του άρ. 33 του ΓΚΠΔ,

δ) προέβη σε αξιολόγηση των κινδύνων για τα επηρεαζόμενα υποκείμενα των δεδομένων λόγω του περιστατικού και πραγματοποίησε ενημέρωση αυτών, σύμφωνα με τα όσα προβλέπονται σχετικώς στο άρ. 34 του ΓΚΠΔ.

14. Σχετικά με τα αίτια του περιστατικού, η παραβίαση του άρθρου 32 του ΓΚΠΔ οφείλεται στη λειτουργία παλαιού διακομιστή εφαρμογών, παρωχημένης τεχνολογίας και χαμηλού επιπέδου ασφαλείας. Η εν λόγω τεχνική ευπάθεια ήταν γνωστή και ευλόγως προβλέψιμη και εκμεταλλεύσιμη με συνήθεις μεθόδους κυβερνοεπίθεσης. Η διατήρηση σε λειτουργία παρωχημένου πληροφοριακού συστήματος με γνωστές ευπάθειες αντιβαίνει στην υποχρέωση λήψης μέτρων, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, δηλαδή σύμφωνα με την κατάσταση της τεχνολογίας αιχμής (state of the art), ιδίως όταν υπάρχουν διαθέσιμες ενημερώσεις ασφαλείας ή εναλλακτικές λύσεις, δεδομένου ότι η υποχρέωση του άρθρου 32 δεν εξαντλείται στην αρχική εγκατάσταση μέτρων, αλλά περιλαμβάνει τη συνεχή επικαιροποίηση, διαχείριση ευπαθειών (vulnerability management), και απόσυρση legacy συστημάτων. Η Αρχή κρίνει ότι η ευπάθεια ήταν γνωστή στην κοινότητα κυβερνοασφάλειας, η εκμετάλλευσή της ήταν τεχνικά απλή, συνεπώς ο κίνδυνος ήταν προβλέψιμος και αποτρέψιμος, άρα η μη λήψη μέτρων συνιστά τουλάχιστον βαριά αμέλεια. Το επιχείρημα της ΕΕΤΑΑ ότι «δεν μπορούσαμε να σταματήσουμε λόγω δημοσίου συμφέροντος» απορρίπτεται διότι το δημόσιο συμφέρον δεν αίρει την υποχρέωση ασφάλειας, όπως επίσης το δημόσιο συμφέρον πλήττεται όταν ευπαθή Πληροφοριακά Συστήματα με κρίσιμα προσωπικά δεδομένα παραμένουν σε λειτουργία. Ομοίως, η αναφορά σε έλλειψη πόρων δεν αποτελεί λόγο απαλλαγής δεδομένου ότι οι οικονομικοί περιορισμοί δεν αίρουν την υποχρέωση συμμόρφωσης με το άρθρο 32 του ΓΚΠΔ. Η αντιμετώπιση της ευπάθειας, επίσης, δεν προκύπτει ότι έχει τέτοιο κόστος, το οποίο να ελήφθη υπόψη και να απορρίφθηκε η υλοποίηση του αντίστοιχου μέτρου λόγω του ύψους του κόστους εφαρμογής.

15. Ενώ η ΕΕΤΑΑ δηλώνει ότι είχε ενημερώσει το ΥΚΟΙΣΟ για την ανάγκη αναβάθμισης των συστημάτων της προκειμένου να καταστούν ασφαλέστερα και περισσότερο λειτουργικά, δεν έχει προσκομιστεί τεκμηρίωση τέτοιας επικοινωνίας. Το ΥΚΟΙΣΟ, επίσης, αρνείται ότι έλαβε οποιαδήποτε σχετική επικοινωνία.

