

II

(Ανακοινώσεις)

ΑΝΑΚΟΙΝΩΣΕΙΣ ΤΩΝ ΘΕΣΜΙΚΩΝ ΚΑΙ ΛΟΙΠΩΝ ΟΡΓΑΝΩΝ ΚΑΙ ΤΩΝ
ΟΡΓΑΝΙΣΜΩΝ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

Έγγραφο καθοδήγησης σχετικά με την προστασία δεδομένων στις εφαρμογές που στηρίζουν την καταπολέμηση της πανδημίας COVID-19

(2020/C 124 I/01)

1 ΠΛΑΙΣΙΟ

Η πανδημία COVID-19 έχει δημιουργήσει μια άνευ προηγουμένου πρόκληση για την Ένωση και τα κράτη μέλη, τα συστήματά τους ιατροφαρμακευτικής περίθαλψης, τον τρόπο ζωής τους, την οικονομική σταθερότητα και τις αξίες τους. Οι ψηφιακές τεχνολογίες και τα δεδομένα θα διαδραματίσουν σημαντικό ρόλο στην καταπολέμηση της κρίσης λόγω της νόσου COVID-19. Οι εφαρμογές για κινητές συσκευές που συνήθως εγκαθίστανται στα έξυπνα τηλέφωνα μπορούν να βοηθήσουν τις αρχές δημόσιας υγείας σε εθνικό και ενωσιακό επίπεδο στην παρακολούθηση και την αναχαίτιση της πανδημίας COVID-19, και έχουν ιδιαίτερη σημασία για το στάδιο άρσης των μέτρων περιορισμού της εξάπλωσης. Μπορούν να παρέχουν άμεση καθοδήγηση στους πολίτες και να στηρίζουν τις προσπάθειες ιχνηλάτησης των επαφών. Σε ορισμένες χώρες, τόσο εντός της ΕΕ όσο και σε παγκόσμιο επίπεδο, οι εθνικές ή οι περιφερειακές αρχές ή οι προγραμματιστές ανακοίνωσαν την κυκλοφορία εφαρμογών με διαφορετικές λειτουργίες που αποσκοπούν στη στήριξη της καταπολέμησης του ιού.

Στις 8 Απριλίου 2020, η Επιτροπή εξέδωσε σύσταση σχετικά με μια κοινή εργαλειοθήκη της Ένωσης για τη χρήση της τεχνολογίας και των δεδομένων με σκοπό την καταπολέμηση της κρίσης COVID-19 και την έξοδο από αυτή, ιδίως όσον αφορά εφαρμογές για φορητές συσκευές και τη χρήση ανωνυμοποιημένων δεδομένων κινητικότητας (στο εξής: σύσταση) ⁽¹⁾. Σκοπός της σύστασης είναι, μεταξύ άλλων, να αναπτυχθεί μια κοινή ευρωπαϊκή προσέγγιση («εργαλειοθήκη») ως προς τη χρήση εφαρμογών για κινητές συσκευές, που θα συντονίζεται σε ενωσιακό επίπεδο, ώστε να παρέχεται η δυνατότητα στους πολίτες να λαμβάνουν αποτελεσματικά μέτρα κοινωνικής αποστασιοποίησης, καθώς και να επιτρέπεται η αποστολή ειδοποιήσεων, η πρόληψη και η ιχνηλάτηση επαφών με σκοπό τη συμβολή στον περιορισμό της εξάπλωσης της νόσου COVID-19. Η σύσταση καθορίζει τις γενικές αρχές που θα πρέπει να διέπουν την ανάπτυξη μιας τέτοιας εργαλειοθήκης και αναφέρει ότι η Επιτροπή θα δημοσιεύσει περαιτέρω κατευθυντήριες γραμμές, μεταξύ άλλων για την προστασία των δεδομένων προσωπικού χαρακτήρα και τις επιπτώσεις στην ιδιωτική ζωή λόγω της χρήσης των εφαρμογών σ' αυτόν τον τομέα.

Με τον κοινό ευρωπαϊκό χάρτη πορείας για την άρση των μέτρων ανάσχεσης της πανδημίας COVID-19, η Επιτροπή, σε συνεργασία με τον Πρόεδρο του Ευρωπαϊκού Συμβουλίου, καθόρισε ορισμένες αρχές με σκοπό την παροχή καθοδήγησης για τη σταδιακή κατάργηση των μέτρων περιορισμού λόγω της πανδημίας COVID-19. Οι εφαρμογές για κινητές συσκευές, συμπεριλαμβανομένων των λειτουργιών ιχνηλάτησης επαφών, μπορούν να διαδραματίσουν σημαντικό ρόλο στο πλαίσιο αυτό. Ανάλογα με τα χαρακτηριστικά των εφαρμογών και τον βαθμό στον οποίο τις χρησιμοποιούν οι πολίτες, οι εφαρμογές μπορούν να έχουν σημαντικό αντίκτυπο στη διάγνωση, τη θεραπεία και τη διαχείριση της νόσου COVID-19 εντός και εκτός του νοσοκομειακού πλαισίου. Είναι ιδιαίτερα σημαντικές κατά το στάδιο άρσης των μέτρων περιορισμού της εξάπλωσης, όταν ο κίνδυνος λοίμωξης αυξάνεται καθώς όλο και περισσότερα άτομα βρίσκονται σε επαφή μεταξύ τους. Οι εν λόγω εφαρμογές μπορούν να συμβάλουν στη διακοπή των αλυσίδων της λοίμωξης ταχύτερα και πιο αποτελεσματικά από ό,τι τα γενικά μέτρα περιορισμού της εξάπλωσης και μπορούν να μειώσουν τον κίνδυνο σημαντικής εξάπλωσης του ιού. Ως εκ τούτου, θα πρέπει να αποτελέσουν σημαντικό στοιχείο της στρατηγικής εξέδου, συμπληρώνοντας άλλα μέτρα, όπως η αύξηση των ικανοτήτων δοκιμών ⁽²⁾. Σημαντική προϋπόθεση για την ανάπτυξη, την αποδοχή και τον ενστερνισμό των εφαρμογών αυτών από τους πολίτες είναι η εμπιστοσύνη. Οι πολίτες πρέπει να είναι βέβαιοι ότι διασφαλίζεται η συμμόρφωση με τα θεμελιώδη δικαιώματα, ότι οι εφαρμογές χρησιμοποιούνται αποκλειστικά για ειδικά καθορισμένους σκοπούς, ότι δεν χρησιμοποιούνται για μαζική παρακολούθηση και ότι οι χρήστες θα

⁽¹⁾ Σύσταση C(2020) 2296 final της 8ης Απριλίου 2020 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

⁽²⁾ https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

διατηρούν τον έλεγχο ως προς τα δεδομένα τους. Αυτό αποτελεί το θεμέλιο της ακρίβειας και της αποτελεσματικότητας των εφαρμογών αυτών όσον αφορά τον περιορισμό της διασποράς του ιού. Ως εκ τούτου, είναι σημαντικό να προσδιοριστούν οι λιγότερο παρεμβατικές λύσεις που συμμορφώνονται πλήρως με τις απαιτήσεις του δικαίου της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής. Επιπλέον, οι εφαρμογές θα πρέπει να απενεργοποιούνται το αργότερο κατά τη στιγμή που η πανδημία θα κηρυχθεί υπό έλεγχο. Επίσης, οι εφαρμογές θα πρέπει να περιλαμβάνουν προστασία αιχμής για την ασφάλεια των πληροφοριών.

Στο παρόν έγγραφο καθοδήγησης λαμβάνεται υπόψη η συνεισφορά του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ) ⁽³⁾ καθώς και συζητήσεις στο πλαίσιο του δικτύου eHealth. Τις προσεχείς ημέρες, το ΕΣΠΔ σκοπεύει να εκδώσει κατευθυντήριες γραμμές σχετικά με τον γεωεντοπισμό και άλλα εργαλεία ιχνηλάτησης στο πλαίσιο της πανδημίας COVID-19.

