ΣΙΑΛΑΡΟΥ & ΣΙΑΛΑΡΟΥ

ΔΙΚΗΓΟΡΟΙ

ΜΕ ΦΑΞ ΚΑΙ ΜΕ EMAIL

ΚΑΤΕΠΕΙΓΟΥΣΑ - ΑΝΟΙΚΤΗ ΕΠΙΣΤΟΛΗ

Προς
Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Κυρία Ειρήνη Λοϊζίδου Νικολαΐδου
Ιάσονος 1, 1082 Λευκωσία
22818456

19/11/2021

Θέμα: CovscanCyprus - Δημιουργία Ηλεκτρονικού Προφίλ Πολιτών

Έντιμη κυρία,

Σε συνέχεια της επιστολής μας ημερομηνίας 08/11/2021 και της απαντητικής σας επιστολής ημερομηνίας 09/11/2021, επανερχόμαστε στο ζήτημα για να σας αναφέρουμε τα ακόλουθα:

Βάσει των όσων μας αναφέρατε, κατά ή περί τις 12/11/2021 αναθέσαμε σε ειδικούς ασφάλειας πληροφοριών εκ της ομάδας εμπειρογνωμόνων "AlarmCall", όπως διερευνήσουν σε προκαταρτικό στάδιο την εφαρμογή Covscan Cyprus η οποία κατ' ισχυρισμό αναπτύχθηκε από το eHealthLab του Πανεπιστημίου Κύπρου[1] για αυτοματοποιημένη πιστοποίηση της κατάστασης εμβολιασμού ή ελέγχου για τηνCovid-19.

Σύμφωνα με τη σχετική σελίδα για το Ευρωπαϊκό Ψηφιακό Πιστοποιητικό COVID του Υπουργείου Υγείας,[2] *το Ευρωπαϊκό Ψηφιακό Πιστοποιητικό COVID είναι η ψηφιακή απόδειξη ότι ένα πρόσωπο είτε έχει εμβολιαστεί κατά της νόσου COVID-19 είτε έχει υποβληθεί σε διαγνωστική εξέταση με αρνητικό αποτέλεσμα είτε έχει αναρρώσει από τη νόσο COVID-19."*

Όπως θα σας επεξηγηθεί κατωτέρω αλλά και όπως θα δείτε στις κατωτέρω προκαταρκτικές αναλύσεις των ειδικών που διερεύνησαν την εφαρμογή Covscan, τίθεται σωρεία ζητημάτων παραβίασης προσωπικών δεδομένων και σε καμία περίπτωση - τουλάχιστον έως ότου διευκρινιστούν τα εν λόγω ζητήματα από το γραφείο σας - δεν πρέπει να επιτραπεί η χρήση της συγκεκριμένης εφαρμογής από οποιοδήποτε άτομο.

---

[1] http://www.ehealthlab.cs.ucy.ac.cy
[2] https://www.eudcc.gov.cy/

Nicolaides Sea View City, Λεωφ. Αρχ. Μακαρίου III 3-7,1ος όροφος, Γραφ.101, 6016, Τ.Θ. 40464, 6304 Λάρνακα
Τηλ: 24656458, 24658468, Φαξ: 24621545, Email: rinaslaw@yahoo.gr

Θεωρούμε συνεπώς την παρέμβασή σας ως άκρως απαραίτητη αφού όπως φαίνεται, στις συνεχείς διαβουλεύσεις του μαζί σας το Υπουργείο Υγείας, δεν σας ανέφερε πως μέχρι στιγμής ουδέποτε είχε γίνει μελέτη DPIA (Data Protection Impact Assessment - Εκτίμηση Αντίκτυπου) καθώς επίσης και το κατά πόσο οποιαδήποτε αρχή DPA (Data Protection Authority) της ΕΕ έχει ελέγξει τις εν λόγω εφαρμογές σε πραγματική εγκατάσταση.

Συμπεραίνεται δε, ότι η Εκτίμηση Αντίκτυπου εναπόκειται στα ίδια τα κράτη μέλη σύμφωνα με την επίσημη ιστοσελίδα της Ε.Ε. αναφορικά με την ηλεκτρονική υγεία, τον Covid 19 και τις διάφορες ηλεκτρονικές εφαρμογές (συμπεριλαμβανομένων και των Ψηφιακών Πιστοποιητικών)[3] κάτι το οποίο δεν φαίνεται να έχει γίνει.

