ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Αρ. Πρωτ: L21-0518-01V1

Προς: Υπουργείο Ψηφιακής Διακυβέρνησης
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Αρχή Διασφάλισης Απορρήτου Επικοινωνιών

Κοιν: Γραφεία Τύπου πολιτικών κομμάτων
ΜΜΕ

Αθήνα, 18/05/2021

Σοβαρό πρόβλημα ασφάλειας στην πλατφόρμα gov.gr

Αξιότιμοι Κύριοι,

Θα θέλαμε να θέσουμε υπ' όψιν σας το παρακάτω σημαντικό πρόβλημα ασφάλειας κατά την επικύρωση εγγράφου που έχει παραχθεί από τις υπηρεσίες του gov.gr (https://is.gd/oDWlC9).

Συγκεκριμένα, παρατηρήσαμε πως μπορεί κανείς να βρει με απλή αναζήτηση στο Google υπερσύνδεσμο (URL) που εμφανίζει την υπεύθυνη δήλωση πολίτη, άσχετου με αυτόν που κάνει την αναζήτηση, ο οποίος έχει δημιουργήσει την δήλωσή του μέσω της πλατφόρμας: https://dilosi.services.gov.gr/create/q/templates. Πρακτικά, αν οποιοσδήποτε βρει από κάποια πηγή ή εντελώς τυχαία τον κωδικό hash key που χρησιμοποιείται για την επικύρωση (validation) τέτοιων εγγράφων εδώ: https://dilosi.services.gov.gr/show/q/validate, **αποκτά αυτόματα στην κατοχή του ένα PDF έγγραφο με όλα τα στοιχεία του υπογράφοντος την υπεύθυνη δήλωση**. Και όλα αυτά είναι διαθέσιμα με ένα απλό URL, χωρίς κανένα έλεγχο πρόσβασης ή αυθεντικοποίηση (login) του χρήστη. Μπορεί μάλιστα να κατεβάσει το έγγραφο τοπικά με την ψηφιακή υπογραφή του Υπουργείου, δηλαδή έτοιμο προς οποιαδήποτε νόμιμη χρήση.

Για του λόγου το αληθές επισυνάπτουμε screenshot (Παράρτημα Α). Έχουν αποκρυφτεί τα ευαίσθητα στοιχεία, έχουμε όμως το URL στη διάθεση οποιουδήποτε για επαλήθευση, καθώς και σχετικές αναφορές παρόμοιων περιστατικών από συναδέλφους μας.

Καταλαβαίνετε φυσικά πως πρόκειται για σοβαρή καταστρατήγηση του πλαισίου της προστασίας των προσωπικών δεδομένων βάσει του GDPR, καθώς και της κείμενης νομοθεσίας σχετικά με την Πολιτική Ασφάλειας που υποχρεωτικά πρέπει να εφαρμόζει κάθε παρόμοια υπηρεσία στο διαδίκτυο. Η προστασία και μόνο με ένα hash key, χωρίς έλεγχο πρόσβασης, χωρίς αυθεντικοποίηση (login) του χρήστη και χωρίς διαδικασία ρητής άδειας μεταβίβασης μεταξύ κατόχου-παραλήπτη, βρίσκεται σαφέστατα εκτός των ελάχιστων υποχρεωτικών προδιαγραφών, όπως ορίζονται σαφέστατα από τη σχετική νομοθεσία.

Το παραπάνω σοβαρότατο κενό ασφάλειας είναι κάτι που από τεχνικής πλευράς θα μπορούσε να διορθωθεί εύκολα και κυρίως πολύ γρήγορα. Εντελώς ενδεικτικά, θα μπο-

ρούσε η επικύρωση να γίνεται **μόνο μέσα σε session** με απαίτηση login από συγκεκριμένο εξουσιοδοτημένο πρόσωπο, το οποίο θα ήταν και ο μόνος που θα είχε το hash key. Θα μπορούσε επίσης να απαιτείται κάποιο επιπλέον συνθηματικό (γενικότερα security token) που θα γνώριζε μόνο ο πολίτης που έχει δημιουργήσει το έγγραφο.

Ακόμα σωστότερο και αποτελεσματικό θα ήταν στην πλατφόρμα να υπάρχει οργανωμένο προσωπικό αρχείο με ψηφιακά έγγραφα το πολίτη στα οποία θα μπορεί να δίνει επιλεκτικά πρόσβαση σε συγκεκριμένα τρίτα πρόσωπα ή φορείς μετά από σχετική (αυτόματη) αίτησή τους στην πλατφόρμα, έτσι ώστε να διατηρείται η αρχή της διμερούς και μόνο ανταλλαγής εγγράφων, όπως άλλωστε γίνεται και με αντίστοιχα φυσικά έγγραφα που βεβαίως δεν αναρτώνται πουθενά δημόσια για χρήση από οποιονδήποτε το επιθυμεί ή απλά γνωρίζει την ύπαρξή τους.

Σε κάθε περίπτωση, το ζήτημα είναι πολύ κρίσιμο και **πρέπει να επιλυθεί άμεσα**. Η Ένωσή μας παραμένει στη διάθεσή σας για οποιαδήποτε επιστημονική βοήθεια ή άλλου είδους συνδρομή.

Τέλος, οφείλουμε να ενημερώσουμε πως βάσει του πλαισίου GDPR (άρθρο 33), καθώς και του Κώδικα Δεοντολογίας των Πληροφορικών (https://tinyurl.com/cf4rzvxb) σχετικά με το Δημόσιο Συμφέρον και την Υποχρέωση Γνωστοποίησης, είμαστε υποχρεωμένοι να δημοσιοποιήσουμε το εν λόγω κενό ασφαλείας σε 72 ώρες από τη στιγμή αποστολής της παρούσας επιστολής προς εσάς.

