ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 09-07-2021
Αριθ. Πρωτ.: 1669

ΓΝΩΜΟΔΟΤΗΣΗ 2/2021

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε, μετά από πρόσκληση του Προέδρου της, σε έκτακτη συνεδρίαση μέσω τηλεδιάσκεψης την 8-07-2021, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Κωνσταντίνος Μενουδάκος, Πρόεδρος της Αρχής, τα τακτικά μέλη Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, ως εισηγητής, και Χαράλαμπος Ανθόπουλος. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν, με εντολή του Προέδρου, οι ελεγκτές Γεωργία Παναγοπούλου και Κωνσταντίνος Λιμνιώτης, ειδικοί επιστήμονες πληροφορικής, ως βοηθοί εισηγητή, και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Το Υπουργείο Ψηφιακής Διακυβέρνησης διαβίβασε στην Αρχή, το με αρ. πρωτ. Γ/ΕΙΣ/4515/07-07-2021 έγγραφο, σχέδιο διατάξεων με τίτλο «Διευκολύνσεις ως προς τη λειτουργία επιχειρήσεων ή άλλων χώρων συνάθροισης», αναφορικά με τη χρήση ειδικής ηλεκτρονικής εφαρμογής σε κινητές συσκευές, μέσω της οποίας θα πραγματοποιείται «*ο έλεγχος της εγκυρότητας, της γνησιότητας και της ακεραιότητας του Ψηφιακού Πιστοποιητικού COVID-19 της Ε.Ε. (EU Digital COVID Certificate - EUDCC) του Κανονισμού (ΕΕ) 2021/953 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Ιουνίου 2021 και της από 30.5.2021 Πράξης Νομοθετικού Περιεχομένου(Α' 87), η οποία κυρώθηκε με το άρθρο 1 του ν. 4806/2021 (Α΄ 95) ή ισοδύναμου πιστοποιητικού ή βεβαίωσης τρίτης χώρας, που φέρει το φυσικό πρόσωπο - κάτοχος, δια της σάρωσης του σχετικού κωδικού QR*».

Λεωφ. Κηφισίας 1-3, 11523 Αθήνα
T: 210 6475 600 • E: contact@dpa.gr • www.dpa.gr

Η Αρχή, μετά από εξέταση του ανωτέρω σχεδίου διατάξεων από την άποψη της νομοθεσίας για την προστασία των προσωπικών δεδομένων και αφού άκουσε τον εισηγητή και τους βοηθούς εισηγητές, οι οποίοι αποχώρησαν μετά τη συζήτηση της υπόθεσης και πριν από τη διάσκεψη, μετά από διεξοδική συζήτηση

ΕΚΔΙΔΕΙ ΤΗΝ ΑΚΟΛΟΥΘΗ ΓΝΩΜΟΔΟΤΗΣΗ

1. Σύμφωνα με τις διατάξεις των άρθρων 51 και 55 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 (εφεξής, ΓΚΠΔ) και του άρθρου 9 του ν. 4624/2019 (ΦΕΚ Α΄ 137), η Αρχή έχει αρμοδιότητα να εποπτεύει την εφαρμογή των διατάξεων του ΓΚΠΔ, του νόμου αυτού και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων.
2. Εισαγωγικά επισημαίνεται ότι το ανωτέρω σχέδιο διατάξεων έχει σταλεί στην Αρχή στις 5 Ιουλίου και στις 8 Ιουλίου, ενόψει του επείγοντος, συνήλθε η Ολομέλεια για να διατυπώσει τη γνώμη της επί του σχεδίου. Παρά το γεγονός ότι στις 8 Ιουλίου κατατέθηκε σε σχέδιο νόμου του Υπουργείου Δικαιοσύνης και ψηφίστηκε την ίδια μέρα από την Ολομέλεια της Βουλής τροπολογία με σχεδόν ταυτόσημες διατάξεις χωρίς να αναμένεται η σχετική γνωμοδότηση, η Αρχή θεωρεί ότι έχει υποχρέωση να διατυπώσει τις σχετικές παρατηρήσεις της.
3. Στην παρ. 1α. αναφέρεται ότι «*αναπτύσσεται ειδική ηλεκτρονική εφαρμογή για κινητές συσκευές (mobile application)…».* Η διατύπωση «*αναπτύσσεται*» μπορεί να εκληφθεί ως ανάπτυξη σε εξέλιξη, ενώ η διάταξη αφορά ειδική ηλεκτρονική εφαρμογή η οποία θα τεθεί σε λειτουργία. Προτείνεται κατάλληλη επαναδιατύπωση.
4. Στην παρ. 1α. αναφέρεται ότι *«… προς τον σκοπό της ορθής εφαρμογής των μέτρων που λαμβάνονται δυνάμει της κοινής υπουργικής απόφασης του άρθρου τεσσαρακοστού τετάρτου της από 1.5.2020 Πράξης Νομοθετικού Περιεχομένου, η οποία κυρώθηκε με το άρθρο 2 του ν. 4690/2020 (Α' 104). Η ειδική ηλεκτρονική εφαρμογή λειτουργεί για όσο χρονικό διάστημα εξακολουθεί να υφίσταται άμεσος κίνδυνος δημόσιας υγείας από τη διασπορά του κορωνοϊού COVID-19, η απουσία του οποίου διαπιστώνεται με απόφαση του Υπουργού Υγείας.»* Λαμβάνοντας