Πεδίο εφαρμογής του εγγράφου καθοδήγησης

Προκειμένου να διασφαλιστεί συνεκτική προσέγγιση σε ολόκληρη την ΕΕ και να παρασχεθεί καθοδήγηση στα κράτη μέλη και στους προγραμματιστές εφαρμογών, το παρόν έγγραφο καθορίζει τα χαρακτηριστικά των εφαρμογών και τις απαιτήσεις που θα πρέπει να πληρούν ώστε να διασφαλίζεται η συμμόρφωση με τη νομοθεσία της ΕΕ για την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα, ιδίως τον γενικό κανονισμό για την προστασία δεδομένων (ΓΚΠΔ) ⁽⁴⁾ και την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ⁽⁵⁾. Το παρόν έγγραφο καθοδήγησης δεν καλύπτει περαιτέρω προϋποθέσεις, συμπεριλαμβανομένων και περιορισμών, που τα κράτη μέλη ενδέχεται να έχουν συμπεριλάβει στο εθνικό τους δίκαιο όσον αφορά την επεξεργασία δεδομένων που αφορούν την υγεία.

Το παρόν έγγραφο καθοδήγησης δεν έχει νομικά δεσμευτικό χαρακτήρα. Δεν θίγει τον ρόλο του Δικαστηρίου της Ευρωπαϊκής Ένωσης, το οποίο είναι το μόνο θεσμικό όργανο που παρέχει δεσμευτική ερμηνεία του δικαίου της ΕΕ.

Το παρόν έγγραφο καθοδήγησης αφορά μόνο τις οικειοθελείς εφαρμογές που στηρίζουν την καταπολέμηση της πανδημίας COVID-19 (εφαρμογές που καταφορτώνονται, εγκαθίστανται και χρησιμοποιούνται από τους χρήστες οικειοθελώς) οι οποίες έχουν μία ή περισσότερες από τις ακόλουθες λειτουργίες:

- παροχή ακριβούς πληροφόρησης προς τους πολίτες σχετικά με την πανδημία COVID-19·
- παροχή ερωτηματολογίων αυτοεξέτασης και καθοδήγησης προς τους πολίτες (λειτουργία ελέγχου συμπτωμάτων) ⁽⁶⁾·
- αποστολή ειδοποιήσεων προς πρόσωπα που έχουν βρεθεί, για ορισμένο χρονικό διάστημα, κοντά σε άτομο που έχει προσβληθεί από τον ιό, ώστε να τους παρέχονται πληροφορίες ως προς το αν χρειάζεται να αυτοαπομονωθούν και πού μπορούν να κάνουν εξετάσεις (λειτουργία ιχνηλάτησης επαφών και αποστολής ειδοποιήσεων)·
- παροχή φόρουμ επικοινωνίας μεταξύ ασθενών και γιατρών όταν οι ασθενείς βρίσκονται σε αυτοαπομόνωση ή για την περαιτέρω διάγνωση και την παροχή συμβουλών θεραπείας (αυξημένη χρήση της τηλεϊατρικής).

Στο πλαίσιο της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, η επιβολή της χρήσης εφαρμογής που άπτεται των δικαιωμάτων απορρήτου των επικοινωνιών που προβλέπεται στο άρθρο 5 είναι δυνατή μόνο μέσω νόμου που είναι αναγκαίος, κατάλληλος και αναλογικός για την προστασία ορισμένων ειδικών στόχων. Δεδομένου του υψηλού βαθμού παρεμβατικότητας της εν λόγω προσέγγισης και των σχετικών προκλήσεων, μεταξύ άλλων όσον αφορά τη θέσπιση κατάλληλων εγγυήσεων, κατά την άποψη της Επιτροπής απαιτείται προσεκτική ανάλυση πριν από τη χρήση αυτής της δυνατότητας. Γι' αυτούς τους λόγους, η Επιτροπή συνιστά τη χρήση οικειοθελών εφαρμογών.

Το παρόν έγγραφο καθοδήγησης δεν καλύπτει εφαρμογές που αποσκοπούν στην επιβολή απαιτήσεων καραντίνας (συμπεριλαμβανομένων των υποχρεωτικών).

2 ΣΥΜΒΟΛΗ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΣΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΠΑΝΔΗΜΙΑΣ COVID-19

Η λειτουργία ελέγχου συμπτωμάτων είναι χρήσιμο εργαλείο για τις αρχές δημόσιας υγείας ώστε να παρέχουν στους πολίτες οδηγίες σχετικά με τις εξετάσεις για την ανίχνευση της COVID-19 και πληροφορίες σχετικά με την αυτοαπομόνωση, τον τρόπο αποφυγής της μετάδοσης σε άλλους και το πότε πρέπει να αναζητήσουν υγειονομική περίθαλψη. Μπορεί επίσης να συμπληρώνει την επιτήρηση σε επίπεδο πρωτοβάθμιας φροντίδας και να παρέχει στοιχεία ως προς τον ρυθμό μετάδοσης της COVID-19 στον πληθυσμό.

⁽³⁾ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

⁽⁴⁾ Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

⁽⁵⁾ Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

⁽⁶⁾ Αν οι εφαρμογές παρέχουν πληροφορίες σχετικά με τη διάγνωση, την πρόληψη, την παρακολούθηση, την πρόβλεψη ή την πρόγνωση, θα πρέπει να αξιολογείται ο ενδεχόμενος χαρακτηρισμός τους ως ιατροτεχνολογικών προϊόντων σύμφωνα με το κανονιστικό πλαίσιο των ιατροτεχνολογικών προϊόντων. Όσον αφορά το εν λόγω πλαίσιο, βλ. οδηγία 93/42/ΕΟΚ του Συμβουλίου, της 14ης Ιουνίου 1993, περί των ιατροτεχνολογικών προϊόντων (ΕΕ L 169 της 12.7.1993, σ. 1) και κανονισμό (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα ιατροτεχνολογικά προϊόντα (ΕΕ L 117 της 5.5.2017, σ. 1).

Οι λειτουργίες ιχνηλάτησης επαφών και αποστολής ειδοποιήσεων αποτελούν εργαλεία ταυτοποίησης των προσώπων που έχουν έρθει σε επαφή με άτομο που έχει προσβληθεί από τον ιό που προκαλεί την COVID-19 και ενημέρωσής τους για τα κατάλληλα επόμενα βήματα, όπως η αυτοαπομόνωση, η υποβολή τους σε εξετάσεις ή η παροχή συμβουλών για το τι να κάνουν αν εμφανίσουν συμπτώματα. Επομένως, αυτή η λειτουργία είναι χρήσιμη τόσο για τους πολίτες όσο και τις αρχές δημόσιας υγείας. Μπορεί επίσης να διαδραματίσει σημαντικό ρόλο στη διαχείριση των μέτρων περιορισμού της εξάπλωσης στο πλαίσιο σεναρίων αποκλιμάκωσης. Ο αντίκτυπος της μπορεί να ενισχυθεί με μια στρατηγική στήριξης της γενίκευσης των εξετάσεων για τα πρόσωπα που παρουσιάζουν ήπια συμπτώματα.

Και οι δύο λειτουργίες μπορούν επίσης να αποτελέσουν σημαντική πηγή δεδομένων για τις αρχές δημόσιας υγείας και να διευκολύνουν τη διαβίβαση των δεδομένων αυτών στις εθνικές επιδημιολογικές αρχές και στο Ευρωπαϊκό Κέντρο Πρόληψης και Ελέγχου Νόσων (ECDC). Αυτό θα βοηθήσει στην κατανόηση της πορείας μετάδοσης και, σε συνδυασμό με τα αποτελέσματα των δοκιμών, θα επιτρέψει να εκτιμηθεί η θετική προγνωστική αξία των αναπνευστικών συμπτωμάτων σε μια δεδομένη κοινότητα, παρέχοντας πληροφορίες για το επίπεδο κυκλοφορίας του ιού.