Α. Πρώτη Προκαταρκτική Ανάλυση:

Όπως φαίνεται από τον προκαταρκτικό έλεγχο που διενεργήθηκε (CovScan Cyprus_1.2.4_apkcombo.com.apk):

1. Η εφαρμογή Covscan αποτελεί πρακτικό μέτρο υλοποίησης του άρθρου 14 του 2011/24/EU Κανονισμού της ΕΕ, για δημιουργία ενός εθελοντικού δικτύου ανταλλαγής δεδομένων ηλεκτρονικής υγείας (eHealth) μεταξύ των χωρών μελών της ΕΕ.[4] Ο Κανονισμός βρίσκεται σε ισχύ από τις 9.3.2011, με έναρξη της περιόδου υλοποίησης την 31.01.2020 και λήξης την 31.12.2020.

2. Η εφαρμογή Covscan βασίζεται στις κατευθυντήριες γραμμές ταυτοποίησιμων πιστοποιητικών εμβολιασμού (https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf)και στις τεχνικές προδιαγραφές των Ευρωπαϊκών Ψηφιακών Πιστοποιητικών για Covid.[5][6].

Τα τεχνικά αυτά έγγραφα εκπονήθηκαν μετά από συναντήσεις του Συμβουλίου της Ευρώπης στις 10/11/2020 και 11/12/2020[7] και στα προφορικά συμπεράσματα των συνεδριάσεων του Συμβουλίου την 21/01/2021.[8] Σημειώνεται ότι η αρχική πρόταση για τα λεγόμενα "πράσινα πιστοποιητικά" αφορούσε την πιστοποίηση ατόμων για διασυνοριακά ταξίδια[9] βάσει της σχετικής πρότασης νομοθεσίας COM/2021/130, πλέον Κανονισμός 2021/953.[10][11] Σημειώνεται επίσης ότι σε καμία

---

[3] https://ec.europa.eu/health/ehealth/covid-19_el
[4] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:en:PDF
[5] https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-value-sets_en.pdf
[6] https://github.com/ehn-dcc-development/hcert-spec
[7] https://www.consilium.europa.eu/media/47296/1011-12-20-euco-conclusions-en.pdf
[8] https://www.consilium.europa.eu/en/press/press-releases/2021/01/21/oral-conclusions-by-president-charles-michel-following-the-video-conference-of-the-members-of-the-european-council-on-21-january-2021/pdf
[9] https://github.com/ehn-dcc-development/dgc-business-rules#-digital-covid-certificates-business-rules
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953
[11] https://github.com/eu-digital-green-certificates/dgca-verifier-app-android/pull/206

περίπτωση ο Κανονισμός αυτός δεν είχε ως στόχο την εφαρμογή σε εθνικό επίπεδο, ενόψει της σημαντικά επεμβατικής του φύσης στον πυρήνα ανθρωπίνων δικαιωμάτων.

Σχετικά με το ζήτημα των δικαιωμάτων αυτών, το Συμβούλιο της Ευρώπης, πολλές φορές έχει εκφράσει την απαραίτητη προστασία τους και την αποφυγή χρήσης του πιστοποιητικού για περιορισμό των δικαιωμάτων των πολιτών, με την τελευταία να είναι μόλις τον Μάιο του 2021[12]. Επιπλέον όμως θα πρέπει να σημειωθεί ότι στόχος του Κανονισμού δεν είναι η διάκριση μεταξύ των πολιτών, το οποίο θα συμβαίνει με την εφαρμογή, εφόσον το πιστοποιητικό που έχει κανείς στην κατοχή του είναι διαφορετικού χρώματος, δίνοντας έτσι, εκ νέου, πληροφορίες σχετικά με το ιατρικό ιστορικό του κάθε προσώπου.

