

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ



ΑΝΑΦΟΡΑ

Αθήνα, 22/07/2020

Του: Κυριάκου Βελόπουλου, Προέδρου Κόμματος, Βουλευτή Λάρισας

ΠΡΟΣ: Τον κ. Υπουργό Ψηφιακής Διακυβέρνησης, Κυριάκο Πιερρακάκη

ΘΕΜΑ: «Καταγγελία της “Ένωσης Πληροφορικών Ελλάδος” για ελλιπή μέτρα ασφαλείας σε ιστοτόπους δημοσίων φορέων στο διαδίκτυο»

Κύριε Υπουργέ,

Παρακαλούμε για την τοποθέτησή σας επί του επισυναπτόμενου Δελτίου Τύπου, με αρ. πρωτ. εξερχομένων: «L20-0717-01V1», της 17/07/2020, που μας προώθησε η «Ένωση Πληροφορικών Ελλάδος», υπογεγραμμένο από την Πρόεδρο του ΔΣ της ανωτέρω Ένωσης, κα Χ. Ξανθάκη, τον Αντιπρόεδρο του ΔΣ της Ένωσης, κο Δ. Κυριακό, τον Γ. Γραμματέα του ΔΣ της Ένωσης, κ. Χ. Γεωργίου, τον Ειδ. Γραμματέα του ΔΣ της Ένωσης, κ. Φ. Αλεξάκο και τον Ταμία του ΔΣ της Ένωσης, κ. Ι. Φάκα, στο οποίο διατυπώνεται η ανησυχία τους για την απουσία προδιαγραφών ασφαλείας σε αριθμό ιστοσελίδων του διαδικτύου που διαχειρίζονται φορείς του Ελληνικού Δημοσίου, όσον αφορά τον κίνδυνο διαρροής προσωπικών δεδομένων των επισκεπτών χρηστών κατά την αρμόδια χρήση των εφαρμογών τους, προσθέτοντας ότι, απουσιάζει για τις ανωτέρω το πιστοποιητικό ασφάλειας σύνδεσης “SSL”, ενώ οι εν λόγω ιστοσελίδες απαριθμούνται στο τέλος της εν λόγω επιστολής.

Με δεδομένα όλα τα παραπάνω, και αφού λάβετε υπόψη το συνημμένο Δελτίο Τύπου, σας παρακαλώ να το εξετάσετε και να αποφανθείτε σχετικά.

Ο Αναφέρων Βουλευτής

Κυριάκος Βελόπουλος

Επισυνάπτεται: Αντίγραφο του ως άνω Δελτίου Τύπου

Προς: Γενική Γραμματεία Ψηφιακής Πολιτικής
Κοινωνία της Πληροφορίας Α.Ε.
Υπουργείο Οικονομικών
Υπουργείο Εσωτερικών

Κοιν: Γραφεία Τύπου πολιτικών κομμάτων
ΜΜΕ

Αθήνα, 17/7/2020

ΔΕΛΤΙΟ ΤΥΠΟΥ

«Ελλιπή τεχνικά μέτρα ασφάλειας σε ιστοτόπους δημόσιων φορέων»

Αξιότιμοι Κύριοι,

Πολύς λόγος γίνεται σήμερα για την ασφάλεια των προσωπικών δεδομένων των πολιτών, ιδίως σε σχέση με παρεχόμενες σε αυτούς ψηφιακές υπηρεσίες από δημόσιους και ιδιωτικούς φορείς. Από το 2018 έχει τυπικά τεθεί σε ισχύ ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)¹ για την προστασία των προσωπικών δεδομένων των πολιτών. Παρόλα αυτά, στη χώρα μας φαίνεται να υπάρχουν ακόμη πολλά κενά στο θέμα αυτό. Θα προσπαθήσουμε να γίνουμε σαφέστεροι μ' ένα παράδειγμα/μελέτη περίπτωσης.

