ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Αρ. Πρωτ: L20-0217-01V1

Προς: Υπουργείο Προστασίας του Πολίτη

Κοιν: Γενική Γραμματεία Έρευνας και Τεχνολογίας
Εταιρεία Ελεύθερου Λογισμικού/Λογισμικού Ανοικτού Κώδικα (ΕΕΛ/ΛΑΚ)
Μέσα Μαζικής Ενημέρωσης
Γραφεία Τύπου πολιτικών κομμάτων

Αθήνα, 17/2/2020

ΘΕΜΑ: **«Νέα προκήρυξη διαγωνιστικής διαδικασίας για την προμήθεια ταυτοτήτων και λοιπών εγγράφων ασφαλείας.»**

Αξιότιμοι κύριοι,

Στις 28/7/2019 η Ένωση Πληροφορικών Ελλάδας (ΕΠΕ) απέστειλε ανοικτή επιστολή προς το Υπουργείο Προστασίας του Πολίτη, σχετικά με την ακύρωση της διαγωνιστικής διαδικασίας για την προμήθεια νέων ηλεκτρονικών ταυτοτήτων[1].

Στην επιστολή επισημαίναμε την επιτακτική ανάγκη σοβαρής μελέτης και ανοικτής διαβούλευσης με τους ειδικούς, κατά κύριο λόγο Πληροφορικούς, ώστε στην επόμενη προκήρυξη να επανασχεδιαστούν οι λειτουργικές και τεχνικές προδιαγραφές του σχεδιαζόμενου πληροφοριακού συστήματος, ώστε αυτό να σχεδιαστεί και να υλοποιηθεί:

1. με βάση τις αρχές των **ανοικτών προτύπων**,
2. με διασφάλιση της **διαλειτουργικότητας** με τα υφιστάμενα ή μελλοντικά πληροφοριακό συστήματα του δημόσιου τομέα,
3. με **έλεγχο των προδιαγραφών** διασφάλισης της πρόσβασης και ασφάλειας των δεδομένων,
4. με μέριμνα για τη **διασφάλιση των δεδομένων προσωπικού χαρακτήρα** των πολιτών, βάσει της εθνικής και ευρωπαϊκής νομοθεσίας.

Η υπόθεση έχει ήδη εκδικαστεί στο Συμβούλιο της Επικρατείας ως προς τη σκοπιμότητα κάποιων από τα τεχνικά χαρακτηριστικά του προτεινόμενου συστήματος, όπως η ενσωμάτωση προσωπικών δεδομένων μη απαραίτητων για την ταυτοποίηση των πολιτών και η ύπαρξη τεχνολογίας ασύρματης μετάδοσης (RFID chip)[2].

Δυστυχώς, βρισκόμαστε για άλλη μια φορά μπροστά σε διαδικασία παρόμοια με την προηγούμενη. Παρατηρούμε τις εξελίξεις επί της νέας διαγωνιστικής διαδικασίας[3] και διαπιστώνουμε ότι οι ίδιες συνθήκες που είχαμε σχολιάσει και τότε επικρατούν και σήμερα. Αντί οι προδιαγραφές να γίνουν πιο διάφανες και δημόσια προσβάσιμες, η νέα προκήρυξη διαγωνισμού γίνεται εντελώς στοχευμένα και

1 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=11832&cHash=bc57aeecc34360f4745d811aa205c0a9

2 https://www.cnn.gr/news/ellada/story/199406/symvoylio-tis-epikrateias-prasino-fos-gia-tis-nees-taytotites

3 http://www.ictplus.gr/default.asp?pid=30&rID=65052&ct=0&la=1

"κλειστά", με ενημέρωση μόνο συγκεκριμένου μικρού συνόλου υποψήφιων εταιριών και με την προσθήκη υποστήριξης λειτουργιών ηλεκτρονικής διακυβέρνησης, έτσι ώστε το έργο να είναι σύμφωνο με την απόφαση του ΣτΕ – αντί οι απαιτούμενες λειτουργίες να καθορίσουν τα δεδομένα και τις τεχνολογίες που είναι απαραίτητα για την υλοποίησή τους[4], όπως διδάσκεται στην Πληροφορική και ειδικότερα στην Τεχνολογία Λογισμικού (Software Engineering) στα Πανεπιστήμια όλου του κόσμου.