3. Η εφαρμογή εσωτερικά φαίνεται να αποκρυπτογραφεί **όλο το μητρώο** του πιστοποιητικού εμβολιασμού/ελέγχου/ανάρρωσης του ατόμου, αν και παρουσιάζονται σαφώς λιγότερα δεδομένα στην οθόνη της συσκευής. Αυτό αφήνει ανοικτό το ενδεχόμενο υποκλοπής των στοιχείων αυτών μέσω της μνήμης της συσκευής, κάτι που πρέπει να εξεταστεί μέσω PenTest (PenetrationTest). Τα σχετικά πεδία που διαβάζει η εφαρμογή φαίνονται στην σελ. 5 του οδηγού τεχνικών προδιαγραφών των Ευρωπαϊκών Ψηφιακών Πιστοποιητικών για Covid.[13]

4. Η εφαρμογή χρησιμοποιεί τις βιβλιοθήκες:

- ανάγνωσης κωδικών QR ZebraCrossing (zxing)[14] η οποία βρίσκεται σε κατάσταση συντήρησης, δηλ. δεν είναι σε ενεργή ανάπτυξη και ενδεχομένως να μην διορθωθούν τυχών προβλήματα ασφαλείας που μπορεί να προκύψουν.

- κρυπτογραφικών λειτουργιών BouncyCastle – βιβλιοθήκη Java που συμπληρώνει την προεπιλεγμένη κρυπτογραφική επέκταση Java (complements the default Java Cryptographic Extension (JCE).[15]

5.Η εφαρμογή είναι βασισμένη σε κώδικα που αναπτύχθηκε από την και/ή είναι ιδιοκτησίας της γερμανικής εταιρείας τηλεπικοινωνιών T-Systems International GmbH και άλλων εταιρειών όπως η DeutscheTelekom AG και η SAP.[16]

6.Η πρακτική χρήση της εφαρμογής και του **όλου οικοσυστήματος των πιστοποιητικών υγείας** της ΕΕ, φαίνεται να έρχεται σε αντιπαράθεση με:

---

[12] https://assembly.coe.int/LifeRay/JUR/Pdf/TextesProvisoires/2021/20210519-CovidCertificates-EN.pdf
[13] https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-value-sets_en.pdf
[14] https://github.com/zxing/zxing
[15] https://bouncycastle.org/
[16] https://github.com/eu-digital-green-certificates/dgca-verifier-app-android#licensing

i. τις συνταγματικές ελευθερίες του πολίτη - η ΕΕ το παραδέχεται σε επικοινωνία της προς το Συμβούλιο της ΕΕ στις 06/12/2012:

> *"2.3 Barriers to deployment of eHealth ...lack of legal clarity for health and wellbeing mobile applications and the lack of transparency regarding the utilisation of data collected by such applications;"(βλ. επίσηςπαράγραφο 4.3).*[17]

ii. τον Γενικό Κανονισμό για την Προστασία των Δεδομένων αφού όπως φαίνεται η ίδια η ομάδα ανάπτυξης της εφαρμογής εξέφρασε τις ανησυχίες της ανοίγοντας σχετικό θέμα για έλεγχο και το οποίο ακόμα παραμένει ανοικτό:[18][19]

Συγκεκριμένα και όπως θα δείτε και στις σχετικές παραπομπές 18 και 19 της παρούσας, στο πρώτο σχόλιο τίθεται η απορία από άτομο της ομάδας ανάπτυξης κατά πόσον έχει γίνει Εκτίμηση Αντίκτυπου και αν οποιαδήποτε αρχή DPA (Data Protection Authority) της ΕΕ έχει ελέγξει σε πραγματική εγκατάσταση.

Παρατίθενται πιο κάτω μερικά από τα σχόλια της ομάδας ανάπτυξης:

> *•######*
>
> *•@on this issue - there are a number of fields that could pose issues under GDPR - **the use of UUIDs, for example, (whether as sha256 representation or otherwise) would be classified as personal data given that they can indirectly be used to identify an individual.***
>
> *•Further to this matter, does @European_Commission/@AnyBody know whether a DPIA has been conducted yet by any appropriate DPA for any deployment?*
>
> *•######*
>
> ***•Have been unable to find an exemplary DPIA for any national member state deployment. Can anybody help?***
>
> *•Deutsche Telekom provided the European Commission with the necessary documents that will be used to create a DPIA template.*
> *We got confirmation from the EC today that these documents have been received and accepted, however this process is now out of our hands and up to the EC to process and forward these to the member states.*

---

[17] https://ec.europa.eu/health/sites/default/files/ehealth/docs/com_2012_736_en.pdf

[18] έχουν ανοίξει και σχετικό θέμα για έλεγχο το ποίο παραμένει ανοικτό (https://github.com/eu-digital-green-certificates/dgc-gateway/issues/107

[19] https://github.com/eu-digital-green-certificates/dgc-overview/issues/37

•@daniel-eder I am unsure why this is closed. so quickly?