υπόψη την αρχή του περιορισμού του σκοπού (άρθρο 5 παρ. 1 στοιχ. β' του ΓΚΠΔ), η διάταξη θα πρέπει να συγκεκριμενοποιεί και να περιορίζει το σκοπό στα πλαίσια του οποίου θα αξιοποιείται η εφαρμογή. Η διατύπωση «*προς τον σκοπό της ορθής εφαρμογής των μέτρων που λαμβάνονται δυνάμει της κοινής υπουργικής απόφασης*» κρίνεται ως γενική, δεδομένου ότι δεν έχει γνωστοποιηθεί στην Αρχή η εν λόγω Κ.Υ.Α. και συνεπώς δεν είναι ορισμένες σαφώς και δεν περιγράφονται επαρκώς οι συγκεκριμένες συνθήκες και προϋποθέσεις χρήσης της εφαρμογής.

Η παύση χρήσης και λειτουργίας της εφαρμογής δεν προσδιορίζεται ρητά, με βάση κριτήρια και προϋποθέσεις που σχετίζονται με το συγκεκριμένο σκοπό που αυτή εξυπηρετεί, παρά μόνο γενικά με την αναφορά σε κινδύνους δημόσιας υγείας: «*για όσο χρονικό διάστημα εξακολουθεί να υφίσταται άμεσος κίνδυνος δημόσιας υγείας από τη διασπορά του κορωνοϊού COVID-19, η απουσία του οποίου διαπιστώνεται με απόφαση του Υπουργού Υγείας*».

Η Αρχή προτείνει οι ανωτέρω διατάξεις να τροποποιηθούν ώστε να περιορίζουν τη χρήση της εφαρμογής μόνο κατά τη χρονική περίοδο που είναι σε ισχύ η υπουργική απόφαση, η οποία θα ορίζει τα συγκεκριμένα μέτρα διευκόλυνσης ως προς τη λειτουργία επιχειρήσεων ή άλλων χώρων συνάθροισης, τα οποία και θα πρέπει να περιγράφονται επαρκώς. Είναι αυτονόητο ότι η ισχύς της υπουργικής απόφασης πρέπει να συνδέεται με το χρονικό διάστημα, κατά το οποίο τα επιβαλλόμενα μέτρα κρίνονται αναγκαία για την προστασία της δημόσιας υγείας από τη διασπορά του κορωνοϊού COVID-19.

5. Στην παρ. 2α. αναφέρεται ότι «*Η χρήση της ηλεκτρονικής εφαρμογής πραγματοποιείται από τους ιδιοκτήτες ή διοργανωτές και από εξουσιοδοτημένους από αυτούς υπαλλήλους επιχειρήσεων εστίασης, επιχειρήσεων προβολής κινηματογραφικών ταινιών, κέντρων διασκέδασης, επιχειρήσεων διεξαγωγής ζωντανών θεαμάτων και ακροαμάτων, λοιπών παραστατικών τεχνών ή κάθε είδους πολιτιστικών ή αθλητικών ή εορταστικών εκδηλώσεων ή εμπορικών εκθέσεων, οι οποίες: i) στεγάζονται ή διοργανώνονται σε κλειστούς χώρους, ή ii) λειτουργούν ή διοργανώνονται σε υπαίθριους χώρους*». Η παράθεση των περιπτώσεων χρήσης είναι ευρεία, αφού δεν συγκεκριμενοποιεί τις συνθήκες και τις προϋποθέσεις χρήσης της, ούτε τον τρόπο με τον οποίο οι χρήστες της εφαρμογής θα προβαίνουν σε δήλωση ότι θα την χρησιμοποιούν και με βάση ποια διάταξη, δηλαδή ποιο το