Ο βαθμός αξιοπιστίας των εκτιμήσεων συνδέεται άμεσα με τον αριθμό και την αξιοπιστία των διαβιβαζόμενων δεδομένων.

Επομένως, σε συνδυασμό με τις κατάλληλες διαγνωστικές στρατηγικές, τόσο η λειτουργία ελέγχου συμπτωμάτων όσο και η λειτουργία ιχνηλάτησης επαφών μπορούν να παρέχουν πληροφορίες σχετικά με το επίπεδο κυκλοφορίας του ιού και να συμβάλλουν στην αξιολόγηση του αντικτύπου των μέτρων τήρησης φυσικής απόστασης και εγκλεισμού. Όπως ορίζεται στη σύσταση, προκειμένου να καταστεί δυνατή η διασυνοριακή συνεργασία και να εξασφαλιστεί η ανίχνευση των επαφών μεταξύ των χρηστών των διαφόρων εφαρμογών (κάτι που έχει ιδιαίτερη σημασία στο πλαίσιο διασυνοριακών μετακινήσεων των πολιτών) θα πρέπει να διασφαλίζεται η διαλειτουργικότητα μεταξύ των λύσεων ΤΠ των διαφόρων κρατών μελών. Όταν άτομο που έχει προσβληθεί από τον ιό έρθει σε επαφή με χρήστη εφαρμογής άλλου κράτους μέλους, πρέπει να είναι δυνατή η διασυνοριακή διαβίβαση δεδομένων προσωπικού χαρακτήρα του εν λόγω χρήστη στις υγειονομικές αρχές του κράτους μέλους του, στον βαθμό που είναι απολύτως αναγκαίο. Οι σχετικές εργασίες επ' αυτού του θέματος θα διεξαχθούν στο πλαίσιο της εργαλειοθήκης που ανακοινώθηκε με τη σύσταση. Η διαλειτουργικότητα θα πρέπει να εξασφαλίζεται τόσο μέσω τεχνικών απαιτήσεων όσο και μέσω της βελτίωσης της επικοινωνίας και της συνεργασίας μεταξύ των εθνικών υγειονομικών αρχών. Ένα μοντέλο ειδικής συνεργασίας (*) θα μπορούσε επίσης να χρησιμοποιηθεί ως πρότυπο διακυβέρνησης για τις εφαρμογές ιχνηλάτησης επαφών κατά την πανδημία COVID-19.

3 ΣΤΟΙΧΕΙΑ ΓΙΑ ΤΗΝ ΕΜΠΙΣΤΟΣΥΝΗ ΚΑΙ ΤΗ ΛΟΓΟΔΟΣΙΑ ΚΑΤΑ ΤΗ ΧΡΗΣΗ ΤΩΝ ΕΦΑΡΜΟΓΩΝ

Οι λειτουργίες που περιλαμβάνονται στις εφαρμογές μπορούν να έχουν διαφορετικές επιπτώσεις σε ευρύ φάσμα δικαιωμάτων που κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, όπως η ανθρώπινη αξιοπρέπεια, ο σεβασμός της ιδιωτικής και οικογενειακής ζωής, η προστασία των δεδομένων προσωπικού χαρακτήρα, η ελεύθερη κυκλοφορία, η απαγόρευση των διακρίσεων, η επιχειρηματική ελευθερία και η ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι. Η παρέμβαση στην ιδιωτική ζωή και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα μπορεί να είναι ιδιαίτερα σημαντικά, δεδομένου ότι ορισμένες από τις λειτουργίες αυτές βασίζονται σε μοντέλο έντασης δεδομένων.

Τα στοιχεία που παρουσιάζονται κατωτέρω αποσκοπούν στην παροχή καθοδήγησης σχετικά με τον τρόπο περιορισμού του παρεμβατικού χαρακτήρα των λειτουργιών των εφαρμογών, ώστε να διασφαλίζεται η συμμόρφωση με τη νομοθεσία της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής.

3.1 Οι εθνικές υγειονομικές αρχές (ή οι οντότητες που ασκούν καθήκοντα δημοσίου συμφέροντος στον τομέα της υγείας) ως υπεύθυνοι επεξεργασίας

Ο προσδιορισμός του ποιος αποφασίζει σχετικά με τα μέσα και τους σκοπούς της επεξεργασίας των δεδομένων (υπεύθυνος επεξεργασίας δεδομένων) είναι ζωτικής σημασίας για να προσδιοριστεί ο υπεύθυνος για τη συμμόρφωση με τους κανόνες της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα, και ειδικότερα: ποιος θα πρέπει να παρέχει πληροφορίες στα πρόσωπα που καταφορτώνουν την εφαρμογή σχετικά με το τι θα συμβεί με τα δεδομένα τους προσωπικού χαρακτήρα (τα οποία ήδη υπάρχουν ή πρόκειται να δημιουργηθούν μέσω της συσκευής, όπως μέσω του έξυπνου τηλεφώνου στο οποίο είναι εγκατεστημένη η εφαρμογή), ποια θα είναι τα δικαιώματά τους, ποιος θα είναι υπεύθυνος σε περίπτωση παραβίασης δεδομένων, κ.λπ.

Δεδομένου του ευαίσθητου χαρακτήρα των οικείων δεδομένων προσωπικού χαρακτήρα και του σκοπού της επεξεργασίας των δεδομένων που περιγράφεται παρακάτω, η Επιτροπή είναι της άποψης ότι οι εφαρμογές θα πρέπει να σχεδιάζονται κατά τρόπο ώστε οι εθνικές υγειονομικές αρχές (ή οι φορείς που εκτελούν καθήκοντα δημοσίου συμφέροντος στον τομέα της υγείας) να είναι οι υπεύθυνοι επεξεργασίας (*). Οι υπεύθυνοι επεξεργασίας είναι υπεύθυνοι για τη συμμόρφωση με τον ΓΚΠΔ (αρχή της λογοδοσίας). Το εύρος της εν λόγω πρόσβασης θα πρέπει να είναι περιορισμένο βάσει των αρχών που περιγράφονται στο τμήμα 3.5 κατωτέρω.

(*) Η συνεργασία αυτή πραγματοποιείται ήδη όσον αφορά το έργο MyHealth@EU για την ανταλλαγή συνοπτικών ιστορικών υγείας και την ηλεκτρονική συνταγογράφηση. Βλ. επίσης άρθρο 5 παράγραφος 5 και αιτιολογική σκέψη 17 της εκτελεστικής απόφασης 2019/1765 της Επιτροπής.

(*) Βλ. αιτιολογική σκέψη 45 του ΓΚΠΔ.

Αυτό θα συμβάλει επίσης στη μεγαλύτερη εμπιστοσύνη των πολιτών ως προς τις εφαρμογές και, ως εκ τούτου, στην αποδοχή τους (καθώς και των υποκείμενων συστημάτων πληροφοριών για τις αλυσίδες μετάδοσης της λοίμωξης) και θα διασφαλίσει ότι τα συστήματα αυτά πληρούν τον στόχο της προστασίας της δημόσιας υγείας. Οι υποκείμενες πολιτικές, οι απαιτήσεις και οι έλεγχοι θα πρέπει να ευθυγραμμίζονται και να εφαρμόζονται συντονισμένα από τις αρμόδιες εθνικές υγειονομικές αρχές.