16. Ο υπεύθυνος επεξεργασίας οφείλει να χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς εγγυήσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, και η ευθύνη για την τήρηση του άρθρου 32 δεν μεταβιβάζεται στον εκτελούντα. Η Αρχή δέχεται ότι η παράβαση του άρθρου 32 από τον εκτελούντα δεν απαλλάσσει τον υπεύθυνο επεξεργασίας, όταν αυτός δεν διασφάλισε εκ των προτέρων την επάρκεια των μέτρων. Ο υπεύθυνος επεξεργασίας δεν εκπλήρωσε την υποχρέωση επιλογής εκτελούντος που παρέχει επαρκείς εγγυήσεις, καθώς δεν προέβη σε ουσιαστική αξιολόγηση της ασφάλειας των Πληροφοριακών Συστημάτων αυτού, ούτε διασφάλισε την ύπαρξη κατάλληλων τεχνικών και οργανωτικών μέτρων. Η χρήση παρωχημένης τεχνολογίας με γνωστές ευπάθειες καταδεικνύει ότι οι παρεχόμενες εγγυήσεις δεν ήταν επαρκείς.

17. Ο χειρισμός του περιστατικού κρίνεται ως επαρκής, λαμβάνοντας υπόψη τις ενέργειες στις οποίες προέβη η ΕΕΤΑΑ, αναθέτοντας σε πρώτη φάση σε εξειδικευμένη εταιρεία τη διενέργεια ενδελεχή ελέγχου και καθαρισμού του συνόλου των Πληροφοριακών Συστημάτων της από κακόβουλο λογισμικό που ενδεχομένως είχε εγκατασταθεί σε αυτά κατά την κυβερνοεπίθεση, στη συνέχεια επαναφέροντας τα δεδομένα από τα αντίγραφα ασφαλείας, αποκαθιστώντας τη λειτουργία των συστημάτων της, και τέλος προβαίνοντας στη λήψη κατάλληλων μέτρων μέσω σύμβασης με εταιρεία για την ενίσχυση της ασφάλειας ώστε να αποτραπεί αντίστοιχο περιστατικό στο μέλλον. Αλλά, και το ΥΚΟΙΣΟ αρχικά, έστω και με σχετική καθυστέρηση για τους λόγους που εξήγησε στο υπόμνημά του, προέβη σε ενέργειες προς το μετριασμό της τυχόν ζημιάς στα επηρεαζόμενα υποκείμενα (όπως ενημέρωση τόσο μέσω της ιστοσελίδας του όσο και απευθείας με ηλεκτρονικό ταχυδρομείο).

18. Σχετικά με την ανάθεση στην ΕΕΤΑΑ εκ μέρους του ΥΚΟΙΣΟ της υλοποίησης των επηρεαζόμενων προγραμμάτων, σημειώνεται ότι, παρόλο που κάθε χρόνο υπογραφόταν μία νέα σχετική Κοινή Υπουργική Απόφαση για το κάθε πρόγραμμα, για το πρόγραμμα «Βρεφονηπιακών Σταθμών» για την περίοδο του περιστατικού παραβίασης δεν υπήρχε ενεργή σύμβαση που να την καλύπτει, καθώς η τελευταία αφορούσε την περίοδο 2022-2023, κατά παράβαση του άρθρου 28 παρ. 3 του ΓΚΠΔ, κυρίως για το ΥΚΟΙΣΟ που δρούσε ως υπεύθυνος

επεξεργασίας, αλλά και για την ΕΕΤΑΑ με την ιδιότητα του εκτελούντος την επεξεργασία. Ο υπεύθυνος επεξεργασίας επέτρεψε την επεξεργασία δεδομένων χωρίς να υφίσταται η απαιτούμενη σύμβαση ή άλλη νομική πράξη. Η Αρχή κρίνει ότι η ύπαρξη σύμβασης δεν αποτελεί τυπική προϋπόθεση, αλλά ουσιώδη εγγύηση νομιμότητας της επεξεργασίας. Ο υπεύθυνος επεξεργασίας δεν απέδειξε ότι εξασφάλισε τη συμβατική δέσμευση του εκτελούντος ούτε καθόρισε σαφώς τις υποχρεώσεις του, προκαλώντας αδυναμία επίδειξης συμμόρφωσης. Η απουσία σύμβασης στέρησε σαφείς υποχρεώσεις ασφάλειας και μηχανισμούς ελέγχου και λογοδοσίας, οπότε συνέβαλε ουσιωδώς στο περιστατικό. Ο υπεύθυνος επεξεργασίας παραβίασε το άρθρο 28 παρ. 3 ΓΚΠΔ, καθώς επέτρεψε την επεξεργασία προσωπικών δεδομένων από εκτελούντα χωρίς να υφίσταται εν ισχύ σύμβαση που να ρυθμίζει την επεξεργασία.