εφαρμοζόμενο μέτρο που αφορά την κάθε περίπτωση (λαμβάνοντας υπόψη ότι, στην πράξη, δεν θα είναι επιτρεπτή η χρήση της εφαρμογής από όλα τα πρόσωπα που περιγράφονται στην εν λόγω διάταξη παρά μόνο εφόσον συντρέχουν συγκεκριμένες προϋποθέσεις). Για παράδειγμα, υπάρχει μια γενική αναφορά σε υπαίθριους χώρους χωρίς να προσδιορίζονται κριτήρια για τη χρήση της εφαρμογής. Θα πρέπει να οριστούν επαρκώς και σαφώς οι διαδικασίες και ο τρόπος δήλωσης των χρηστών ανάλογα με την κατηγορία στην οποία εμπίπτουν, καθώς επίσης και ο τρόπος λήψης και χρήσης της εφαρμογής.

Σχετικώς παρατηρείται ότι η ρύθμιση αυτή είναι πρωθύστερη διότι προϋποθέτει τον καθορισμό, με την υπουργική απόφαση που προβλέπεται στην παράγραφο 1 του σχεδίου, των χώρων εφαρμογής των επιβαλλόμενων μέτρων, στον έλεγχο των οποίων αποβλέπει η ανωτέρω εφαρμογή.

6. Στην παρ. 3α. αναφέρεται « *… ένδειξη σχετικά με την εγκυρότητα, γνησιότητα ή ακεραιότητα*». Δεν προσδιορίζεται ποια είναι η ένδειξη που επιστρέφεται, δηλαδή «ναι/όχι/άλλο». Επίσης η αναφορά σε εγκυρότητα, γνησιότητα ή ακεραιότητα φαίνεται μάλλον περιττή διότι η διασφάλιση της εγκυρότητας του εγγράφου περιλαμβάνει τον έλεγχο των άλλων δύο ιδιοτήτων. Προτείνουμε να παραμείνει ο όρος εγκυρότητα, και να προσδιοριστεί επακριβώς η ένδειξη, την οποία επιστρέφει η εφαρμογή σε όλες τις περιπτώσεις χρήσης της, υπό το φως της αρχής της ελαχιστοποίησης των δεδομένων (άρθρο 5 παρ. 1 στοιχ. γ’ του ΓΚΠΔ), έτσι ώστε να διασφαλίζεται ότι στους χρήστες της εφαρμογής δεν θα γνωστοποιείται περισσότερη πληροφορία από ό,τι είναι αναγκαίο για την επίτευξη του σκοπού επεξεργασίας. Ειδικότερα, ο σκοπός του ελέγχου των πιστοποιητικών είναι να είναι «υγειονομικά ασφαλής» ο πολίτης που εισέρχεται σε ένα χώρο, με τον τρόπο που η ασφάλεια αυτή ορίζεται στην κάθε περίπτωση. Ως εκ τούτου, η επαλήθευση των πιστοποιητικών μέσω της εφαρμογής θα πρέπει να οδηγεί σε ένα αποτέλεσμα της μορφής «ναι/όχι» (π.χ. πράσινο ή κόκκινο χρώμα), επιπλέον της ταυτότητας του κατόχου τους, έτσι ώστε να εξάγεται η πληροφορία αν ο πολίτης που εισέρχεται σε ένα χώρο είναι «υγειονομικά ασφαλής», χωρίς όμως να αποκαλύπτονται ειδικότερες πληροφορίες σχετικά με το εάν έχει εμβολιαστεί, έκανε τεστ ή έχει νοσήσει προηγουμένως από λοίμωξη με COVID-19 .