3.2 Διασφάλιση ότι το πρόσωπο διατηρεί τον έλεγχο

Ένας καθοριστικός παράγοντας ώστε οι πολίτες να εμπιστεύονται τις εφαρμογές είναι να τους αποδειχθεί ότι οι ίδιοι θα διατηρούν τον έλεγχο των δεδομένων τους προσωπικού χαρακτήρα. Για να διασφαλιστεί αυτό, η Επιτροπή θεωρεί ότι θα πρέπει να πληρούνται, ιδίως, οι ακόλουθες προϋποθέσεις:

- η εγκατάσταση της εφαρμογής στη συσκευή τους θα πρέπει να είναι οικειοθελής και να μην έχει αρνητικές συνέπειες για τον πολίτη που αποφασίζει να μην καταφορτώσει/χρησιμοποιήσει την εφαρμογή·
- οι διάφορες λειτουργίες της εφαρμογής (π.χ. οι λειτουργίες πληροφόρησης, ελέγχου συμπτωμάτων, ιχνηλάτησης επαφών και αποστολής ειδοποιήσεων) δεν θα πρέπει να είναι δεσμοποιημένες, έτσι ώστε ο χρήστης να μπορεί να δίνει τη συγκατάθεσή του ειδικά για την κάθε λειτουργία. Αυτό δεν θα πρέπει να εμποδίζει τον χρήστη από το να συνδυάζει διαφορετικές λειτουργίες της εφαρμογής εάν η επιλογή αυτή προσφέρεται από τον πάροχο·
- αν χρησιμοποιούνται δεδομένα εγγύτητας [δεδομένα που παράγονται από σήματα Bluetooth χαμηλής κατανάλωσης ενέργειας (BLE) μεταξύ συσκευών σε συναφή από επιδημιολογικής άποψης απόσταση και σε συναφή από επιδημιολογικής άποψης χρόνο], θα πρέπει να αποθηκεύονται στη συσκευή του χρήστη. Εάν τα εν λόγω δεδομένα πρόκειται να κοινοποιηθούν στις υγειονομικές αρχές, θα πρέπει να κοινοποιούνται μόνον αφού επιβεβαιωθεί ότι το οικείο πρόσωπο έχει προσβληθεί από την COVID-19 και υπό τον όρο ότι το εν λόγω πρόσωπο το επιλέξει·
- οι υγειονομικές αρχές θα πρέπει να παρέχουν στους χρήστες όλες τις απαραίτητες πληροφορίες που σχετίζονται με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα (σύμφωνα με τα άρθρα 12 και 13 του ΓΚΠΔ και το άρθρο 5 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)·
- ο χρήστης θα πρέπει να μπορεί να ασκεί τα δικαιώματά του βάσει του ΓΚΠΔ (ιδίως τα δικαιώματα πρόσβασης, διόρθωσης και διαγραφής). Κάθε περιορισμός των δικαιωμάτων βάσει του ΓΚΠΔ και της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες θα πρέπει να είναι σύμφωνος με τις εν λόγω πράξεις και να είναι αναγκαίος, αναλογικός και να προβλέπεται στη νομοθεσία·
- οι εφαρμογές θα πρέπει να απενεργοποιούνται το αργότερο κατά τη στιγμή που η πανδημία θα κηρυχθεί υπό έλεγχο· η απενεργοποίηση δεν θα πρέπει να εξαρτάται από την απεγκατάσταση της εφαρμογής από τον χρήστη.

3.3 Νομική βάση για την επεξεργασία

Εγκατάσταση εφαρμογών και αποθήκευση πληροφοριών στη συσκευή του χρήστη

Όπως προαναφέρθηκε, βάσει της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (άρθρο 5), η αποθήκευση πληροφοριών στη συσκευή του χρήστη ή η απόκτηση πρόσβασης σε πληροφορίες που έχουν ήδη αποθηκευτεί σ' αυτήν επιτρέπεται μόνο εάν i) ο χρήστης έχει δώσει τη συγκατάθεσή του ή ii) η αποθήκευση και/ή η πρόσβαση είναι απολύτως απαραίτητες για την υπηρεσία της κοινωνίας της πληροφορίας (π.χ. την εφαρμογή) που έχει ζητηθεί ρητά (δηλαδή έχει εγκατασταθεί και ενεργοποιηθεί) από τον χρήστη.

Η αποθήκευση πληροφοριών στη συσκευή του χρήστη και η απόκτηση πρόσβασης σε πληροφορίες που είναι ήδη αποθηκευμένες στην εν λόγω συσκευή είναι συνήθως απαραίτητες για τη λειτουργία των εφαρμογών. Επιπλέον, η λειτουργία ιχνηλάτησης επαφών και αποστολής ειδοποιήσεων απαιτεί να αποθηκεύονται στη συσκευή του χρήστη και ορισμένες άλλες πληροφορίες (όπως τα προσωρινά αναγνωριστικά χρήστη που αλλάζουν σε περιοδική βάση και που χρησιμοποιούνται από τους χρήστες της εν λόγω λειτουργίας που βρίσκονται σε μικρή απόσταση). Επιπλέον, η εν λόγω λειτουργία ενδέχεται να απαιτεί από τον χρήστη (που έχει προσβληθεί ή ενδέχεται να έχει προσβληθεί από τον ιό) να αναφορτώνει δεδομένα εγγύτητας. Η εν λόγω αναφόρτωση δεν είναι απαραίτητη για τη λειτουργία της εφαρμογής αυτής καθαυτής. Επομένως, δεν πληρούνται οι προϋποθέσεις της επιλογής ii) που αναφέρεται στην προηγούμενη παράγραφο. Ως εκ τούτου, η συγκατάθεση [επιλογή i) ανωτέρω] αποτελεί την πλέον κατάλληλη βάση για τις σχετικές δραστηριότητες. Η εν λόγω συγκατάθεση θα πρέπει να είναι «ελεύθερη», «συγκεκριμένη», «ρητή» και «εν πλήρη επιγνώσει» κατά την έννοια του ΓΚΠΔ. Θα πρέπει να εκφράζεται με σαφή θετική ενέργεια του προσώπου· αυτό αποκλείει σιωπηρές μορφές συγκατάθεσης (π.χ. σιωπή· αδράνεια) (*).

(*) Βλ. τις κατευθυντήριες γραμμές του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τη συγκατάθεση:
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Νομική βάση για την επεξεργασία από τις εθνικές υγειονομικές αρχές — δίκαιο της Ένωσης ή των κρατών μελών

Κατά κανόνα, οι εθνικές υγειονομικές αρχές προβαίνουν σε επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν υπάρχει νομική υποχρέωση που προβλέπεται στο δίκαιο της ΕΕ ή του κράτους μέλους η οποία επιτάσσει την εν λόγω επεξεργασία και εφόσον πληρούνται τις προϋποθέσεις του άρθρου 6 παράγραφος 1 στοιχείο γ) και του άρθρου 9 παράγραφος 2 στοιχείο θ) του ΓΚΠΔ ή όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον που αναγνωρίζεται από το δίκαιο της ΕΕ ή κράτους μέλους ⁽¹⁰⁾.

Το εθνικό δίκαιο πρέπει να προβλέπει ειδικά και κατάλληλα μέτρα ώστε να διασφαλίζονται τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων. Κατά γενικό κανόνα, όσο μεγαλύτερος είναι ο αντίκτυπος στις ελευθερίες των προσώπων, τόσο ισχυρότερες θα πρέπει να είναι οι αντίστοιχες εγγυήσεις που προβλέπονται στη σχετική νομοθεσία.

Οι νόμοι της ΕΕ και των κρατών μελών που προϋπήρχαν της πανδημίας COVID-19 και οι νόμοι τους οποίους θεσπίζουν ειδικά τα κράτη μέλη για την καταπολέμηση της εξάπλωσης επιδημιών μπορούν, καταρχήν, να χρησιμοποιούνται ως νομική βάση για την επεξεργασία των δεδομένων των προσώπων, εφόσον προβλέπουν μέτρα για την παρακολούθηση των επιδημιών και εφόσον ο οικείος νόμος πληροί τις περαιτέρω απαιτήσεις που ορίζονται στο άρθρο 6 παράγραφος 3 του ΓΚΠΔ.