The project, repository custodians, and Member States have an obligation to conduct development according to Data-protection-by-design-and-default principles. Each Member State will be legally required to include data protection principles along the development path. This is a requirement within Article 24 and Article 42, and so should have a specific repository in order for Member States to comply.

Do we have sight of when the template will be released to Member States?

•######

7. Τίθενται ζητήματα που χρήζουν περαιτέρω τεχνικού ελέγχου και διευκρινίσεις όπως την πνευματική ιδιοκτησία της εφαρμογής CovScan Cyprus αφού η σελίδα του έργου πάνω στο οποίο είναι βασισμένο το CovScan Cyprus αναφέρει ξεκάθαρα:

> ***"Copyright (C) 2021 T-Systems International GmbH and all other contributors. Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License."***[20]

Η σημείωση πνευματικής ιδιοκτησίας όπως αναφέρεται πιο πάνω **δεν υπάρχει στην εφαρμογή CovScan Cyprus,** άρα ενδεχομένως η εφαρμογή να συγκρούεται με την πολιτική πνευματικής ιδιοκτησίας του Google Play Store.[21] [22]

8. Χρήζει επίσης εξέτασης και της νομιμότητας της χρήσης των πιο κάτω υπηρεσιών:

i) καταγραφής και παρακολούθησης (platform logging and monitoring components) που εντοπίστηκαν στην εφαρμογή:

   a. Micrometer Prometheus application minitoring (micrometer-registry-prometheus)[23]
   b. Java logging & metrics (com.sap.hcp.cf.logging)[24]

ii) Συνδέσεις με βάσεις δεδομένων που παρουσιάζουν **πολλαπλά προβλήματα ασφαλείας** (database connectivity):

---

[20] https://github.com/eu-digital-green-certificates/dgca-verifier-app-android#licensing
[21] https://play.google.com/about/developer-content-policy/

[22] https://support.google.com/googleplay/answer/2853570?hl=en&co=GENIE.Platform=Android

[23] https://mvnrepository.com/artifact/io.micrometer/micrometer-registry-prometheus
[24] https://javadoc.org/artifact/com.sap.hcp.cf.logging

a. MySQL v5.7 – πολλαπλά προβλήματα ασφαλείας (https://www.tenable.com/plugins/nessus/154259)
b. Postgres v9.6 - πολλαπλά προβλήματα ασφαλείας (https://www.debian.org/security/2017/dsa-3936)
c. H2 (Java SQL database)

iii) Συνδέσεις με API (Application Programming Interface) / SDK (Software Development Kit):

a. SAP Cloud SDK v3.43.0 (com.sap.cloud.sdk.cloudplatform - https://developers.sap.com/topics/cloud-sdk.html)

Β. Δεύτερη Προκαταρκτική Ανάλυση:

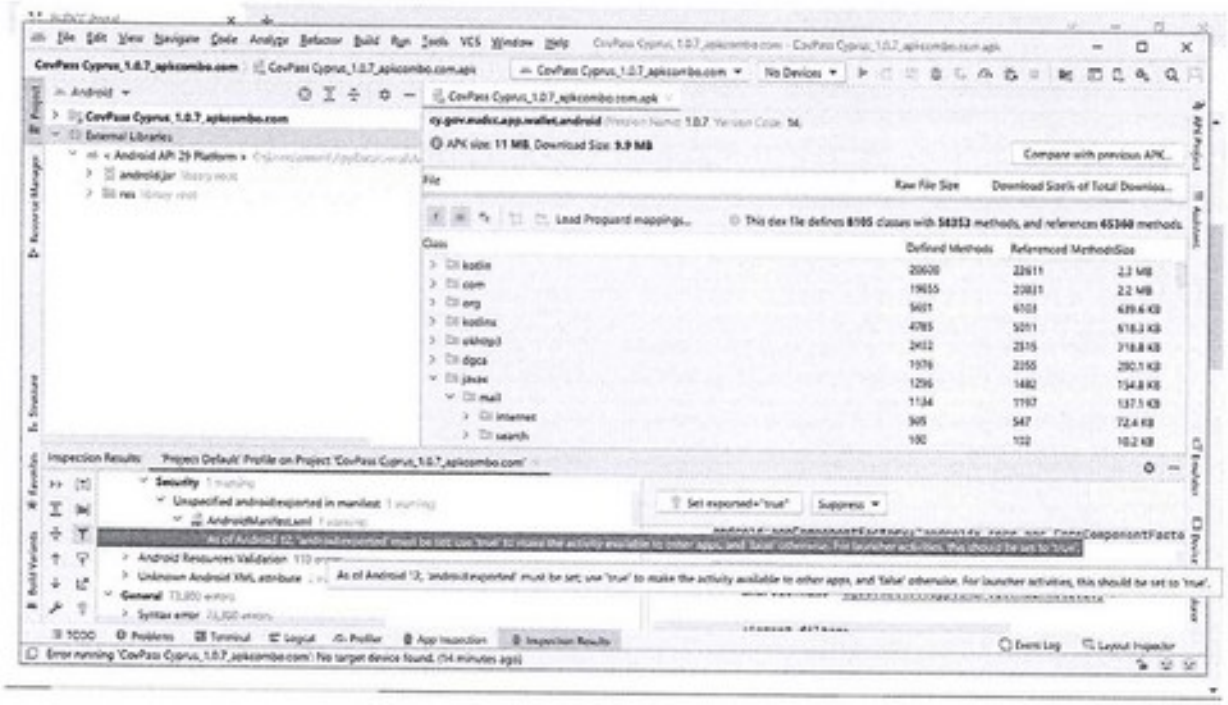
Σύμφωνα με τον δεύτερο προκαταρκτικό έλεγχο που διενεργήθηκε:

1. Τόσο η εφαρμογή Covscan όσο και η εφαρμογή Covpass, δεν έχουν μέχρι στιγμής εγκριθεί από την πλατφόρμα Apple Store, παρά το γεγονός ότι εδώ και μήνες είχαν κατατεθεί για έγκριση εδώ και μήνες. Αυτό οφείλεται στη μη ικανοποίηση των προτύπων και/ή κατευθυντήριων γραμμών που ορίζονται από την Applesχετικά με τον τρόπο διαχείρισης των προσωπικών και/ή ιατρικών δεδομένων από τις συγκεκριμένες εφαρμογές, καταδεικνύοντας έτσι και την έλλειψη δικλείδων ασφαλείας για τους χρήστες.

2. Οι συγκεκριμένες εφαρμογές δεν συμμορφώνονται με τις οδηγίες απορρήτου και ασφάλειας δεδομένων που υποδεικνύονται από τοGoogle (AndroidStore). Συγκεκριμένα το Android 12 ορίζει ότι όλες οι εφαρμογές πρέπει να υποδεικνύουν στον πηγαίο κώδικά τους (source code) εάν το **android:exported** είναι αληθές ή ψευδές για την εφαρμογή. Για σκοπούς ευκολίας ατόμων που δεν έχουν υπόβαθρο προγραμματισμού, έχειζητηθεί από την Googleνα επεξηγήσει τι σημαίνει android:exception και σας παραθέτουμετην απάντησή τους:

> *android:exported: Whether or not the broadcast receiver can receive messages from sources outside its application — "true" if it can, and "false" if not. If "false", the only messages the broadcast receiver can receive are those sent by components of the same application or applications with the same user ID. All developers are requested to set this to true or false as "exported" attribute describes whether or not someone else can be allowed to use your data.*

Μπορείτε να βρείτε πιο κάτω στιγμιότυπο οθόνης του Πηγαίου Κώδικα (Source Code) της εφαρμογής Covpass όπου το android:exception δεν έχει ορισθεί σε true ή false. **Παρακαλώ όπως προσέξετε ιδιαίτερα το επισημασμένο κείμενο με μπλε.**



Τόσο η εφαρμογή Covscanόσο και η εφαρμογή Covpass, παραβιάζουν τις πολιτικές απορρήτου της Apple (iOS) και της Google (Android) που υποδεικνύουν ότι <u>κατά την εκκίνηση της εφαρμογής από τον τελικό χρήστη, θα πρέπει να παρουσιάζεται από την ομάδα ανάπτυξης προειδοποιητικό μήνυμα στον χρήστη ότι ο τελευταίος δίνει την συγκατάθεσή του στην μεταφορά και/ή κοινοποίηση και/ή επεξεργασία των προσωπικών του δεδομένων μεταξύ άλλων εφαρμογών και/ή servers.</u> Το πιο πάνω καθίσταται υποχρεωτικό **αφού στο Source Code και των δύο εφαρμογών το android:exported δεν έχει ορισθεί σε true ή false.**