7. Στην παρ. 3β. αναφέρεται ότι «*Το Υπουργείο Υγείας και η Γενική Γραμματεία Πολιτικής Προστασίας ορίζονται ως αυτοτελώς Υπεύθυνοι Επεξεργασίας των δεδομένων προσωπικού χαρακτήρα της παρ. 3α' ..».* Δεν παρέχονται επαρκή στοιχεία που να διασαφηνίζουν το λόγο για τον οποίο ορίζονται το Υπουργείο Υγείας και η Γενική Γραμματεία Πολιτικής Προστασίας ως υπεύθυνοι επεξεργασίας, αφού τα δεδομένα της παρ. 3α αφορούν το αποτέλεσμα από τον τρόπο λειτουργίας της εφαρμογής μόνο. Εξάλλου, δεν προσδιορίζεται με ποιο τρόπο και για ποια επεξεργασία το Υπουργείο Υγείας και η Γενική Γραμματεία Πολιτικής Προστασίας καθορίζουν το σκοπό και τα μέσα της επεξεργασίας, καθώς επίσης και ποιος ο ρόλος τους στην άσκηση των δικαιωμάτων των υποκειμένων, ώστε να δικαιολογείται ο χαρακτηρισμός τους ως αυτοτελώς Υπευθύνων Επεξεργασίας.
8. Στην παρ. 3β. αναφέρεται επίσης ότι «*Οι ιδιοκτήτες ή οι διοργανωτές της παρ. 2α ορίζονται επίσης ως αυτοτελώς Υπεύθυνοι Επεξεργασίας των ανωτέρω δεδομένων για τον σκοπό του ελέγχου της εγκυρότητας, της γνησιότητας και της ακεραιότητας των πιστοποιητικών ή των βεβαιώσεων της παρ. 1α.».* Όσον αφορά τη συμμόρφωση με τις υποχρεώσεις διαφάνειας, οι εν λόγω υπεύθυνοι επεξεργασίας δεδομένων πρέπει να παρέχουν στους ενδιαφερόμενους κατάλληλες πληροφορίες, σύμφωνα με τα άρθρα 12 και 13 του ΓΚΠΔ. Οι πληροφορίες, κατανοητές από όσο το δυνατόν περισσότερα άτομα, θα πρέπει ιδίως να είναι διαθέσιμες το νωρίτερο δυνατό πριν από την επαλήθευση (για παράδειγμα, σε ιστότοπους κρατήσεων συναυλιών κ.λπ.) και να τοποθετούνται σε θέσεις προσβάσιμες και ορατές κατά την πρόσβαση στον τόπο, την εγκατάσταση ή εκδήλωση που αφορά η επεξεργασία. Προκειμένου να διασφαλιστεί η συνοχή και η συμμόρφωση αυτών των ενημερωτικών μέτρων με τα άρθρα 12 και 13 του ΓΚΠΔ, η Αρχή συστήνει να διατίθενται από την κυβέρνηση υποδείγματα πληροφοριών στους ενδιαφερόμενους επαγγελματίες.
9. Στην παρ. 3γ ορίζεται ως εκτελούσα την επεξεργασία η ΗΔΙΚΑ ΑΕ, ενώ η ίδια έχει οριστεί ως υπεύθυνος επεξεργασίας για το ψηφιακό πιστοποιητικό, σύμφωνα με τη σχετική Πράξη Νομοθετικού Περιεχομένου (ΦΕΚ Α'87/30.05.2021) που κυρώθηκε με το ν. 4806/2021 (ΦΕΚ Α΄95/10.6.2021). Επίσης η «Ε.Δ.Υ.Τ.Ε. Α.Ε.» ορίζεται ως υποεκτελούσα την επεξεργασία για τους σκοπούς εφαρμογής του παρόντος και αναπτύσσει την ειδική ηλεκτρονική εφαρμογή της παρ. 1. Δεδομένου ότι η ανάπτυξη εφαρμογής δεν συνιστά επεξεργασία προσωπικών δεδομένων, είναι

σκόπιμο να προσδιοριστεί ο ρόλος της «Ε.Δ.Υ.Τ.Ε. Α.Ε.» στην όλη λειτουργία της εφαρμογής, καθώς και τυχόν επεξεργασία προσωπικών δεδομένων που της έχει ανατεθεί. Επίσης θα πρέπει η εκτέλεση επεξεργασίας να καλύπτεται από απαραίτητες συμβάσεις, ή έστω από μνημόνια συνεργασίας, στις οποίες θα προβλέπονται οι κατάλληλες εγγυήσεις για την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων (όπως αναφέρεται και στη Σκέψη 78 του ΓΚΠΔ, «*κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των τελευταίων εξελίξεων, να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων*»).

