

Αθήνα, 10 Οκτωβρίου 2026

## ΕΡΩΤΗΣΗ και ΑΙΤΗΣΗ ΚΑΤΑΘΕΣΗΣ ΕΓΓΡΑΦΩΝ

**Προς: Τον Υπουργό Ψηφιακής Διακυβέρνησης κ. Δημήτρη Παπαστεργίου**  
**Τον Υπουργό Εθνικής Άμυνας κ. Νικόλαο Δένδια**  
**Τον Υπουργό Προστασίας του Πολίτη κ. Μιχάλη Χρυσοχοΐδη**

**Θέμα: «Έκθεση προσωπικών δεδομένων κρατικών αξιωματούχων, στρατιωτικών και στελεχών των Σωμάτων Ασφαλείας σε πλατφόρμες data brokers – Μέτρα προστασίας έναντι της συγκέντρωσης, εμπορικής διάθεσης και στοχευμένης αξιοποίησής τους»**

Σοβαρά ζητήματα προστασίας προσωπικών δεδομένων και ασφάλειας ανέκυψαν μετά από δημοσίευμα της εφημερίδας «Το Βήμα» της 20ής Σεπτεμβρίου 2026, σύμφωνα με το οποίο αριθμοί τηλεφώνων, διευθύνσεις ηλεκτρονικού ταχυδρομείου και άλλα στοιχεία που φέρονται να συνδέονται με κυβερνητικούς αξιωματούχους, πολιτικά πρόσωπα, στρατιωτικούς και στελέχη των Σωμάτων Ασφαλείας εμφανίζονται σε εμπορικές πλατφόρμες συλλογής και διάθεσης δεδομένων, γνωστές ως data brokers.

Στις 21 Σεπτεμβρίου 2026 η Εθνική Αρχή Κυβερνοασφάλειας τοποθετήθηκε επισήμως επί του ζητήματος. Σύμφωνα με την ανακοίνωσή της, από τα στοιχεία που εξετάστηκαν δεν προέκυψε παραβίαση κρατικού πληροφοριακού συστήματος, κακόβουλη πρόσβαση σε κρατική υποδομή ή υποκλοπή. Η Αρχή ανέφερε ότι το υλικό που τέθηκε υπόψη της συνδεόταν με συσώρευση παλαιών, δημοσίως διαθέσιμων ή κατά το παρελθόν κοινοποιημένων πληροφοριών, καθώς και δεδομένων που μπορεί να προέρχονται από καταλόγους, δημόσια προφίλ, παλαιότερες καταχωρίσεις και διαρροές τρίτων υπηρεσιών.

Η συγκεκριμένη διευκρίνιση είναι κρίσιμη, καθώς το ζήτημα δεν αφορά, με βάση τα έως σήμερα επίσημα δεδομένα, επιβεβαιωμένη κυβερνοεπίθεση εναντίον κρατικών πληροφοριακών συστημάτων. Αναδεικνύει όμως ένα διαφορετικό και ευρύτερο πρόβλημα: τη δυνατότητα μαζικής συγκέντρωσης, διασταύρωσης, εμπορικής διάθεσης και επαναχρησιμοποίησης προσωπικών δεδομένων προσώπων που κατέχουν θέσεις αυξημένης ευθύνης.

Η ίδια η Εθνική Αρχή Κυβερνοασφάλειας αναγνώρισε στην ανακοίνωσή της ως «υπαρκτό διαρθρωτικό πρόβλημα» την ανεξέλεγκτη εμπορία προσωπικών δεδομένων και την ανάγκη θεσμικής αντιμετώπισής της σε ευρωπαϊκό επίπεδο.

Παράλληλα, διατύπωσε συγκεκριμένες συστάσεις, μεταξύ των οποίων τον έλεγχο και την αφαίρεση παλαιών προσωπικών στοιχείων από ιστοσελίδες φορέων, την υποβολή αιτημάτων διαγραφής προς data brokers, την αποφυγή δημοσιοποίησης προσωπικών αριθμών κινητής τηλεφωνίας και ιδιωτικών διευθύνσεων ηλεκτρονικού ταχυδρομείου σε ανακοινώσεις, έγγραφα και συνημμένα αρχεία, καθώς

και την ενίσχυση της ασφάλειας λογαριασμών υψηλής αξίας με ισχυρότερες μεθόδους πολυπαραγοντικής ταυτοποίησης.

Η διαθεσιμότητα μεμονωμένων στοιχείων στο διαδίκτυο αποκτά διαφορετική διάσταση όταν αυτά συγκεντρώνονται, συσχετίζονται και οργανώνονται σε ενιαίο ψηφιακό προφίλ. Στην περίπτωση στρατιωτικών, στελεχών των Σωμάτων Ασφαλείας, στελεχών κρίσιμων κρατικών υπηρεσιών και κυβερνητικών αξιωματούχων, μια τέτοια συγκέντρωση πληροφοριών μπορεί να διευκολύνει απόπειρες στοχευμένης εξαπάτησης, κοινωνικής μηχανικής, πλαστοπροσωπίας, παραβίασης λογαριασμών ή άλλες ενέργειες που απαιτούν ιδιαίτερη αξιολόγηση κινδύνου.