19. Ο εκτελών όφειλε να διασφαλίσει ότι η επεξεργασία διενεργείται βάσει έγκυρης σύμβασης. Η Αρχή δέχεται ότι η υποχρέωση ύπαρξης σύμβασης αφορά αμφότερα τα μέρη. Η επεξεργασία στερείται του απαιτούμενου νομικού πλαισίου άρα είναι μη εξουσιοδοτημένη. Η έλλειψη σύμβασης συνεπάγεται έλλειψη σαφών οδηγιών, έλλειψη δεσμεύσεων ασφάλειας, απουσία ελέγχου, γεγονός που ενίσχυσε τον κίνδυνο. Ο εκτελών την επεξεργασία παραβίασε το άρθρο 28 παρ. 3 ΓΚΠΔ, καθώς προέβη σε επεξεργασία προσωπικών δεδομένων χωρίς να υφίσταται εν ισχύ σύμβαση με τον υπεύθυνο επεξεργασίας που να ρυθμίζει τους όρους αυτής. Κατά τον καθορισμό των διοικητικών προστίμων, η Αρχή λαμβάνει υπόψη ότι ο υπεύθυνος επεξεργασίας φέρει πρωτεύουσα ευθύνη για τη συμμόρφωση με τον ΓΚΠΔ, ιδίως ως προς την επιλογή και εποπτεία του εκτελούντος. Στην προκειμένη περίπτωση, η πλήρης απουσία εν ισχύ σύμβασης κατά το άρθρο 28 ΓΚΠΔ και η μη διενέργεια ουσιαστικού ελέγχου του επιπέδου ασφάλειας του εκτελούντος συνιστούν ιδιαίτερα σοβαρές παραβάσεις.

20. Συνεπώς, με βάση τα ανωτέρω, η Αρχή διαπιστώνει τις εξής παραβάσεις για το ΥΚΟΙΣΟ ως υπεύθυνο επεξεργασίας:

α) του άρθρου 5 παρ. 1 στοιχ. στ’ σε συνδυασμό με το άρθρο 32 παρ. 1 του ΓΚΠΔ αναφορικά με την ασφάλεια της επεξεργασίας (βλ. ανωτέρω Σκέψη 15), και

β) του άρθρου 28 παρ. 3 του ΓΚΠΔ αναφορικά με την έλλειψη ενεργής σύμβασης μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία (βλ. ανωτέρω Σκέψη 18).

21. Περαιτέρω, με βάση τα ανωτέρω, η Αρχή διαπιστώνει τις εξής παραβάσεις για την ΕΕΤΑΑ ως εκτελούσα την επεξεργασία:

α) του άρθρου 5 παρ. 1 στοιχ. στ' σε συνδυασμό με το άρθρο 32 παρ. 1 του ΓΚΠΔ αναφορικά με την ασφάλεια της επεξεργασίας (βλ. ανωτέρω Σκέψη 14), και

β) του άρθρου 28 παρ. 3 του ΓΚΠΔ αναφορικά με την έλλειψη ενεργής σύμβασης μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία (βλ. ανωτέρω Σκέψη 19).

22. Βάσει των ανωτέρω, η Αρχή κρίνει ότι συντρέχει περίπτωση να ασκήσει τις κατά το άρθρο 58 παρ. 2 του ΓΚΠΔ διορθωτικές εξουσίες της σε σχέση με τις διαπιστωθείσες παραβάσεις του ΓΚΠΔ.