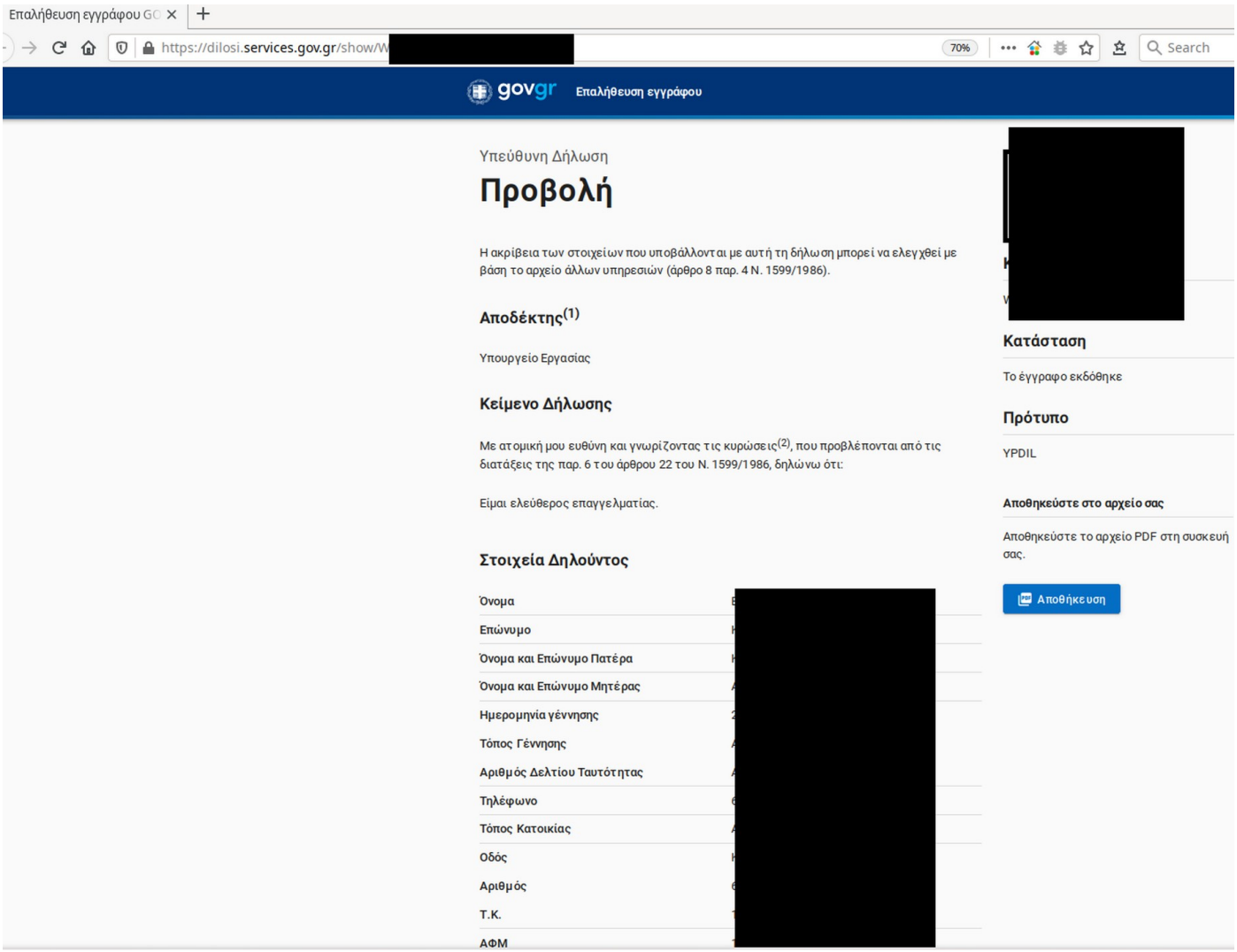
Με εκτίμηση,

Το ΔΣ της Ένωσης Πληροφορικών Ελλάδας (ΕΠΕ)

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

Ένωση Πληροφορικών Ελλάδας, Τ.Θ. 13801, Τ.Κ. 10310, Αθήνα
Email: info@epe.org.gr – Τηλέφωνο: 210 5699408

ΠΑΡΑΡΤΗΜΑ Α


Επαλήθευση εγγράφου
https://dilosi.services.gov.gr/show/[redacted]
Search
govgr Επαλήθευση εγγράφου
Υπεύθυνη Δήλωση
Προβολή
Η ακρίβεια των στοιχείων που υποβάλλονται με αυτή τη δήλωση μπορεί να ελεγχθεί με βάση το αρχείο άλλων υπηρεσιών (άρθρο 8 παρ. 4 Ν. 1599/1986).
Αποδέκτης(1)
Υπουργείο Εργασίας
Κείμενο Δήλωσης
Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις(2), που προβλέπονται από τις διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:
Είμαι ελεύθερος επαγγελματίας.
Στοιχεία Δηλούντος
Όνομα
Επώνυμο
Όνομα και Επώνυμο Πατέρα
Όνομα και Επώνυμο Μητέρας
Ημερομηνία γέννησης
Τόπος Γέννησης
Αριθμός Δελτίου Ταυτότητας
Τηλέφωνο
Τόπος Κατοικίας
Οδός
Αριθμός
Τ.Κ.
ΑΦΜ
[redacted]
Κατάσταση
Το έγγραφο εκδόθηκε
Πρότυπο
YPDIL
Αποθηκεύστε στο αρχείο σας
Αποθηκεύστε το αρχείο PDF στη συσκευή σας.
Αποθήκευση