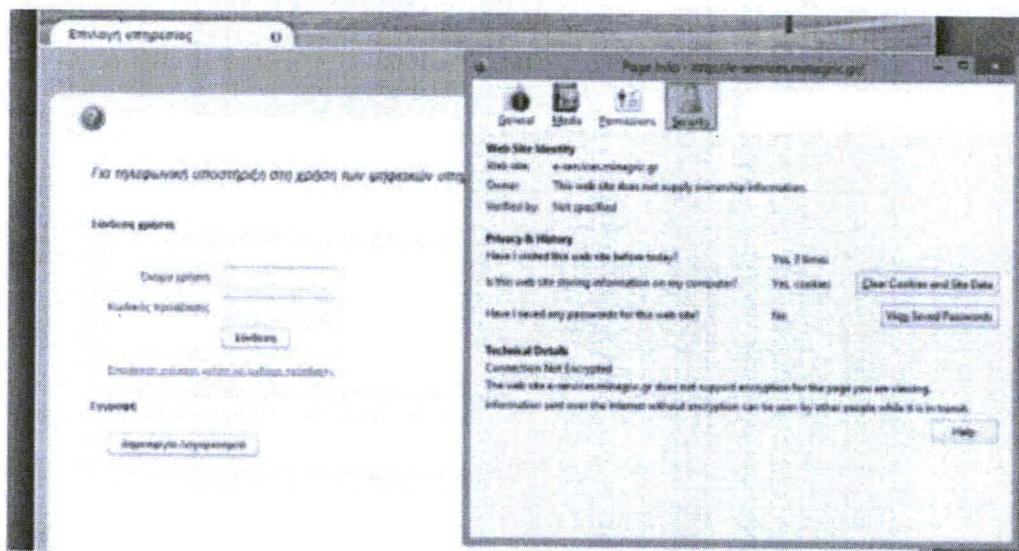
Ας υποθέσουμε λοιπόν ότι έρχεται ο καιρός για κάποιον αγρότη να ενημερώσει διαδικτυακά το μητρώο του στον Ο.Π.Ε.Κ.Ε.Π.Ε.² προκειμένου να αναγνωρίζεται ως αγρότης με ό,τι φορολογικά ή άλλα οφέλη αποκομίζει από αυτή του την ιδιότητα. Πρόκειται δηλαδή για εργασία που είναι υποχρεωτική για τον καθένα τους. Πλέον, θα χρειαστεί να επισκεφθεί τον ιστότοπο³ του μητρώου αγροτών του ΥΠΑΑΤ (Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων), ο οποίος πράγματι έχει ασφάλεια με πιστοποιητικό SSL. Αφού όμως γίνει η είσοδος εκεί με τον μηχανισμό ταυτοποίησης του TaxisNet και εφόσον δεν υπάρχουν ακόμη στοιχεία στο μητρώο, απαιτείται εγγραφή στον ιστότοπο⁴ ηλεκτρονικών υπηρεσιών του ΥΠΑΑΤ, ο οποίος όμως δεν παρέχει υποστήριξη κρυπτογραφημένης σύνδεσης HTTPS (συγκεκριμένα λείπει το 'S' - secure από το URL που χρησιμοποιεί απλό πρωτόκολλο HTTP).

1 <https://is.gd/ef6tGP>

2 <https://is.gd/ddh27Y>

3 <https://maae.minagric.gr/maae/>

4 <http://e-services.minagric.gr>



Μάλιστα φαίνεται ότι από το 2015 έχει να ενημερωθεί και να αναβαθμιστεί η υποδομή της εν λόγω ηλεκτρονικής πλατφόρμας. Η πολιτική χρήσης είναι αρκετά λιτή και ελλιπής, μόλις μια σελίδα⁵, ενώ δεν υπάρχει πολιτική χρήσης προσωπικών δεδομένων ούτε ενημέρωση για το GDPR. Παρόλα αυτά υπάρχει και μια σύνδεση της Google Analytics⁶ για την καταγραφή στατιστικών επισκεψιμότητας, κάτι που δεν είναι απαραίτητο και καθόλου χρήσιμο για τη σωστή λειτουργία της ηλεκτρονικής αυτής υπηρεσίας.

Τα παραπάνω θα έπρεπε να αποθαρρύνουν κάθε σώφρονα πολίτη να χρησιμοποιήσει την εν λόγω ηλεκτρονική υπηρεσία, τουλάχιστον μέχρις ότου η πλατφόρμα αποκτήσει ασφάλεια σύνδεσης με πιστοποιητικό SSL. Παρόλα αυτά, οι πολίτες οδηγούνται από το κράτος στο να εκθέσουν τα δεδομένα τους σε κίνδυνο χωρίς καμία διασφάλιση εμπιστευτικότητας. Ακολούθως, όσο αυξάνεται ο αριθμός των χρηστών τόσο αυξάνεται ο κίνδυνος παραβίασης και κλοπής προσωπικών δεδομένων, καθώς αυξάνεται το προσδοκώμενο όφελος από μια τέτοια παραβίαση ασφάλειας.

Παρόμοια προβλήματα είχαμε καταδείξει και στο παρελθόν⁷ σχετικά με ιδιώτη ανάδοχο της υπηρεσίας του Κτηματολογίου Αθηνών⁸. Ευτυχώς τότε οι παρατηρήσεις μας είχαν υιοθετηθεί από τους εμπλεκόμενους Δημόσιους και Ιδιωτικούς φορείς, με αποτέλεσμα την -έστω και πρόχειρη- λήψη ανάλογων μέτρων από τους τελευταίους.

⁵ <https://is.gd/PqalYS>

⁶ <https://analytics.withgoogle.com/>

⁷ <https://is.gd/mn8B15>

⁸ <https://www.ktimatologio-athina.gr/>

Για να καταδείξουμε τη σημασία του πρωτοκόλλου HTTPS, επισημαίνουμε ότι από το 2017 και μετά, τα προγράμματα πλοήγησης (browsers) Mozilla Firefox, Google Chrome, Opera, Vivaldi και Microsoft Edge προειδοποιούν τους χρήστες για το ότι η σύνδεση με συγκεκριμένους ιστότοπους επίσκεψης ενδέχεται να μην είναι ασφαλής. Επίσης, από τον Ιούλιο του 2018 και μετά την κυκλοφορία της έκδοσης 68, το Chrome επισημαίνει πλέον όλες τις τοποθεσίες HTTP (δηλαδή όσες δεν διαθέτουν SSL) ως «μη ασφαλείς», υποστηρίζοντας έντονα ότι οι ιστότοποι πρέπει να υιοθετήσουν την κρυπτογράφηση HTTPS, με την εγκατάσταση ενός πιστοποιητικού ασφαλείας SSL⁹.