Σύμφωνα με τις μέχρι τώρα πληροφορίες, *"...η αναθέτουσα αρχή, το υπουργείο Προστασίας του Πολίτη, απέστειλε σε 26 επιχειρήσεις επιστολές με τις οποίες ζητείται να προσέλθουν να παραλάβουν την προκήρυξη του σχετικού έργου αλλά και να υπογράψουν τις σχετικές συμβάσεις μη αποκάλυψης των σχετικών πληροφοριών της προκήρυξης του έργου..."*[5] Η διαδικασία έναρξης κατάθεσης των προσφορών έχει προγραμματιστεί για τις 3 Μαρτίου, παρότι ήδη εγείρονται νομικές ενστάσεις ως προς τον τρόπο αιτιολόγησης του συγκεκριμένου διαγωνισμού ως "απόρρητου", κάτι που καθορίζει εντελώς διαφορετική διαδικασία σε σχέση με τις κανονικές προμήθειες Δημοσίου[6].

Πιο συγκεκριμένα, με την υπουργική απόφαση 8200/0 – 181623/ΦΕΚ Β 1357/19.4.2019 ορίστηκαν οι προδιαγραφές του νέου δελτίου ταυτότητας και χαρακτηρίστηκαν ως απόρρητες και μη δημοσιοποιήσιμες. Λίγο καιρό αργότερα πληροφορηθήκαμε ότι ματαιώθηκε η διαγωνιστική διαδικασία προμήθειας ταυτοτήτων διότι *"...οι προδιαγραφές του συστήματος, οι οποίες υποτίθεται ότι είναι απόρρητες, ήδη κυκλοφορούσαν στην αγορά"*[7]. Είχαμε σχολιάσει τότε ότι τα πληροφοριακά συστήματα του δημόσιου τομέα θα πρέπει να σχεδιάζονται και να υλοποιούνται με βάση **ανοικτά πρότυπα** (open standards), όπως σε κάθε άλλη σύγχρονη χώρα. Παρόλα αυτά, με την επανέναρξη της διαγωνιστικής διαδικασίας **διαπιστώνουμε ξανά απόρρητες και μη δημοσιοποιήσιμες προδιαγραφές**.

Επί της ουσίας, <u>πουθενά δεν τεκμηριώνεται επιστημονικά ο λόγος που οι προδιαγραφές του εν λόγω συστήματος κρίνονται απόρρητες</u>. Ακόμα και για συστήματα εθνικής άμυνας και κρίσιμων υποδομών, ο απόρρητος χαρακτήρας κάποιων τεχνικών χαρακτηριστικών κρίνεται σκόπιμος μόνο σε πολύ συγκεκριμένες περιπτώσεις. Ένα σύστημα εθνικής ηλεκτρονικής ταυτότητας για τους πολίτες όχι μόνο δεν πρέπει να είναι "κλειστό" σύστημα, αλλά αντίθετα **επιβάλλεται** να βασίζεται σε ανοικτά πρότυπα, τόσο στην ανάπτυξη όσο και στη λειτουργία του.

Ο σχεδιασμός και η υλοποίηση πληροφοριακών συστημάτων και έργων ΤΠΕ (Τεχνολογίες Πληροφορικής & Επικοινωνιών) με βάση τα ανοιχτά πρότυπα εξασφαλίζει -μεταξύ άλλων- τον ενδελεχή έλεγχο των προδιαγραφών και των προτεινόμενων λύσεων, τη διαφάνεια κατά την παραλαβή και την εύρυθμη λειτουργία των έργων αυτών, καθώς καθίσταται εφικτή ο λεπτομερή διαδικασία επικύρωσης (acceptance tests, code audits)[8] από ειδικούς εμπειρογνώμονες που θα παραλάβουν τα τελικά παραδοτέα του έργου, αλλά και σε όλα τα στάδια ανάπτυξής του. Επιπλέον, δίνει τη δυνατότητα αποτελεσματικής επικαιροποίησης, αναβάθμισης και ευχερέστερης μελλοντικής

4 ISO/IEC 25010:2011 [ISO/IEC 25010:2011] Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models.

5 https://www.kathimerini.gr/1057609/article/oikonomia/epixeirhseis/stis-3-martioy-2020-h-ypovolh-prosforwn-gia-tis-nees-taytothtes

6 https://www.kathimerini.gr/1063405/article/oikonomia/ellhnikh-oikonomia/nomiko-keno-proekyye-ston-diagwnismo-gia-tis-nees-taytothtes

7 http://www.ictplus.gr/default.asp?pid=30&rID=62227&ct=0&la=1

8 ISO/IEC/IEEE 29119-1-2013: Software and Systems Engineering – Software Testing – Part 1: Concepts and Definitions (ISO: 2013).