Δεδομένης της φύσης των οικείων δεδομένων προσωπικού χαρακτήρα (ιδίως των δεδομένων υγείας ως ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα), καθώς και των συνθηκών της τρέχουσας πανδημίας COVID-19, η επίκληση του νόμου ως νομικής βάσης θα συμβάλει στην ασφάλεια δικαίου, δεδομένου ότι i) θα καθορίζει λεπτομερώς την επεξεργασία συγκεκριμένων δεδομένων υγείας και θα ορίζει σαφώς τους σκοπούς της επεξεργασίας· ii) θα προσδιορίζει με σαφήνεια ποιος είναι ο υπεύθυνος επεξεργασίας, δηλαδή η οντότητα που επεξεργάζεται τα δεδομένα, καθώς και ποιος μπορεί να έχει πρόσβαση στα εν λόγω δεδομένα, εκτός από τον υπεύθυνο επεξεργασίας· iii) θα αποκλείει τη δυνατότητα επεξεργασίας των εν λόγω δεδομένων για σκοπούς άλλους από εκείνους που παρατίθενται στη νομοθεσία και iv) θα προβλέπει ειδικές εγγυήσεις. Για να μην υπονομευθεί η χρησιμότητα και η αποδοχή των εφαρμογών από το κοινό, ο εθνικός νομοθέτης θα πρέπει να δώσει ιδιαίτερη προσοχή στη λύση που θα επιλεγεί ώστε να είναι όσο το δυνατόν πιο συμπεριληπτική ως προς τους πολίτες.

Η επεξεργασία από τις υγειονομικές αρχές βάσει της νομοθεσίας δεν αλλάζει το γεγονός ότι οι πολίτες εξακολουθούν να μπορούν να επιλέξουν ελεύθερα αν θα εγκαταστήσουν την εφαρμογή ή όχι και αν θα κοινοποιήσουν τα δεδομένα τους στις υγειονομικές αρχές. Συνεπώς, δεν θα πρέπει να υπάρχουν αρνητικές συνέπειες για τους χρήστες όταν η εφαρμογή απεγκαθίσταται.

Οι εφαρμογές ιχνιλάτησης επαφών και αποστολής ειδοποιήσεων προβλέπουν την ειδοποίηση των προσώπων. Όταν η εν λόγω ειδοποίηση παρέχεται απευθείας από την εφαρμογή, η Επιτροπή εφιστά την προσοχή στην απαγόρευση υπαγωγής των φυσικών προσώπων σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, η οποία παράγει έννομα αποτελέσματα που τα αφορούν ή τα επηρεάζει σημαντικά με παρόμοιο τρόπο (άρθρο 22 του ΓΚΠΔ).

3.4 Ελαχιστοποίηση δεδομένων

Τα δεδομένα που παράγονται μέσω συσκευών και έχουν ήδη προηγουμένως αποθηκευτεί στις εν λόγω συσκευές προστατεύονται ως εξής:

- Ως «δεδομένα προσωπικού χαρακτήρα», δηλαδή κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (άρθρο 4 παράγραφος 1 του ΓΚΠΔ), προστατεύονται δυνάμει του ΓΚΠΔ. Τα δεδομένα που αφορούν την υγεία απολαύουν πρόσθετης προστασίας (άρθρο 9 του ΓΚΠΔ).
- Ως «δεδομένα θέσης», δηλαδή δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη, προστατεύονται βάσει της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (άρθρο 5 παράγραφος 1, άρθρα 6 και 9) ⁽¹¹⁾.
- Κάθε πληροφορία που είναι αποθηκευμένη στον τερματικό εξοπλισμό του χρήστη και προσβάσιμη απ' αυτόν προστατεύεται βάσει του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Τα δεδομένα μη προσωπικού χαρακτήρα (όπως τα αμετακλήτως ανωνυμοποιημένα δεδομένα) δεν προστατεύονται δυνάμει του ΓΚΠΔ.

Η Επιτροπή υπενθυμίζει ότι η αρχή της ελαχιστοποίησης των δεδομένων απαιτεί να υποβάλλονται σε επεξεργασία μόνο δεδομένα προσωπικού χαρακτήρα επαρκή, συναφή και περιορισμένα στο μέτρο του αναγκαίου σε σχέση με τον σκοπό της επεξεργασίας ⁽¹²⁾. Η εκτίμηση της αναγκαιότητας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και της συνάφειας των εν λόγω δεδομένων προσωπικού χαρακτήρα θα πρέπει να διενεργείται με γνώμονα τον επιδιωκόμενο σκοπό ή σκοπούς.

Η Επιτροπή επισημαίνει, για παράδειγμα, ότι εάν σκοπός της λειτουργίας είναι ο έλεγχος συμπτωμάτων ή η τηλεϊατρική, οι εν λόγω σκοποί δεν απαιτούν πρόσβαση στον κατάλογο επαφών του ατόμου που κατέχει τη συσκευή.

⁽¹⁰⁾ Άρθρο 6 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ.

⁽¹¹⁾ Ο Κώδικας Ηλεκτρονικών Επικοινωνιών προβλέπει ότι καλύπτονται επίσης οι υπηρεσίες που είναι λειτουργικά ισοδύναμες με τις υπηρεσίες ηλεκτρονικών επικοινωνιών.

⁽¹²⁾ Αρχή της ελαχιστοποίησης των δεδομένων.

Η παραγωγή και επεξεργασία λιγότερων δεδομένων περιορίζει τους κινδύνους για την ασφάλεια. Ως εκ τούτου, η συμμόρφωση με τα μέτρα ελαχιστοποίησης των δεδομένων παρέχει επίσης εγγυήσεις για την ασφάλεια.

— Λειτουργία πληροφόρησης:

Μια εφαρμογή με μόνη την εν λόγω λειτουργία δεν χρειάζεται να επεξεργάζεται δεδομένα που αφορούν την υγεία των χρηστών. Απλώς θα τους παρέχει πληροφορίες. Για την εκπλήρωση του σκοπού αυτού, δεν είναι δυνατή η επεξεργασία άλλων πληροφοριών που είναι αποθηκευμένες στον τερματικό εξοπλισμό και προσβάσιμες απ' αυτόν, πέρα από εκείνες που είναι απαραίτητες για την παροχή των εν λόγω πληροφοριών.

— Λειτουργίες ελέγχου συμπτωμάτων και τηλεϊατρικής:

Εάν η εφαρμογή περιλαμβάνει μία ή δύο απ' αυτές τις λειτουργίες, θα επεξεργάζεται δεδομένα προσωπικού χαρακτήρα που αφορούν την υγεία. Ως εκ τούτου, στην υποκείμενη νομοθεσία που εφαρμόζεται για τις υγειονομικές αρχές θα πρέπει να καθορίζεται κατάλογος των δεδομένων που μπορούν να υποβάλλονται σε επεξεργασία.

Επιπλέον, οι υγειονομικές αρχές ενδέχεται να χρειάζονται τους αριθμούς τηλεφώνου των ατόμων που χρησιμοποίησαν τη λειτουργία ελέγχου συμπτωμάτων και αναφόρτωσαν τα αποτελέσματα. Οι πληροφορίες που αποθηκεύονται στον τερματικό εξοπλισμό και είναι προσβάσιμες απ' αυτόν μπορούν να υποβάλλονται σε επεξεργασία μόνο στον βαθμό που είναι αναγκαίο για την εκπλήρωση του σκοπού που εξυπηρετεί η εφαρμογή και για τη λειτουργία της.

— Λειτουργία ιχνηλάτησης επαφών και αποστολής ειδοποιήσεων:

Η νόσος COVID-19 μεταδίδεται στην πλειονότητα των περιπτώσεων μέσω σταγονιδίων που διανύουν μόνο περιορισμένη απόσταση. Ο εντοπισμός, το ταχύτερο δυνατόν, των ατόμων που βρέθηκαν κοντά σε άτομο που έχει προσβληθεί από τον ιό αποτελεί βασικό παράγοντα για τη διακοπή της αλυσίδας των λοιμώξεων. Ο προσδιορισμός της εγγύτητας αποτελεί συνάρτηση της απόστασης και της διάρκειας της επαφής και θα πρέπει να πραγματοποιείται από επιδημιολογική άποψη. Η διακοπή της αλυσίδας των λοιμώξεων είναι ιδιαίτερα σημαντική για την αποφυγή της επανεμφάνισης λοιμώξεων κατά το στάδιο της εξόδου από την κρίση.