23. Περαιτέρω, η Αρχή κρίνει ότι ως προς τις διαπιστωθείσες παραβάσεις, σύμφωνα με το άρθρο 58 παρ. 2 κατ' εφαρμογή της διάταξης του άρθρου 58 παρ. 2 εδ. θ' ΓΚΠΔ, προσήκει η επιβολή αποτελεσματικού, αναλογικού και αποτρεπτικού διοικητικού χρηματικού προστίμου, συμφώνως προς τα άρθρα 83 ΓΚΠΔ και 39 του Ν. 4624/2019, τόσο στον υπεύθυνο επεξεργασίας όσο και στον εκτελούντα την επεξεργασία.

24. Για την επιμέτρηση των προστίμων, με βάση το άρθρο 83 του ΓΚΠΔ η Αρχή, λαμβάνει υπόψη τις κατευθυντήριες γραμμές 4/2022 του ΕΣΠΔ για τον υπολογισμό των διοικητικών προστίμων[3] και τα εξής:

i) Η διαπιστωθείσα παράβαση του άρθρου 5 παρ. 1 στοιχ. στ' του ΓΚΠΔ από τον υπεύθυνο επεξεργασίας υπάγεται, σύμφωνα με τις διατάξεις του άρθρου 83 παρ. 5 εδ. α' του ΓΚΠΔ, στην ανώτερη προβλεπόμενη κατηγορία του συστήματος διαβάθμισης διοικητικών προστίμων.

ii) Η διαπιστωθείσα παράβαση του άρθρου 28 του ΓΚΠΔ από τον υπεύθυνο επεξεργασίας την επεξεργασία υπάγεται, σύμφωνα με τις διατάξεις του άρθρου

[3] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_en - έκδοση 2.0, μετά τη διαβούλευση

83 παρ. 4 εδ. α' του ΓΚΠΔ, στην χαμηλότερη προβλεπόμενη κατηγορία του συστήματος διαβάθμισης διοικητικών προστίμων.

iii) Η παραβίαση προσωπικών δεδομένων σχετίζεται με τις κύριες δραστηριότητες του υπευθύνου επεξεργασίας.

iv) Το περιστατικό είχε ως συνέπεια την διακινδύνευση και ειδικής κατηγορίας προσωπικών δεδομένων, των οποίων η παραβίαση μπορεί να επιφέρει σοβαρούς κινδύνους[4].

v) Ο αριθμός των υποκειμένων των δεδομένων που επηρεάστηκαν από το περιστατικό είναι εξαιρετικά μεγάλος.

vi) Δεν έχει διαπιστωθεί προηγούμενη αντίστοιχη παράβαση από τον υπεύθυνο επεξεργασίας.

vii) Η διαπιστωθείσα παράβαση του άρθρου 32 και του άρθρου 28 του ΓΚΠΔ από τον εκτελούντα την επεξεργασία υπάγεται, σύμφωνα με τις διατάξεις του άρθρου 83 παρ. 4 εδ. α' ΓΚΠΔ, στην χαμηλότερη προβλεπόμενη κατηγορία του συστήματος διαβάθμισης διοικητικών προστίμων.

viii) Η παραβίαση προσωπικών δεδομένων σχετίζεται με τις κύριες δραστηριότητες του εκτελούντος την επεξεργασία.

ix) Το περιστατικό είχε ως συνέπεια την διακινδύνευση και ειδικής κατηγορίας προσωπικών δεδομένων, των οποίων η παραβίαση μπορεί να επιφέρει σοβαρούς κινδύνους[5].

x) Ο αριθμός των υποκειμένων των δεδομένων που επηρεάστηκαν από το περιστατικό είναι εξαιρετικά μεγάλος.

xi) Το γεγονός ότι ο κύκλος εργασιών της εταιρείας για το οικονομικό έτος 2024 ανήλθε σε 10.187.657 Ευρώ[6].

