



Κάσος, 18 Μαΐου 2025
Αρ. Πρωτοκόλλου: 2505.14

ΠΡΟΣ: κ. Μιχάλη Ερωτόκριτο
Δήμαρχο Η.Ν. Κάσου

ΚΟΙΝΟΠ.: κ. Γεώργιο Κουριαντάκη
Πρόεδρο επιτροπής ψηφιακού
μετασχηματισμού

ΘΕΜΑ: Επισήμανση ελλείψεων
συμμόρφωσης της ιστοσελίδας
kasos-heroicisland.gr με τον GDPR
και ανάγκη ενίσχυσης της
κυβερνοασφάλειας των ψηφιακών
υποδομών του Δήμου

Αγαπητέ Δήμαρχε,
Αγαπητέ Πρόεδρε της επιτροπής Ψηφιακού Μετασχηματισμού,

Στο πλαίσιο των αρμοδιοτήτων μου ως μέλος της Επιτροπής Ψηφιακού Μετασχηματισμού και δεδομένης της επαγγελματικής μου εμπειρίας στον τομέα της πληροφορικής, προέβην σε έλεγχο της επίσημης ιστοσελίδας του Δήμου μας kasos-heroicisland.gr, καθώς και της γενικότερης ψηφιακής παρουσίας και υποδομής του Δήμου, με στόχο την αξιολόγηση της συμμόρφωσης με τον **Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)** και την **ασφάλεια των πληροφοριακών συστημάτων**.

Τα ευρήματα μου είναι αρκετά κρίσιμα και παρουσιάζονται παρακάτω:

1. Νομικές Ελλείψεις (GDPR):

- Απουσία **αναλυτικής Πολιτικής Απορρήτου** και **Όρων Χρήσης**.
- Έλλειψη **αναφοράς σε Υπεύθυνο Προστασίας Δεδομένων (DPO)**.
- Ελλιπής **πολιτική cookies** και μη προσβάσιμες πληροφορίες από το υποσέλιδο.
- Απουσία διαδικασιών για την **άσκηση δικαιωμάτων των πολιτών** (π.χ. διαγραφή, διόρθωση, φορητότητα).

2. Ελλείψεις στην Κυβερνοασφάλεια:

Δεν διαπιστώθηκε **καμία δημόσια ή μη αναφορά ή τεκμηρίωση πολιτικής κυβερνοασφάλειας**.

Δεν υπάρχουν ενδείξεις για:

- **Firewall ή προστασία από επιθέσεις DDoS**
- **Κρυπτογράφηση δεδομένων**
- **Διαχείριση πρόσβασης και ελέγχου ταυτότητας**
- **Διαδικασίες ανάκαμψης από κυβερνοεπιθέσεις**

Η απουσία αυτών των μέτρων καθιστά τις υποδομές του Δήμου **ευάλωτες σε επιθέσεις**, όπως:

- **Ransomware** (κλείδωμα αρχείων και απαίτηση λύτρων)
- **Phishing** (παραπλάνηση υπαλλήλων)
- **Data breaches** (διαρροή προσωπικών δεδομένων πολιτών)

Η **Οδηγία NIS2** (Network and Information Security Directive) είναι η νέα ευρωπαϊκή οδηγία για την κυβερνοασφάλεια, η οποία **ενσωματώθηκε στην ελληνική νομοθεσία με τον Νόμο 5160/2024 (ΦΕΚ Α' 195/27.11.2024)**

Τι προβλέπει η NIS2:

- **Υποχρεωτική συμμόρφωση** για δημόσιους και ιδιωτικούς φορείς που παρέχουν κρίσιμες ή σημαντικές υπηρεσίες — περιλαμβάνονται και οι **Οργανισμοί Τοπικής Αυτοδιοίκησης (ΟΤΑ)**.
- **Υποχρέωση αναφοράς περιστατικών κυβερνοασφάλειας** εντός 24 ωρών από τη διαπίστωση.
- **Ευθύνη της διοίκησης** για την εφαρμογή πολιτικών ασφάλειας (όχι μόνο των τεχνικών υπευθύνων).
- **Διοικητικά πρόστιμα και κυρώσεις** σε περίπτωση μη συμμόρφωσης, ακόμα και **προσωρινή αναστολή λειτουργίας υπηρεσιών ή ευθύνη φυσικών προσώπων**.

3. Κίνδυνοι και Επιπτώσεις:

- **Διοικητικά πρόστιμα** από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
- **Απώλεια εμπιστοσύνης των πολιτών** και δυσφήμιση του Δήμου.
- **Διακοπή λειτουργίας κρίσιμων υπηρεσιών** σε περίπτωση κυβερνοεπίθεσης.
- **Νομικές ευθύνες** για παραβίαση προσωπικών δεδομένων.

4. Προτάσεις:

1. **Άμεση συμμόρφωση με τον GDPR** με σύνταξη και ανάρτηση των απαραίτητων πολιτικών.
2. **Σύνταξη και εφαρμογή Στρατηγικής Κυβερνοασφάλειας**, με:
 - Ανάλυση κινδύνων (risk assessment)

- Εκπαίδευση προσωπικού
 - Εφαρμογή τεχνικών μέτρων προστασίας
3. **Ορισμός DPO και Υπεύθυνου Κυβερνοασφάλειας.**
 4. **Αξιοποίηση εθνικών εργαλείων μέσω της Εθνική Αρχή Κυβερνοασφάλειας και βέβαια τις οδηγίες της Εθνικής Αρχής Κυβερνοασφάλειας.**

Η προστασία των ψηφιακών υποδομών και των προσωπικών δεδομένων των πολιτών μας δεν είναι απλώς νομική υποχρέωση, αλλά και ηθική ευθύνη.

Είμαι στη διάθεσή σας για περαιτέρω συνεργασία και υποστήριξη.



Με εκτίμηση,
Εμμανουήλ Ι. Πέπης

Δημοτικός Σύμβουλος
«ΜΑΖΙ ΓΙΑ ΤΗΝ ΚΑΣΟ»

manos@pepis.gr
kasos@mazigiathnkaso.gr