συντήρησής του χωρίς εξαρτήσεις από συγκεκριμένους προμηθευτές, όπως επίσης και τη δυνατότητα διασφάλισης των απαιτούμενων επιπέδων ελέγχου ποιότητας (software quality assurance – SQA) και ασφάλειας της πρόσβασης, βάσει της υφιστάμενης εθνικής και ευρωπαϊκής νομοθεσίας.

Πληροφορούμαστε ότι οι προσδοκίες για το νέο σύστημα ταυτοτήτων είναι υψηλές και ότι η ταυτότητα της **Εσθονίας** επιλέχθηκε ως μοντέλο για τις νέες ελληνικές ψηφιακές ταυτότητες[9]. Αν και θετικό ως βήμα, διαφωνούμε με την επιμονή σε "κλειστά" και ιδιοταγή/εμπορικά (proprietary) πρότυπα, τα οποία δεσμεύουν στο διηνεκές τις σχεδιαστικές και αρχιτεκτονικές προσεγγίσεις του προμηθευτή και δεν επιτρέπουν την εξέταση και τον έλεγχό τους από εμπειρογνώμονες ή ανεξάρτητους αξιολογητές, ενώ μπορεί να διαθέτουν "τρύπες" ασφάλειας[10], να δημιουργούν νόθευση του ανταγωνισμού και να οδηγούν σε συνεχή εξάρτηση από συγκεκριμένο προμηθευτή για την συντήρηση ή την αναβάθμισή τους. Υπενθυμίζουμε τους κινδύνους αυτούς επίσης με το παράδειγμα της Εσθονίας που **αναγκάστηκε να μηνύσει**[11] την ανάδοχο εταιρία των ηλεκτρονικών ταυτοτήτων Gemalto, η οποία **φαίνεται να λαμβάνει μέρος και στον ελληνικό διαγωνισμό**[12], για τα πολυετή κενά ασφάλειας του συστήματος που παρέδωσε.

Τελικά, τα ερωτήματα που τίθενται είναι τα εξής:

1. Ποιος επιθυμεί να προμηθευτεί ένα πληροφοριακό σύστημα που θα διαχειρίζεται τα πιο κρίσιμα προσωπικά δεδομένα των πολιτών, στο οποίο μόνο ο ιδιώτης προμηθευτής θα μπορεί να επέμβει, να ελέγξει, να αναβαθμίζει και να συντηρεί;
2. Πώς διασφαλίζεται ότι έτσι δεν θα επιτραπεί σε ιδιώτη προμηθευτή να έχει πλήρη πρόσβαση στα προσωπικά δεδομένα όλων των πολιτών ή στον τρόπο χρήσης ή επεξεργασίας τους;
3. Εφόσον οι νέες ταυτότητες πρόκειται να ενσωματώνουν και διαδικασίες ηλεκτρονικής διακυβέρνησης, ποια είναι η μελέτη εκτίμησης ρίσκου ως προς την ασφάλεια των πολιτών, όπως για παράδειγμα η "κλοπή ταυτότητας" (identity theft)[13] μέσω κακοτεχνίας ή "τρύπας" ασφάλειας, όπως αυτή που διαπιστώθηκε στην Εσθονία;

Επιπλέον, η πρόφαση ότι λόγω του ότι πρόκειται για κρίσιμο πληροφοριακό σύστημα υποδομής θα πρέπει οι προδιαγραφές του να παραμείνουν μυστικές αποτελεί επιστημονική και τεχνολογική ανακρίβεια που αποκαλύπτει είτε παντελή **άγνοια** του αντικειμένου είτε **σκόπιμο αποκλεισμό** των ειδικών του κλάδου από την κριτική αξιολόγηση των προδιαγραφών του έργου.