10. Στην παρ. 3γ στοιχ. δ) αναφέρεται ότι η ΗΔΙΚΑ *«..δύναται να προσλαμβάνει υποεκτελούντα την επεξεργασία μετά από ενημέρωση των ανωτέρω υπευθύνων επεξεργασίας*». Η Αρχή επισημαίνει ότι δεν αρκεί η ενημέρωση, καθώς απαιτείται η έγκριση των υπευθύνων επεξεργασίας για να νομιμοποιείται η ανάθεση από εκτελούντα σε υποεκτελούντα, σύμφωνα με το άρθρο 28 παρ. 2 του ΓΚΠΔ. Επίσης, δεν είναι σαφές σε ποιους υπευθύνους επεξεργασίας αναφέρεται, οι οποίοι πρέπει να προσδιοριστούν ρητά.
11. Στην παρ. 4 αναφέρεται ότι «*Τα πρόσωπα των παρ. 2α και 2β προβαίνουν στην απολύτως αναγκαία επεξεργασία των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στα πιστοποιητικά ή τις βεβαιώσεις της παρ. 1α για τον σκοπό του ελέγχου της εγκυρότητας, της γνησιότητας και της ακεραιότητας αυτών. Απαγορεύεται, ύστερα από την ολοκλήρωση της διαδικασίας ελέγχου ή επαλήθευσης, η καθ' οιονδήποτε τρόπο αποθήκευση ή τήρηση αντιγράφων των πιστοποιητικών ή βεβαιώσεων της παρ. 1α ή των δεδομένων προσωπικού χαρακτήρα που εμφανίζονται κατά τη σάρωση*». Η διάταξη πρέπει να συμπληρωθεί

ώστε να προσδιορίζονται οι συγκεκριμένες παραβάσεις και οι αντίστοιχες προβλεπόμενες κυρώσεις.

12. Στην παρ. 5. αναφέρεται ότι «*Με κοινή απόφαση των Υπουργών Εξωτερικών, Προστασίας του Πολίτη, Υγείας και Ψηφιακής Διακυβέρνησης εξειδικεύονται τα πιστοποιητικά ή οι βεβαιώσεις τρίτων χωρών που μπορούν να αποτελέσουν αντικείμενο σάρωσης σύμφωνα με την παρ. 1α.».* Δεν φαίνεται να υπάρχει πρόβλεψη για έκδοση κανονιστικής πράξης που θα προσδιορίζει τα τεχνικά και οργανωτικά μέτρα για τη λειτουργία της εφαρμογής αυτής, ούτε και πρόβλεψη για την απαραίτητη – σύμφωνα με το άρθρο 35 παρ. 3 του ΓΚΠΔ, αλλά και σύμφωνα με την υπ' αριθμ. 65/2018 Απόφαση της Αρχής – διενέργεια εκτίμησης αντικτύπου στην προστασία προσωπικών δεδομένων (ΕΑΠΔ). Επίσης, δεν έχουν κοινοποιηθεί στην Αρχή οι τελικές τεχνικές και λειτουργικές προδιαγραφές της εφαρμογής που απαιτούνται ώστε ο Υπεύθυνος Επεξεργασίας να τεκμηριώσει, και η Αρχή να κρίνει, την επάρκεια των εφαρμοζόμενων μέτρων όσον αφορά την τήρηση των αρχών στην προστασία προσωπικών δεδομένων, όπως είναι η νομιμότητα, αναλογικότητα, ασφάλεια, ελαχιστοποίηση, προστασία δεδομένων εκ σχεδιασμού και εξ ορισμού. Πρέπει επίσης να ληφθεί υπόψη ότι η χρήση «έξυπνων» εφαρμογών εγείρει διάφορα ζητήματα ιδιωτικότητας αν δεν ληφθούν εγκαίρως κατάλληλα μέτρα κατά την ανάπτυξή τους, όπως για παράδειγμα ο κίνδυνος διαρροής δεδομένων σε τρίτα μέλη (third parties) αν χρησιμοποιηθούν έτοιμες βιβλιοθήκες κώδικα τρίτων μελών. Η ΕΑΠΔ θα πρέπει να απαριθμήσει τα τεχνικά και οργανωτικά μέτρα που σχεδιάστηκαν για την ελαχιστοποίηση των εντοπισθέντων κινδύνων. Οι κίνδυνοι που απορρέουν από τη δόλια έκδοση, την παράνομη χρήση ή ακόμη και την παραποίηση των ψηφιακών στοιχείων που περιέχονται στα πιστοποιητικά θα πρέπει να ληφθούν υπόψη στην ανάλυση, εάν αυτοί οι κίνδυνοι έχουν αντίκτυπο σχετικά με τα δικαιώματα και τις ελευθερίες των ατόμων που επιθυμούν να έχουν πρόσβαση σε τόπους, εγκαταστάσεις ή εκδηλώσεις, που η πρόσβαση υπόκειται σε έλεγχο ως προς την υγειονομική τους κατάσταση. Σκόπιμο είναι επίσης, για λόγους διαφάνειας και προκειμένου να ενισχυθεί η εμπιστοσύνη των πολιτών, η εν λόγω εφαρμογή να είναι ανοιχτού κώδικα (open source).

Ο Πρόεδρος	Η Γραμματέας
Κωνσταντίνος Μενουδάκος	**Ειρήνη Παπαγεωργοπούλου**