[4] Βλ. συναφώς και τη Σκέψη 57 των Κατευθυντηρίων Γραμμών 4/2022 του ΕΣΠΔ.
[5] Βλ. συναφώς και τη Σκέψη 57 των Κατευθυντηρίων Γραμμών 4/2022 του ΕΣΠΔ.
[6] https://publicity.businessportal.gr/company/377501000

xii) Δεν έχει διαπιστωθεί προηγούμενη αντίστοιχη παράβαση από τον εκτελούντα την επεξεργασία.

25. Η Αρχή κρίνει ότι, με βάση τις περιστάσεις που διαπιστώθηκαν και τα ανωτέρω κριτήρια, οι κυρώσεις που αναφέρονται στο διατακτικό της απόφασης είναι το αποτελεσματικό, αναλογικό και αποτρεπτικό μέτρο τόσο προς αποκατάσταση της συμμόρφωσης, όσο και για την τιμωρία της παράνομης συμπεριφοράς.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή:

α) Επιβάλλει με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, διοικητικό πρόστιμο στο Υπουργείο Κοινωνικής Συνοχής και Οικογένειας συνολικού ύψους 150.000 ευρώ, για την παραβίαση του άρθρου 5 παρ. 1 στοιχ. στ'. σε συνδυασμό με το άρθρο 32 παρ. 1 του Κανονισμού (ΕΕ) 2016/679.

β) Επιβάλλει με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, διοικητικό πρόστιμο στο Υπουργείο Κοινωνικής Συνοχής και Οικογένειας συνολικού ύψους 50.000 ευρώ, για την παραβίαση του άρθρου 28 παρ. 3 του Κανονισμού (ΕΕ) 2016/679.

γ) Επιβάλλει με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ διοικητικό πρόστιμο στην εταιρεία με την επωνυμία «Ελληνική Εταιρεία Τοπικής Ανάπτυξης και Αυτοδιοίκησης Α.Ε.» συνολικού ύψους 100.000 ευρώ, για την παραβίαση του άρθρου 32 παρ. 1 του Κανονισμού (ΕΕ) 2016/679.

δ) Επιβάλλει με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ διοικητικό πρόστιμο στην εταιρεία με την επωνυμία «Ελληνική Εταιρεία Τοπικής Ανάπτυξης και Αυτοδιοίκησης Α.Ε.» συνολικού ύψους 50.000 ευρώ, για την παραβίαση του άρθρου 28 παρ. 3 του Κανονισμού (ΕΕ) 2016/679.

ε) Δίνει εντολή με βάση το άρθρο 58 παρ. 2 εδ. δ' του ΓΚΠΔ στο Υπουργείο Κοινωνικής Συνοχής και Οικογένειας και στην εταιρεία με την επωνυμία «Ελληνική Εταιρεία Τοπικής Ανάπτυξης και Αυτοδιοίκησης Α.Ε.» να προβούν άμεσα σε σύναψη της απαιτούμενης σύμβασης σύμφωνα με το άρθρο 28 του ΓΚΠΔ εντός αποκλειστικής

προθεσμίας ενός μήνα από τη λήψη της παρούσας και να ενημερώσουν σχετικά την Αρχή.

στ) Δίνει εντολή με βάση το άρθρο 58 παρ. 2 εδ. δ’ του ΓΚΠΔ στην εταιρεία με την επωνυμία «Ελληνική Εταιρεία Τοπικής Ανάπτυξης και Αυτοδιοίκησης Α.Ε.» να προβεί σε πλήρη υλοποίηση του συνόλου των μέτρων που αναφέρονται στο Εμπιστευτικό Παράρτημα, τα οποία έχει ήδη προγραμματίσει, εντός αποκλειστικής προθεσμίας ενός μήνα από τη λήψη της παρούσας και να ενημερώσει σχετικά την Αρχή προσκομίζοντας την κατάλληλη τεκμηρίωση.

Ο εκτελών χρέη Προέδρου
Αναπληρωτής Πρόεδρος

Γεώργιος Μπατζαλέξης

Η Γραμματέας

Ειρήνη Παπαγεωργοπούλου