Ιδιαίτερη σημασία έχει επίσης το γεγονός ότι το πρόβλημα δεν περιορίζεται σε δεδομένα που τηρούνται από το Δημόσιο. Οι data brokers μπορούν να συγκεντρώνουν πληροφορίες από διαφορετικές πηγές και διαφορετικές χρονικές περιόδους, δημιουργώντας προφίλ τα οποία ενδέχεται να περιλαμβάνουν παλαιά, ανακριβή ή ήδη δημοσιοποιημένα στοιχεία μαζί με νεότερες πληροφορίες.

Η προστασία των προσωπικών δεδομένων στελεχών που υπηρετούν σε ευαίσθητες θέσεις δεν αποτελεί αποκλειστικά ζήτημα ιδιωτικότητας. Συνδέεται με την κυβερνοασφάλεια, την προστασία των Ενόπλων Δυνάμεων και των Σωμάτων Ασφαλείας, την ασφάλεια κρίσιμων κρατικών λειτουργιών και την πρόληψη στοχευμένων επιθέσεων κοινωνικής μηχανικής.

#### **Με βάση τα ανωτέρω, ερωτάσθε:**

1. Μετά τη γνωστοποίηση του ζητήματος στις αρχές Σεπτεμβρίου 2026, πραγματοποιήθηκε από τις αρμόδιες κρατικές υπηρεσίες συστηματικός έλεγχος για την έκθεση προσωπικών ή υπηρεσιακών στοιχείων κυβερνητικών αξιωματούχων, στελεχών των Ενόπλων Δυνάμεων, των Σωμάτων Ασφαλείας και άλλων υπηρεσιών αυξημένης κρισιμότητας σε πλατφόρμες data brokers;
2. Εφόσον πραγματοποιήθηκε σχετικός έλεγχος, πόσα πρόσωπα ή καταχωρίσεις εντοπίστηκαν ανά γενική κατηγορία υπηρεσίας, χωρίς αναφορά σε ονόματα ή άλλα προσωπικά δεδομένα; Διαπιστώθηκαν περιπτώσεις στις οποίες υπήρχαν ενεργά και επικαιροποιημένα στοιχεία επικοινωνίας;
3. Έχει πραγματοποιηθεί ειδική αξιολόγηση του κινδύνου που δημιουργείται από τη δυνατότητα συγκέντρωσης και συσχέτισης προσωπικών και επαγγελματικών δεδομένων προσώπων που υπηρετούν σε θέσεις σχετικές με την εθνική άμυνα, τη δημόσια ασφάλεια, την κυβερνοασφάλεια ή τη λειτουργία κρίσιμων υποδομών;
4. Έχουν ενημερωθεί τα στελέχη για τα οποία διαπιστώθηκε έκθεση στοιχείων τους και έχουν δοθεί συγκεκριμένες οδηγίες για την προστασία των προσωπικών και υπηρεσιακών λογαριασμών τους;

5. Έχουν υποβληθεί από κρατικούς φορείς ή κατόπιν κρατικής καθοδήγησης αιτήματα αφαίρεσης ή διαγραφής προσωπικών δεδομένων προς πλατφόρμες data brokers; Εάν ναι, πόσα αιτήματα έχουν υποβληθεί, προς πόσους διαφορετικούς παρόχους και πόσα έχουν έως σήμερα ικανοποιηθεί;
6. Έχουν πραγματοποιηθεί έλεγχοι σε ιστοσελίδες υπουργείων, εποπτευόμενων οργανισμών, δημόσιες ανακοινώσεις, αναρτήσεις και συνοδευτικά έγγραφα προκειμένου να εντοπιστούν παλαιές δημοσιεύσεις προσωπικών τηλεφωνικών αριθμών, ιδιωτικών διευθύνσεων ηλεκτρονικού ταχυδρομείου ή άλλων στοιχείων στελεχών που δεν είναι απαραίτητο να παραμένουν δημόσια διαθέσιμα;
7. Έχουν εκδοθεί μετά τις σχετικές αποκαλύψεις δεσμευτικές οδηγίες προς δημόσιους φορείς ώστε να αποφεύγεται η ανάρτηση προσωπικών κινητών τηλεφώνων και ιδιωτικών ηλεκτρονικών διευθύνσεων σε ανακοινώσεις, ιστοσελίδες, έγγραφα και ηλεκτρονικά συστήματα δημόσιας πρόσβασης;
8. Υφίσταται ειδικό πρωτόκολλο ψηφιακής ασφάλειας για πρόσωπα και λογαριασμούς αυξημένης αξίας ή επικινδυνότητας, ιδίως ως προς τη χρήση ξεχωριστών προσωπικών και υπηρεσιακών στοιχείων επικοινωνίας, την πολυπαραγοντική ταυτοποίηση και τη χρήση σύγχρονων μεθόδων προστασίας από υποκλοπή διαπιστευτηρίων;
9. Έχει εξεταστεί η εφαρμογή της σύστασης της Εθνικής Αρχής Κυβερνοασφάλειας για χρήση ισχυρότερων μεθόδων ταυτοποίησης, όπως φυσικά κλειδιά ασφαλείας ή passkeys, σε λογαριασμούς υψηλής αξίας και ευαισθησίας;
10. Ποιος είναι ο προβλεπόμενος μηχανισμός συνεργασίας μεταξύ της Εθνικής Αρχής Κυβερνοασφάλειας, των αρμόδιων Υπουργείων και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για περιστατικά κατά τα οποία δεδομένα στελεχών ευαίσθητων κρατικών υπηρεσιών εμφανίζονται σε εμπορικές βάσεις δεδομένων;
11. Υπάρχει σήμερα κεντρικός μηχανισμός μέσω του οποίου το Ελληνικό Δημόσιο μπορεί να εντοπίζει συστηματικά δεδομένα στελεχών του σε data brokers που εδρεύουν εντός ή εκτός Ευρωπαϊκής Ένωσης και να κινεί διαδικασίες αφαίρεσης ή περιορισμού της επεξεργασίας τους;
12. Ποιες πρωτοβουλίες προτίθεται να αναλάβει η Ελληνική Κυβέρνηση, σε εθνικό και ευρωπαϊκό επίπεδο, για την αποτελεσματικότερη εποπτεία της δραστηριότητας των data brokers, ιδίως όταν η συγκέντρωση δεδομένων αφορά πρόσωπα που υπηρετούν σε θέσεις αυξημένης σημασίας για την ασφάλεια του κράτους;