Τα δεδομένα εγγύτητας θα μπορούσαν να είναι απαραίτητα για τον σκοπό αυτό. Για τη μέτρηση της εγγύτητας και των στενών επαφών, οι επικοινωνίες μέσω Bluetooth χαμηλής κατανάλωσης ενέργειας (BLE) μεταξύ συσκευών φαίνονται ακριβέστερες και, ως εκ τούτου, πιο κατάλληλες από τη χρήση δεδομένων γεωεντοπισμού (δεδομένα GNSS/GPS ή κυψελοειδή δεδομένα θέσης). Το BLE αποφεύγει τη δυνατότητα παρακολούθησης (σε αντίθεση με τα δεδομένα γεωεντοπισμού). Ως εκ τούτου, η Επιτροπή συνιστά τη χρήση των δεδομένων επικοινωνίας μέσω BLE (ή δεδομένων που παράγονται από ισοδύναμη τεχνολογία) για τον προσδιορισμό της εγγύτητας.

Τα δεδομένα θέσης δεν είναι απαραίτητα για τους σκοπούς των λειτουργιών ιχνηλάτησης επαφών, καθώς στόχος των τελευταίων δεν είναι να παρακολουθούν τις κινήσεις των ατόμων ή να επιβάλλουν εντολές. Επιπλέον, η επεξεργασία δεδομένων θέσης στο πλαίσιο της ιχνηλάτησης επαφών θα ήταν δύσκολο να δικαιολογηθεί με βάση την αρχή της ελαχιστοποίησης των δεδομένων και μπορεί να δημιουργήσει ζητήματα ασφάλειας και προστασίας της ιδιωτικής ζωής. Για τον λόγο αυτόν, η Επιτροπή συνιστά να μην χρησιμοποιούνται τα δεδομένα θέσης σε αυτό το πλαίσιο.

Ανεξάρτητα από τα τεχνικά μέσα που χρησιμοποιούνται για τον προσδιορισμό της εγγύτητας, δεν φαίνεται αναγκαίο να αποθηκεύεται ο ακριβής χρόνος της επαφής ή ο τόπος (εάν είναι διαθέσιμος). Ωστόσο, μπορεί να είναι χρήσιμο να αποθηκεύεται η ημέρα της επαφής, για να καθίσταται γνωστό αν η επαφή πραγματοποιήθηκε όταν το άτομο είχε αναπτύξει συμπτώματα (ή 48 ώρες πριν⁽¹³⁾) και να προσαρμόζεται το περιεχόμενο του επακόλουθου μηνύματος με συμβουλές π.χ. σχετικά με τη διάρκεια της αυτοαπομόνωσης.

Τα δεδομένα εγγύτητας θα πρέπει να παράγονται και να υποβάλλονται σε επεξεργασία μόνον εάν υπάρχει πραγματικός κίνδυνος λοίμωξης (ανάλογα με την εγγύτητα και τη διάρκεια της επαφής).

Θα πρέπει να σημειωθεί ότι η αναγκαιότητα και η αναλογικότητα της συλλογής δεδομένων θα εξαρτάται, συνεπώς, από παράγοντες όπως ο βαθμός στον οποίο είναι διαθέσιμες εγκαταστάσεις δοκιμών, ιδίως όταν έχουν ήδη επιβληθεί μέτρα όπως ο εγκλεισμός. Η προειδοποίηση των ατόμων που έχουν έρθει σε στενή επαφή με άτομο που έχει προσβληθεί από τον ιό μπορεί να γίνει με δύο τρόπους:

Σύμφωνα με την πρώτη προσέγγιση, παραδίδεται αυτόματα ειδοποίηση μέσω της εφαρμογής στις στενές επαφές όταν ένας χρήστης ενημερώνει την εφαρμογή —με την έγκριση ή την επιβεβαίωση της υγειονομικής αρχής, για παράδειγμα μέσω κωδικού QR ή TAN— ότι βρέθηκε θετικός (αποκεντρωμένη επεξεργασία). Το περιεχόμενο του μηνύματος ειδοποίησης θα πρέπει, κατά προτίμηση, να καθορίζεται από την υγειονομική αρχή. Σύμφωνα με τη δεύτερη προσέγγιση, τα τυχαία προσωρινά αναγνωριστικά αποθηκεύονται σε διακομιστή backend της υγειονομικής αρχής (λύση του διακομιστή backend). Οι χρήστες δεν μπορούν να ταυτοποιηθούν άμεσα μέσω των εν λόγω δεδομένων. Μέσω των αναγνωριστικών, οι χρήστες που έχουν έρθει σε στενή επαφή με χρήστη που έχει βρεθεί θετικός, λαμβάνουν ειδοποίηση στη συσκευή τους. Εάν οι υγειονομικές αρχές επιθυμούν να επικοινωνήσουν με τους χρήστες που έχουν έρθει σε στενή επαφή με άτομο που έχει προσβληθεί από τον ιό και μέσω τηλεφώνου ή SMS, χρειάζονται τη συγκατάθεση των εν λόγω χρηστών για την παροχή των αριθμών τηλεφώνου τους.

⁽¹³⁾ Το άτομο που έχει προσβληθεί από τον ιό μπορεί να τον μεταδώσει 48 ώρες πριν από την εκδήλωση συμπτωμάτων.

3.5 Περιορισμός της κοινολόγησης δεδομένων / πρόσβασης σε δεδομένα

— Λειτουργία πληροφόρησης:

Καμία πληροφορία που αποθηκεύεται σε τερματικό εξοπλισμό και είναι προσβάσιμη απ' αυτόν δεν μπορεί να κοινοποιηθεί στις υγειονομικές αρχές, πέραν των αναγκαίων για τη λειτουργία πληροφόρησης. Δεδομένου ότι η λειτουργία αυτή παρέχει μόνο τα μέσα επικοινωνίας, οι υγειονομικές αρχές δεν θα έχουν πρόσβαση σε άλλα δεδομένα.

— Λειτουργίες ελέγχου συμπτωμάτων και τηλεϊατρικής:

Η λειτουργία ελέγχου συμπτωμάτων μπορεί να είναι χρήσιμη για τα κράτη μέλη ώστε να καθοδηγούν τους πολίτες σχετικά με το κατά πόσον θα πρέπει να υποβληθούν σε εξετάσεις, να παρέχουν πληροφορίες σχετικά με την απομόνωση και τον χρόνο και τον τρόπο πρόσβασης στην υγειονομική περίθαλψη, ιδίως για τις ομάδες υψηλού κινδύνου. Η λειτουργία αυτή μπορεί επίσης να συμπληρώνει την επιτήρηση της πρωτοβάθμιας υγειονομικής περίθαλψης και να συμβάλει στην κατανόηση των ποσοστών λοίμωξης του πληθυσμού με τη νόσο COVID-19. Ως εκ τούτου, μπορεί να αποφασιστεί ότι οι αρμόδιες υγειονομικές αρχές και εθνικές επιδημιολογικές αρχές θα πρέπει να έχουν πρόσβαση στις πληροφορίες που παρέχονται από τον ασθενή. Το Ευρωπαϊκό Κέντρο Πρόληψης και Ελέγχου Νόσων (ECDC) θα μπορούσε να λαμβάνει συγκεντρωτικά δεδομένα από τις εθνικές αρχές για επιδημιολογική επιτήρηση.

Εάν επιλεγεί η επικοινωνία με υπαλλήλους του τομέα της υγείας και όχι μόνο μέσω της ίδιας της εφαρμογής, τότε είναι επίσης αναγκαία η γνωστοποίηση στις εθνικές υγειονομικές αρχές του αριθμού τηλεφώνου των χρηστών της εφαρμογής.