Λαμβάνοντας υπόψη και τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, είναι εμφανέστατο ότι η ανάγκη για συγκατάθεση από τον χρήστη δεν εξυπηρετείται. Συγκεκριμένα, στο άρθρο 4 του Κανονισμού αναφέρεται ο ορισμός της «συγκατάθεσης» του υποκειμένου επεξεργασίας:

> *«κάθε ένδειξη βουλήσεως, **<u>ελεύθερη</u>**, συγκεκριμένη, ρητή και **<u>εν πλήρει επιγνώσει</u>**, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι **<u>συμφωνεί</u>**, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν»*

Στην παρούσα περίπτωση, τα υποκείμενα του ελέγχου σε καμία περίπτωση δεν έχουν τη δυνατότητα να δώσουν ελεύθερη συγκατάθεση, εφόσον το πιστοποιητικό, είτε στην μέχρι σήμερα μορφή του είτε ως ψηφιακό, απαιτείται ακόμα και για την πρόσβαση σε απαραίτητες για τη διαβίωση υπηρεσίες όπως είναι οι υπεραγορές, για την αγορά τροφίμων. Πώς θα μπορούσε οποιοδήποτε άτομο να δώσει ελεύθερη συγκατάθεση όταν απειλείται η δυνατότητά του να φροντίσει τον εαυτό του και την οικογένειά του; Επιπλέον όμως, εφόσον αυτό αποτελεί προϋπόθεση για την πρόσβαση σε ιατρικές υπηρεσίες, πώς θα μπορούσε οποιοδήποτε άτομο να δώσει ελεύθερη συγκατάθεση όταν απειλείται η υγεία του ιδίου και της οικογένειάς του; Πέραν όμως των ζητημάτων περί προστασίας προσωπικών δεδομένων, εφόσον το θέμα αφορά την προστασία της δημόσιας υγείας, πώς το καθήκον αυτό του Κράτους εκπληρώνεται εάν τίθενται επεμβατικοί περιορισμοί στην πρόσβαση στην υγεία;

Το άρθρο 7(4) του Κανονισμού σχετικά με τις Προϋποθέσεις για Συγκατάθεση, αναφέρει ρητά ότι:

> *"Κατά την εκτίμηση κατά πόσο η συγκατάθεση **δίνεται ελεύθερα**, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που **δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης**".*

Εν προκειμένω, η επεξεργασία των προσωπικών δεδομένων μέσω της εν λόγω εφαρμογής - που όπως έχουμε παραθέσει ανωτέρω σε καμία περίπτωση δεν τηρεί τις απαραίτητες προϋποθέσεις - δεν αποτελεί απαραίτητο μέτρο εφόσον μέχρι σήμερα δεν χρησιμοποιείτο και ο έλεγχος γινόταν επιτυχώς.

Σημαντικό είναι δε να σημειωθεί ότι οι αρχές που διέπουν την επεξεργασία δεδομένων καθορίζουν ρητά ότι τα δεδομένα προσωπικού χαρακτήρα *"υποβάλλονται σε **σύννομη** και **θεμιτή** επεξεργασία με **διαφανή τρόπο** σε σχέση με το υποκείμενο των δεδομένων (νομιμότητα, αντικειμενικότητα και διαφάνεια Άρθρο 5(1)(α))"*[25], κάτι οποίο δεν τηρείται, εκτός αν εσείς και οι υπεύθυνοι προβείτε σε περαιτέρω εξέταση της εφαρμογής ώστε να δοθούν όλα τα απαραίτητα δεδομένα προς τους πολίτες, περιλαμβανομένων και των αρνητικών στοιχείων και κινδύνων.

Στο ίδιο άρθρο στην παράγραφο (γ) αναφέρεται επίσης ότι τα προσωπικά δεδομένα τα οποία λαμβάνονται *«είναι κατάλληλα, **συναφή** και **περιορίζονται στο αναγκαίο για τους σκοπούς** για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»)»*.