**Και αιτούμεθα την κατάθεση των παρακάτω εγγράφων:**

Παρακαλούνται οι αρμόδιοι Υπουργοί να καταθέσουν στη Βουλή, στο μέτρο που τα σχετικά έγγραφα δεν είναι διαβαθμισμένα, δεν περιλαμβάνουν προσωπικά δεδομένα και η δημοσιοποίησή τους δεν δημιουργεί κίνδυνο για την εθνική ή τη δημόσια ασφάλεια:

1. Τις εγκυκλίους, οδηγίες ή λοιπά έγγραφα που έχουν εκδοθεί από τις 7 Σεπτεμβρίου 2026 και μετά σχετικά με την προστασία προσωπικών και υπηρεσιακών στοιχείων κυβερνητικών αξιωματούχων, στρατιωτικών, στελεχών των Σωμάτων Ασφαλείας και λοιπών προσώπων αυξημένου κινδύνου από τη συγκέντρωση και διάθεσή τους μέσω data brokers.
2. Τις τυχόν μη διαβαθμισμένες και ανωνυμοποιημένες εκτιμήσεις ή αξιολογήσεις κινδύνου που έχουν συνταχθεί από αρμόδιες κρατικές υπηρεσίες αναφορικά με την έκθεση τέτοιων δεδομένων.
3. Συγκεντρωτικά και πλήρως ανωνυμοποιημένα στοιχεία σχετικά με τον αριθμό των αιτημάτων αφαίρεσης ή διαγραφής δεδομένων που υποβλήθηκαν προς data brokers από τις 7 Σεπτεμβρίου 2026 μέχρι την ημερομηνία απάντησης στην παρούσα, καθώς και τον αριθμό των αιτημάτων που ικανοποιήθηκαν.
4. Τις μη διαβαθμισμένες οδηγίες που έχουν αποσταλεί σε δημόσιους φορείς σχετικά με τη δημοσιοποίηση προσωπικών αριθμών κινητής τηλεφωνίας, ιδιωτικών διευθύνσεων ηλεκτρονικού ταχυδρομείου και άλλων στοιχείων επικοινωνίας στελεχών τους.
5. Κάθε μη διαβαθμισμένο έγγραφο από το οποίο προκύπτουν οι ενέργειες που έχουν πραγματοποιηθεί για την εφαρμογή των δημόσια διατυπωμένων συστάσεων της Εθνικής Αρχής Κυβερνοασφάλειας αναφορικά με τον καθαρισμό παλαιού ψηφιακού αποτυπώματος, την αφαίρεση προσωπικών στοιχείων από παλαιές διαδικτυακές αναρτήσεις και την ενίσχυση της ασφάλειας λογαριασμών υψηλής αξίας.
6. Τα διαθέσιμα συγκεντρωτικά στοιχεία, χωρίς οποιαδήποτε αναφορά σε ταυτοποιήσιμα φυσικά πρόσωπα, σχετικά με τον αριθμό των περιπτώσεων στις οποίες εντοπίστηκε έκθεση δεδομένων στελεχών των Ενόπλων Δυνάμεων, των Σωμάτων Ασφαλείας ή άλλων κρίσιμων κρατικών υπηρεσιών σε εμπορικές πλατφόρμες συγκέντρωσης δεδομένων.

Η Βουλευτής

Ασπασία Ιωάννη Κουρουπάκη  
ΒΟΥΛΕΥΤΗΣ Β1' ΒΟΡΕΙΟΥ ΤΟΜΕΑ ΑΘΗΝΩΝ