Με αφορμή το παραπάνω ενδεικτικό παράδειγμα, θεωρούμε πως είναι πλέον επιτακτική ανάγκη να γίνει καταγραφή των ιστοτόπων του δημόσιου τομέα που δεν είναι επαρκώς ασφαλείς, ώστε οι αντίστοιχες υπηρεσίες να μεταβούν άμεσα στην αντίστοιχη αναβάθμιση των ψηφιακών υποδομών τους, ιδίως σε αυτήν την εποχή της Πανδημίας που η αξιοποίηση ψηφιακών υπηρεσιών έχει γίνει απαραίτητη. Μια ενδεχομένως καλή αρχή θα ήταν οι διαχειριστές των “προβληματικών” ιστοτόπων να χρησιμοποιήσουν δωρεάν πιστοποιητικά SSL από υπηρεσίες όπως π.χ. η Let’s Encrypt¹⁰, μέχρις ότου μεταβούν σε άλλη αρχή πιστοποίησης που θα προσφέρει πιστοποιητικά με περισσότερα χαρακτηριστικά που θα καλύπτουν καλύτερα τις ανάγκες τους.

Στο παρακάτω παράρτημα παραθέτουμε μια ενδεικτική λίστα ιστοτόπων που πρέπει να αξιολογηθούν ως προς τη συμμόρφωση με το GDPR και την ασφάλεια που παρέχουν στον χρήστη.

Με εκτίμηση,

Το ΔΣ της Ένωσης Πληροφορικών Ελλάδας (ΕΠΕ)

Η Πρόεδρος	Ο Αντιπρόεδρος	Ο Γενικός Γραμματέας	Ο Ειδικός Γραμματέας	Ο Ταμίας
Χαρά Ξανθάκη proedros@epe.org.gr	Δημήτρης Κυριακός antiproedros@epe.org.gr	Χάρης Γεωργίου gen_grammateas@epe.org.gr	Φώτης Αλεξάκος eid_grammateas@epe.org.gr	Γιάννης Φάκας tamias@epe.org.gr

Ένωση Πληροφορικών Ελλάδας, Τ.Θ. 13801, Τ.Κ. 10310, Αθήνα
Email: info@epe.org.gr – Τηλέφωνο: 698 172 3690

⁹ <https://is.gd/ZwIXuM>

¹⁰ <https://letsencrypt.org>

ΠΑΡΑΡΤΗΜΑ

Αρμόδιοι φορείς τηλεπικοινωνιών

<http://www.adae.gr/> - ΑΑΔΕ

Υπουργεία

<http://www.mindev.gov.gr/> - Υπουργείο Ανάπτυξης

<http://www.minagric.gr/> - ΥΠΠΑΤ - Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων

<http://visitgreece.gr/> - Εθνικός Οργανισμός Τουρισμού - καμπάνια Visit Greece

(Υπ. Εργασίας)

<http://oaed.gr/> - ΟΑΕΔ - Οργανισμός Απασχόλησης Εργατικού Δυναμικού

Ασφαλιστικά ταμεία

<http://www.tsay.gr/> - ΤΣΑΥ - Ταμείο Σύνταξης Ασφάλισης Υγειονομικών

<http://www.etaa.gr/> - ΕΤΑΑ - Ενιαίο Ταμείο Ανεξάρτητα Απασχολούμενων

Παιδεία

<http://ebooks.edu.gr/> - Αποθετήριο σχολικών βιβλίων

<http://duth.gr/> - Δημοκρίτειο Πανεπιστήμιο Θράκης

Διοικητικοί φορείς

<http://www.et.gr/> - Εθνικό Τυπογραφείο

<http://www.opengov.gr/> - Ανοιχτή Διακυβέρνηση

<http://www.data.gov.gr/> - Ανοιχτά Δεδομένα

<http://www.kep.gov.gr/> - Κέντρο Εξυπηρέτησης Πολιτών

<http://www.e-poleodomia.gr/> - Πολεοδομία

Νομικά

<http://www.areiospagos.gr/> - Άρειος Πάγος

<http://www.gak.gr/> - Γενικά Αρχεία του Κράτους

Αρμόδιοι φορείς αγροτικού τομέα

<http://elga.gr/> - ΕΓΛΑ - Οργανισμού Ελληνικών Γεωργικών Ασφαλίσεων

Συγκοινωνίες

<http://www.olp.gr/en/> - Οργανισμός Λιμένα Πειραιά

Σώματα ασφαλείας

<http://www.astynomia.gr/> - Ελληνική Αστυνομία

<http://www.passport.gov.gr/> - Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας - Ελληνική

Αστυνομία