Εφόσον λοιπόν μέχρι σήμερα τα προσωπικά δεδομένα των ατόμων, παρότι δε δίνονταν με ελεύθερη συγκατάθεση, δεν καταγράφονταν σε ηλεκτρονική βάση δεδομένων, κάτι το οποίο δούλευε, κατά τα λεγόμενα των Κυβερνόντων, ποια η ανάγκη η οποία για την εφαρμογή του CovScan;

3. Παρά το ότι μας αναφέρετε στην επιστολή σας ημερομηνίας 09/11/2021 ότι τα δεδομένα αποθηκεύονται σε βάση δεδομένων της Ευρωπαϊκής Ένωσης, έχουμε συμπεράνει ότι τα συγκεκριμένα

---

[25] Άρθρο 5(1)(α) του Κανονισμού

δεδομένα αποθηκεύονται, έστω και προσωρινά στο Πανεπιστήμιο Κύπρου (eHealthLab) όντας η ομάδα ανάπτυξης στην Κύπρο. Κατά την δεύτερη προκαταρτική ανάλυση, έχει εξαχθεί το συμπέρασμα ότι τα δεδομένα των Κυπρίων πολιτών αποθηκεύονται σε σχετικά παλαιούς servers στο Πανεπιστήμιο Κύπρου, με υπηρεσίες "Microsoft Azure."Είναι δε γεγονός πως τα τελευταία χρόνια υπήρξε πληθώρα παραβιάσεων σε servers πολύ πιο νέους από τους servers που χρησιμοποιεί το πανεπιστήμιο Κύπρου, και ιδιαίτερα στους servers με υπηρεσίες Microsoft Azure, με την πιο πρόσφατη να έχει γίνει τον Αύγουστο του 2021. [26] [27] [28]

Αρκεί μόνο μια μικρή έρευνα στο διαδίκτυο για να αντιληφθεί κανείς πόσο εύκολα μια κυβερνοεπίθεση (φαινόμενο το οποίο βρίσκεται σε έξαρση τελευταία) μπορεί να εκθέσει τα δεδομένα χιλιάδων πολιτών όπως τα ιατρικά και προσωπικά δεδομένα, αριθμό δελτίου ταυτότητας, φύλο, ημερομηνία γέννησης, ονοματεπώνυμο, τηλέφωνο και ηλεκτρονικά ταχυδρομεία, **πόσο μάλλον, εάν αυτά αποθηκεύονται σε μη ασφαλή συστήματα.**

Γ. Καταληκτικά Σχόλια

Ανεξαρτήτως των ανωτέρω σοβαρότατων ελλείψεων και/ή ανακριβειών σχετικά με τις εφαρμογές Covscan και Covpass, επιθυμούμε όπως σας παραθέσουμε το πιο κάτω χρονοδιάγραμμα ως τροφή για σκέψη:

- Κατά ή περί τον Σεπτέμβριο του 2019 η Ευρωπαϊκή Επιτροπή δημοσιοποίησε έγγραφο με τίτλο*"ROADMAP FOR THE IMPLEMENTATION OF ACTIONS BY THE EUROPEAN COMMISSION BASED ON THE COMMISSION COMMUNICATION AND THE COUNCIL RECOMMENDATION ON STRENGTHENING COOPERATION AGAINST VACCINE PREVENTABLE DISEASES"*. Στο εν λόγω έγγραφο, εξετάζεται κατά πόσο είναι εφικτή η ανάπτυξη μιας κοινής κάρτας εμβολιασμού από το 2019-2021 ("Examine the feasibility of developing a common vaccination card/passport for EU citizens (that takes into account potentially different national vaccination schedules and), that is compatible with **electronic immunisation information systems and recognised for use across borders**, without duplicating work at national level")η οποία από το 2022 και μετέπειτα προτείνεται να πάρει την μορφή διαβατηρίου.[29]

- Στις 30/01/2020 Ο Π.Ο.Υ. ανακηρύσσει παγκόσμια υγειονομική κρίση για τον Covid-19.

- Στις 31/01/2020 αρχίζει η περίοδος υλοποίησης για το δίκτυο eHealth (ψηφιακά πιστοποιητικά υγείας) της ΕΕ.

---

[26] https://www.theverge.com/2021/8/27/22644161/microsoft-azure-database-vulnerabilty-chaosdb
[27] https://www.securitymagazine.com/articles/96098-critical-azure-security-vulnerabilities-affects-large-organizations
[28] https://techbeacon.com/security/huge-us-data-leak-microsoft-cloud-65-households-risk
[29] https://ec.europa.eu/health/sites/default/files/vaccination/docs/2019-2022_roadmap_en.pdf

- Στις 11/03/2020 - Ο Π.Ο.Υ. ανακηρύσσειπαγκόσμια πανδημία για τον CoViD-19.