— Λειτουργία ιχνηλάτησης επαφών και αποστολής ειδοποιήσεων:

— Δεδομένα του ατόμου που έχει προσβληθεί από τον ιό

Οι εφαρμογές παράγουν ψευδοτυχαία, προσωρινά και περιοδικά μεταβαλλόμενα αναγνωριστικά των τηλεφώνων που έρχονται σε επαφή με τον χρήστη. Μια επιλογή είναι η αποθήκευση των αναγνωριστικών στη συσκευή του χρήστη (η λεγόμενη αποκεντρωμένη επεξεργασία). Μια άλλη επιλογή μπορεί να προβλέπει ότι τα εν λόγω αυθαίρετα αναγνωριστικά αποθηκεύονται στον διακομιστή στον οποίο έχουν πρόσβαση οι υγειονομικές αρχές (η λεγόμενη λύση του διακομιστή backend). Η αποκεντρωμένη λύση συνάδει περισσότερο με την αρχή της ελαχιστοποίησης. Οι υγειονομικές αρχές θα πρέπει να έχουν πρόσβαση μόνο στα δεδομένα εγγύτητας από τις συσκευές ατόμων που έχουν προσβληθεί από τον ιό, ώστε να μπορούν να έρθουν σε επαφή με άτομα που διατρέχουν κίνδυνο προσβολής από τον ιό.

Τα εν λόγω δεδομένα θα είναι διαθέσιμα στις υγειονομικές αρχές μόνον αφού το άτομο που έχει προσβληθεί από τον ιό (μετά την υποβολή του σε εξετάσεις) μοιραστεί προδραστικά τα εν λόγω δεδομένα με αυτές.

Το άτομο που έχει προσβληθεί από τον ιό δεν θα πρέπει να ενημερώνεται για την ταυτότητα των ατόμων με τα οποία ήρθε σε ενδεχομένως επιδημιολογικά σημαντική επαφή και τα οποία θα ειδοποιηθούν.

— Δεδομένα των ατόμων που ήρθαν σε (επιδημιολογική) επαφή με το άτομο που έχει προσβληθεί από τον ιό

Η ταυτότητα του ατόμου που έχει προσβληθεί από τον ιό δεν θα πρέπει να αποκαλύπτεται στα άτομα με τα οποία έχει έρθει σε επιδημιολογική επαφή. Αρκεί να τους γνωστοποιείται το γεγονός ότι, κατά τις τελευταίες 16 ημέρες, ήρθαν σε επιδημιολογική επαφή με άτομο που έχει προσβληθεί από τον ιό. Όπως προαναφέρθηκε, δεν θα πρέπει να αποθηκεύονται δεδομένα σχετικά με τον χρόνο και τον τόπο των εν λόγω επαφών. Συνεπώς, δεν είναι ούτε αναγκαία ούτε δυνατή η κοινοποίηση των εν λόγω δεδομένων.

Για τον εντοπισμό των επιδημιολογικών επαφών χρήστη ηλεκτρονικής εφαρμογής που διαπιστώνεται ότι έχει προσβληθεί από τον ιό, οι εθνικές υγειονομικές αρχές θα πρέπει να ενημερώνονται μόνο για το αναγνωριστικό του ατόμου με το οποίο το άτομο που έχει προσβληθεί από τον ιό ήρθε σε επιδημιολογική επαφή εντός του χρονικού διαστήματος που άρχεται 48 ώρες πριν από την εκδήλωση των συμπτωμάτων και λήγει 14 ημέρες μετά την εκδήλωση των συμπτωμάτων, με βάση την εγγύτητα και τη διάρκεια της επαφής.

Το ECDC θα μπορούσε να λαμβάνει συγκεντρωτικά δεδομένα ιχνηλάτησης επαφών από τις εθνικές αρχές με σκοπό την επιδημιολογική επιτήρηση βάσει δεικτών που καθορίζονται σε συνεργασία με τα κράτη μέλη.

3.6 Πρόβλεψη συγκεκριμένων σκοπών της επεξεργασίας

Η νομική βάση (η νομοθεσία της Ένωσης ή κράτους μέλους) θα πρέπει να προβλέπει τον σκοπό της επεξεργασίας. Ο σκοπός θα πρέπει να είναι συγκεκριμένος, ώστε να μην υπάρχει αμφιβολία ως προς το είδος των δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητο να υποβληθούν σε επεξεργασία προκειμένου να επιτευχθεί ο επιδιωκόμενος στόχος, και ρητός.

Ο ακριβής σκοπός ή σκοποί θα εξαρτάται από τις λειτουργίες της εφαρμογής. Μπορεί να υπάρχουν αρκετοί σκοποί για κάθε λειτουργία μιας εφαρμογής. Προκειμένου να παρέχεται στους χρήστες πλήρης έλεγχος επί των δεδομένων τους, η Επιτροπή συνιστά να μην δεσμοποιούνται διαφορετικές λειτουργίες. Σε κάθε περίπτωση, ο χρήστης θα πρέπει να έχει τη δυνατότητα επιλογής μεταξύ διαφορετικών λειτουργιών, καθεμία από τις οποίες επιδιώκει ξεχωριστό σκοπό.

Η Επιτροπή συνιστά να μην χρησιμοποιούνται τα δεδομένα που συλλέγονται υπό τις ανωτέρω συνθήκες για άλλους σκοπούς πέραν της καταπολέμησης της νόσου COVID-19. Εάν κρίνονται αναγκαίοι σκοποί όπως η επιστημονική έρευνα και οι στατιστικές, θα πρέπει να περιλαμβάνονται στον αρχικό κατάλογο σκοπών και να κοινοποιούνται με σαφήνεια στους χρήστες.

— Λειτουργία πληροφόρησης:

Σκοπός αυτής της λειτουργίας είναι η παροχή των πληροφοριών που κρίνονται σημαντικές κατά την άποψη των υγειονομικών αρχών στο πλαίσιο της κρίσης.

— Λειτουργίες ελέγχου συμπτωμάτων και τηλεϊατρικής:

Η λειτουργία ελέγχου συμπτωμάτων μπορεί να αποτελέσει ένδειξη του ποσοστού των ατόμων που εμφανίζουν συμπτώματα συμβατά με τη νόσο COVID-19 τα οποία έχουν πράγματι προσβληθεί από τον ιό (π.χ. με τη λήψη επιχρίσματος και την εξέταση όλων ή τυχαίου αριθμού ατόμων με τέτοια συμπτώματα, εφόσον υπάρχει σχετική δυνατότητα). Ο εν λόγω καθορισμός του σκοπού θα πρέπει να καθιστά σαφές ότι τα δεδομένα προσωπικού χαρακτήρα που αφορούν την υγεία θα υποβάλλονται σε επεξεργασία προκειμένου i) να παρέχεται στο άτομο η δυνατότητα να εκτιμά μόνο του, βάσει μιας σειράς ερωτήσεων που του τίθενται, εάν έχει αναπτύξει συμπτώματα της νόσου COVID-19, ή ii) να λάβει ιατρική συμβουλή εάν έχει αναπτύξει τα συμπτώματα της νόσου COVID-19.

— Λειτουργίες ιχνηλάτησης επαφών και αποστολής ειδοποιήσεων:

Η απλή αναφορά του σκοπού «πρόληψη περαιτέρω κρουσμάτων COVID-19» δεν είναι αρκετά συγκεκριμένη. Στην εν λόγω περίπτωση, η Επιτροπή συνιστά την περαιτέρω εξειδίκευση του σκοπού ή των σκοπών προς την εξής κατεύθυνση: «συλλογή των επαφών των ατόμων που χρησιμοποιούν την εφαρμογή και τα οποία ενδέχεται να έχουν εκτεθεί σε λοίμωξη από COVID-19 με σκοπό την προειδοποίηση των εν λόγω ατόμων που ενδέχεται να έχουν προσβληθεί από τον ιό».