9 https://www.tanea.gr/2019/11/22/greece/nees-taytotites-ola-ta-stoixeia-mazi-enas-arithmos-kai-ena-yper-tsip/

10 https://www.efsyn.gr/themata/infowar/231378_i-asfaleia-dedomenon-paei-synnefo

11 https://www.reuters.com/article/estonia-gemalto/estonia-sues-gemalto-for-152-mln-euros-over-id-card-flaws-idUSL8N1WD5JZ

12 https://www.kathimerini.gr/1057609/article/oikonomia/epixeirhseis/stis-3-martioy-2020-h-ypovolh-prosforwn-gia-tis-nees-taytothtes

13 https://en.wikipedia.org/wiki/Identity_theft

Επισημαίνουμε για μια ακόμη φορά το παγκοσμίως αποδεκτό και προφανές:

> (Kerckhoffs's principle, 1883)[14]: *"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."*
>
> (Shannon's maxim, 1949)[15]: *"One ought to design systems under the assumption that the enemy will immediately gain full familiarity with them."*

Με άλλα λόγια: Κανένα σύστημα ασφάλειας, ειδικά σε θέματα κρυπτογράφησης και ψηφιακών υπογραφών, δεν βασίζει την ορθότητα και την αξιοπιστία του στο αν οι αλγόριθμοι και οι υλοποιήσεις του είναι ανοικτά διαθέσιμες ή όχι. Το αντίθετο, έχει αποδειχθεί ότι η ανοικτότητα ενισχύει σημαντικά την αξιοπιστία τους, τον έγκαιρο εντοπισμό αδυναμιών και σφαλμάτων, καθώς και την έγκαιρη ενημέρωση των αρμόδιων φορέων και των πολιτών όταν εντοπιστεί οποιοδήποτε πρόβλημα ασφάλειας. Το γεγονός και μόνο ότι κάποιοι εξακολουθούν να διατυπώνουν τη μη-προσβασιμότητα στις προδιαγραφές ως προϋπόθεση για τη διασφάλιση της αξιοπιστίας του συστήματος αποτελεί **απόδειξη της προχειρότητας** και του νέου αυτού διαγωνισμού, σε ανησυχητικό επίπεδο για το τι ακριβώς θα παραδοθεί και πως θα λειτουργεί τελικά.

Ως επιστημονικός και επαγγελματικός φορέας των Πληροφορικών της χώρας, καλούμε την Πολιτεία:

- να **δημοσιεύσει άμεσα** τις προδιαγραφές του νέου συστήματος,
- να ξεκινήσει **δημόσια διαβούλευση** επί αυτών,
- να ορίσει **ανοικτή διαδικασία ελέγχου και επικύρωσης** του συστήματος που θα παραδοθεί, έτσι ώστε η ακαδημαϊκή κοινότητα και κάθε άλλος ειδικός στον τομέα της ασφάλειας και της προστασίας των προσωπικών δεδομένων να επιβεβαιώσει πως το σύστημα πληρεί τις απαιτήσεις.

Σε διαφορετική περίπτωση είναι σχεδόν βέβαιο ότι το νέο αυτό εγχείρημα θα αποτύχει, όχι μόνο σε επίπεδο λειτουργικότητας αλλά κυρίως με εξαιρετικά μεγάλο ρίσκο για την ασφάλεια του συνόλου των προσωπικών δεδομένων των πολιτών.

Αυτή τη φορά δεν θα πρόκειται απλώς για τη διαρροή των φορολογικών φακέλων 9,5 εκατ. πολιτών[16], όπου το τελικό αποτέλεσμα ήταν απλώς ένα ελάχιστο πρόστιμο προς τον αρμόδιο κρατικό φορέα (Γ.Γ.Π.Σ.) που πληρώθηκε από τους ίδιους τους θιγόμενους πολίτες, αλλά για κάτι πολλαπλάσια σοβαρότερο και επιζήμιο για όλους μας.

14 Kerckhoffs, Auguste (January 1883). "La cryptographie militaire" [Military cryptography]. Journal des sciences militaires [Military Science Journal] (in French). IX: 5–83.

15 Shannon, Claude (4 October 1949). "Communication Theory of Secrecy Systems". Bell System Technical Journal. 28: 662.

16 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=2499&cHash=8328d35d984f6cf2cd66723d41e84a28

Με εκτίμηση,

Το ΔΣ της Ένωσης Πληροφορικών Ελλάδας (ΕΠΕ)

Ο Πρόεδρος	Ο Αντιπρόεδρος	Ο Γενικός Γραμματέας	Ο Ειδικός Γραμματέας	Η Ταμίας
Δημήτρης Κυριακός proedros@epe.org.gr	Μάριος Παπαδόπουλος antiproedros@epe.org.gr	Χάρης Γεωργίου gen_grammateas@epe.org.gr	Φώτης Αλεξάκος eid_grammateas@epe.org.gr	Λένα Καπετανάκη tamias@epe.org.gr

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