- Στις11/06/2020 αρχίζει η ανάπτυξη του Digital Covid Certificate Schema[30]

- Στις 31/12/2020 σηματοδοτείται το τέλος της περιόδου υλοποίησης για το δίκτυο eHealth (ψηφιακά πιστοποιητικά υγείας) της ΕΕ.

- Κατά ή περί τον Απρίλιο του 2021 αρχίζει η πρακτική υλοποίηση των πράσινων πιστοποιητικών υγείας της ΕΕ.[31]

- Στις 01/07/2021 - Τα πράσινα πιστοποιητικά υγείας μετονομάζονται σε ψηφιακά πιστοποιητικά Covid (EUDCC – European Union Digital Covid Certificates) και αρχικά θα είχαν ισχύ για ένα χρόνο, (δηλαδήμέχρι τις 01/07/2022), κάτι το οποίο δεν ισχύει πλέον αφού *"...η χρήση του πιστοποιητικού θα επεκταθεί πέραν του καλοκαιριού του 2022."*[32]

Με βάση όλα τα ανωτέρω, παρακαλούμε πολύ όπως επανεξετάσετε άμεσα τα αναπάντητα ερωτήματα και τα πολύ σοβαρά ζητήματα παραβίασης προσωπικών δεδομένων (και όχι μόνο) με τη χρήση τέτοιων πιστοποιητικών, λαμβάνοντας ιδιαίτερα υπόψη το μεγαλεπήβολο οικοσύστημα και τα πρότυπα στα οποία αυτό βασίζεται, τα οποία αφορούν μια "προσωρινή" κατάσταση λεγόμενη "εκτάκτου ανάγκης", (η οποία παρεμπιπτόντως δεν προκηρύχθηκε ποτέ βάσει του άρθρου 183 του Συντάγματος) που δημιουργήθηκε λόγω του ιού SARS-CoV-2, και αναρωτηθείτε κατά πόσο εν τέλει θα υπάρξει πιο πλατύ πεδίο εφαρμογής, αφού όπως φαίνεται είναι πρακτικά απίθανο να έχει καταβληθεί αυτή η τεραστίων διαστάσεων προσπάθεια και επένδυση από την ΕΕ για κάλυψη μιας "προσωρινής" κατάστασης.

Υπερτονίζουμε δε, πως η σωρεία προβλημάτων που σας παρουσιάζουμε ανωτέρω είναι ο λόγος που ζητούμε την παρέμβασή σας για άμεση αναστολή ενεργοποίησης της συγκεκριμένης εφαρμογής, αφού είναι αυτονόητο πως το όποιο "όφελος" από αυτή (επιβεβαίωση γνήσιων πιστοποιητικών), θα είναι δυσανάλογα μικρό από τη ζημιά που θα προκαλέσει από την παραβίαση των προσωπικών δεδομένων εκατοντάδων χιλιάδων πολιτών.

Υπενθυμίζουμε πως το πεδίο εφαρμογής του δικτύου eHealth ήταν η ανταλλαγή των στοιχείων υγείας ενός ασθενή μεταξύ χωρών μελών της ΕΕ και αντίστοιχα των ψηφιακών πιστοποιητικών υγείας για διευκόλυνση των διασυνοριακών ταξιδιών εντός ΕΕ και πως ανέκαθεν υπήρχαν νομικά εμπόδια (legal barriers) στην εφαρμογή οικοσυστημάτων ηλεκτρονικής υγείας, ιδιαίτερα όσο αφορά την

[30]https://github.com/ehn-dcc-development/ehn-dcc-schema#readme)
[31]https://github.com/orgs/ehn-dcc-development/repositories
[32]https://politis.com.cy/politis-news/protasi-komision-taxidia-entos-ee-mono-gia-osoys-echoyn-kanei-tin-3i-dosi/

προστασία των προσωπικών δεδομένων. Πώς αυτό κατέληξε να αποτελεί έλεγχο για είσοδο σε καταστήματα, υπηρεσίες και υποστατικά;

Αναμένοντας την θετική σας απάντηση,

Με εκτίμηση,

Αντρέας Σιάλαρος
Δικηγόρος

Αλέξης Στυλιανού
Δικηγόρος