3.7 Καθορισμός αυστηρών ορίων στην αποθήκευση δεδομένων

Η αρχή του περιορισμού της περιόδου αποθήκευσης απαιτεί να μην διατηρούνται τα δεδομένα προσωπικού χαρακτήρα για μεγαλύτερο χρονικό διάστημα από το αναγκαίο. Τα χρονοδιαγράμματα θα πρέπει να βασίζονται στα ιατρικά δεδομένα (ανάλογα με τον σκοπό της εφαρμογής: περίοδος επώασης κ.λπ.) καθώς και στη ρεαλιστική διάρκεια των διοικητικών μέτρων που μπορεί να χρειαστεί να ληφθούν.

— Λειτουργία πληροφόρησης:

Εάν συλλέγονται δεδομένα κατά την εγκατάσταση της εν λόγω λειτουργίας, πρέπει να διαγράφονται αμέσως. Η διατήρηση των εν λόγω δεδομένων δεν δικαιολογείται.

— Λειτουργίες ελέγχου συμπτωμάτων και τηλεϊατρικής:

Τα εν λόγω δεδομένα θα πρέπει να διαγράφονται από τις υγειονομικές αρχές μετά από έναν μήνα κατ' ανώτατο όριο (περίοδος επώασης συν περιθώριο) ή μετά την εξέταση του προσώπου το αποτέλεσμα της οποίας είναι αρνητικό. Οι υγειονομικές αρχές μπορούν να διατηρούν δεδομένα για μεγαλύτερα χρονικά διαστήματα για τους σκοπούς της υποβολής εκθέσεων επιτήρησης και της έρευνας, υπό την προϋπόθεση ότι τα δεδομένα είναι ανωνυμοποιημένα.

— Λειτουργίες ιχνηλάτησης επαφών και αποστολής ειδοποιήσεων:

Τα δεδομένα εγγύτητας θα πρέπει να διαγράφονται αμέσως μόλις παύουν να είναι απαραίτητα για τον σκοπό της ειδοποίησης ατόμων. Αυτό θα πρέπει να συμβαίνει μετά από έναν μήνα κατ' ανώτατο όριο (περίοδος επώασης συν περιθώριο) ή μετά την εξέταση του προσώπου το αποτέλεσμα της οποίας είναι αρνητικό. Οι υγειονομικές αρχές μπορούν να διατηρούν τα δεδομένα εγγύτητας για μεγαλύτερα χρονικά διαστήματα για τους σκοπούς της υποβολής εκθέσεων επιτήρησης και της έρευνας, υπό την προϋπόθεση ότι τα δεδομένα είναι ανωνυμοποιημένα.

Τα δεδομένα θα πρέπει να αποθηκεύονται στη συσκευή του χρήστη και μόνο τα δεδομένα που έχουν κοινοποιηθεί από τους χρήστες και είναι αναγκαία για την εκπλήρωση του σκοπού θα πρέπει να αναφορτώνονται στον διακομιστή, στη διάθεση των υγειονομικών αρχών, εφόσον έχει γίνει αυτή η επιλογή (δηλαδή να αναφορτώνονται στον διακομιστή μόνο τα δεδομένα των «στενών επαφών» του ατόμου που βρέθηκε θετικό στη λοίμωξη COVID-19).

3.8 Διασφάλιση των δεδομένων

Η Επιτροπή συνιστά την αποθήκευση των δεδομένων στην τερματική συσκευή του χρήστη σε κρυπτογραφημένη μορφή με χρήση σύγχρονων τεχνικών κρυπτογράφησης. Σε περίπτωση αποθήκευσης των δεδομένων σε κεντρικό διακομιστή, η πρόσβαση, συμπεριλαμβανομένης της διοικητικής πρόσβασης, στον εν λόγω διακομιστή θα πρέπει να καταγράφεται.

Δεδομένα εγγύτητας θα πρέπει να παράγονται και να αποθηκεύονται μόνο στην τερματική συσκευή του χρήστη σε κρυπτογραφημένη μορφή και κατόπιν ψευδωνυμοποίησης. Για να αποφευχθεί η παρακολούθηση από τρίτους θα πρέπει να είναι δυνατή η ενεργοποίηση του Bluetooth χωρίς να απαιτείται η ενεργοποίηση άλλων υπηρεσιών γεωτοποιομίου.

Κατά τη συλλογή των δεδομένων εγγύτητας μέσω του BLE, είναι προτιμότερο να δημιουργούνται και να αποθηκεύονται προσωρινά αναγνωριστικά χρήστη που μεταβάλλονται τακτικά αντί να αποθηκεύεται το πραγματικό αναγνωριστικό της συσκευής. Το μέτρο αυτό παρέχει πρόσθετη προστασία από τη λαθρακρόαση και την παρακολούθηση από χάκερ και, ως εκ τούτου, καθιστά δυσχερέστερη την ταυτοποίηση των χρηστών.

Η Επιτροπή συνιστά να δημοσιοποιείται και να καθίσταται διαθέσιμος προς εξέταση ο πηγαίος κώδικας της εφαρμογής.

Μπορούν να προβλεφθούν πρόσθετα μέτρα για τη διασφάλιση των δεδομένων που υποβάλλονται σε επεξεργασία, ιδίως με αυτόματη διαγραφή ή ανωνυμοποίηση των δεδομένων μετά από ορισμένη χρονική στιγμή. Γενικά, ο βαθμός ασφάλειας πρέπει να αντιστοιχεί στον όγκο και στον ευαίσθητο χαρακτήρα των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία.

Όλες οι μεταδόσεις από την προσωπική συσκευή προς τις εθνικές υγειονομικές αρχές πρέπει να είναι κρυπτογραφημένες.

Όταν η εθνική νομοθεσία προβλέπει ότι τα συλλεγόμενα προσωπικά δεδομένα μπορούν επίσης να αποτελέσουν αντικείμενο επεξεργασίας για τους σκοπούς της επιστημονικής έρευνας, θα πρέπει, κατ' αρχήν, να χρησιμοποιείται ψευδωνυμοποίηση.

3.9 Διασφάλιση της ακρίβειας των δεδομένων

Η διασφάλιση της ακρίβειας των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία δεν αποτελεί μόνο προαπαιτούμενο για την αποτελεσματικότητα της εφαρμογής, αλλά και απαίτηση βάσει της νομοθεσίας για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Στο πλαίσιο αυτό, είναι σημαντικό να διασφαλίζεται η ακρίβεια των πληροφοριών σχετικά με το κατά πόσον έχει πραγματοποιηθεί επαφή με άτομο που έχει προσβληθεί από τον ιό (επιδημιολογική απόσταση και διάρκεια), ώστε να ελαχιστοποιείται ο κίνδυνος ψευδώς θετικών αποτελεσμάτων. Αυτό θα πρέπει να αφορά τα σενάρια κατά τα οποία δύο χρήστες της εφαρμογής έρχονται σε επαφή στον δρόμο, εντός των δημόσιων συγκοινωνιών ή εντός κτιρίου. Δεν είναι πιθανό η χρήση των δεδομένων θέσης που βασίζονται σε δίκτυα κινητής τηλεφωνίας να είναι αρκετά ακριβής για κάτι τέτοιο.

Ως εκ τούτου, συνιστάται η χρήση τεχνολογιών που επιτρέπουν ακριβέστερη αξιολόγηση της επαφής (όπως το Bluetooth).

3.10 Συμμετοχή των αρχών προστασίας δεδομένων

Οι αρχές προστασίας δεδομένων θα πρέπει να συμμετέχουν ενεργά και να καλούνται σε διαβούλευση στο πλαίσιο της ανάπτυξης της εφαρμογής, καθώς και να επανεξετάζουν την θέση της σε χρήση. Δεδομένου ότι η επεξεργασία των δεδομένων στο πλαίσιο της εφαρμογής θα χαρακτηρίζεται ως επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων (δεδομένων που αφορούν την υγεία), η Επιτροπή εφιστά την προσοχή στο άρθρο 35 του ΓΚΠΔ για την εκτίμηση ανικτύπου σχετικά με την προστασία δεδομένων.
