Συστάσεις 02/2021 σχετικά με τη νομική βάση για την αποθήκευση δεδομένων πιστωτικών καρτών με αποκλειστικό σκοπό τη διευκόλυνση περαιτέρω ηλεκτρονικών συναλλαγών

Εγκρίθηκε στις 19 Μαΐου 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 70 παράγραφος 1 στοιχείο ε) του κανονισμού (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 (εφεξής «ΓΚΠΔ»),

Έχοντας υπόψη τη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο και ιδίως το παράρτημα XI και το πρωτόκολλο 37 αυτής, όπως τροποποιήθηκαν με την απόφαση της Μικτής Επιτροπής του ΕΟΧ αριθ. 154/2018 της 6ης Ιουλίου 2018,

Έχοντας υπόψη το άρθρο 12 και το άρθρο 22 του εσωτερικού κανονισμού του

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΣΥΣΤΑΣΕΙΣ:

1. Στο πλαίσιο της πανδημίας COVID-19 η ψηφιακή οικονομία και το ηλεκτρονικό εμπόριο αναπτύσσονται συνεχώς. Ανάλογη ανάπτυξη παρουσιάζουν οι κίνδυνοι που απορρέουν από τη χρήση δεδομένων πιστωτικών καρτών στο διαδίκτυο. Όπως αναφέρει η ομάδα εργασίας του άρθρου 29 στις κατευθυντήριες γραμμές της για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων, η παραβίαση των δεδομένων πιστωτικών καρτών *«σαφώς επηρεάζει σημαντικά την καθημερινή ζωή του υποκειμένου των δεδομένων»*, καθώς τα οικονομικά δεδομένα θα μπορούσαν να χρησιμοποιηθούν σε τέλεση *«απάτης πληρωμών»*[1].

2. Ως εκ τούτου, είναι πολύ σημαντικό οι υπεύθυνοι επεξεργασίας να θέσουν σε εφαρμογή κατάλληλες εγγυήσεις για τα υποκείμενα των δεδομένων και να διασφαλίσουν τον έλεγχο των δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων με στόχο τη μείωση του κινδύνου αθέμιτης επεξεργασίας και την εδραίωση της εμπιστοσύνης στο ψηφιακό περιβάλλον. Το ΕΣΠΔ θεωρεί ότι η εμπιστοσύνη αυτή είναι ζωτικής σημασίας για τη βιώσιμη ανάπτυξη της ψηφιακής οικονομίας.

3. Για τον σκοπό αυτόν, οι παρούσες συστάσεις σκοπεύουν να ενθαρρύνουν την εναρμονισμένη εφαρμογή των κανόνων περί προστασίας δεδομένων που αφορούν την επεξεργασία των δεδομένων πιστωτικών καρτών εντός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ), καθώς και να εγγυηθούν την ομοιογενή προστασία των δικαιωμάτων των υποκειμένων των δεδομένων με πλήρη σεβασμό των θεμελιωδών αρχών της προστασίας δεδομένων, σύμφωνα με τις απαιτήσεις του ΓΚΠΔ.

4. Ειδικότερα, οι παρούσες συστάσεις διαλαμβάνουν σχετικά με την αποθήκευση των δεδομένων πιστωτικών καρτών από διαδικτυακούς παρόχους αγαθών και υπηρεσιών για τον αποκλειστικό και συγκεκριμένο σκοπό της διευκόλυνσης περαιτέρω αγορών από τα υποκείμενα των δεδομένων[2]. Οι συστάσεις αυτές καλύπτουν την περίπτωση κατά την οποία το υποκείμενο των

[1] ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ - Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.

[2] Επισημαίνεται ότι δεν καλύπτουν ιδρύματα πληρωμών που λειτουργούν σε ηλεκτρονικά καταστήματα ούτε τις δημόσιες αρχές. Δεν καλύπτουν επίσης την αποθήκευση δεδομένων πιστωτικών καρτών για οποιονδήποτε

δεδομένων αγοράζει κάποιο προϊόν ή πληρώνει μια υπηρεσία μέσω διαδικτυακού τόπου ή κάποιας εφαρμογής και παρέχει δεδομένα πιστωτικών του καρτών, κατά κανόνα με τη χρήση ειδικού εντύπου, προκειμένου να πραγματοποιήσει την εκάστοτε συναλλαγή.

5. Όπως συμβαίνει σε κάθε περίπτωση επεξεργασίας, ο υπεύθυνος επεξεργασίας πρέπει να διαθέτει έγκυρη νομική βάση δυνάμει του άρθρου 6 του ΓΚΠΔ για να αποθηκεύσει τα εν λόγω δεδομένα. Στο πλαίσιο αυτό, επισημαίνεται ότι ορισμένες από τις νομικές βάσεις που αναφέρονται στο άρθρο 6 του ΓΚΠΔ δεν ισχύουν στη συγκεκριμένη περίπτωση και θα πρέπει να αποκλείονται. Η αποθήκευση δεδομένων πιστωτικών καρτών μετά τη συναλλαγή για τη διευκόλυνση περαιτέρω αγορών δεν μπορεί να θεωρηθεί απαραίτητη για τη συμμόρφωση προς έννομη υποχρέωση (άρθρο 6 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ) ούτε για τη διαφύλαξη ζωτικού συμφέροντος φυσικού προσώπου (άρθρο 6 παράγραφος 1 στοιχείο δ) του ΓΚΠΔ). Η εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας (άρθρο 6 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ) δεν μπορεί επίσης να θεωρηθεί κατάλληλη νομική βάση.

6. Επιπλέον, η αποθήκευση δεδομένων πιστωτικών καρτών μετά την πληρωμή αγαθών ή υπηρεσιών δεν είναι, αυτή καθεαυτή, απαραίτητη για την εκτέλεση σύμβασης (άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ). Ενώ, κατ' αρχάς, η επεξεργασία των δεδομένων που σχετίζονται με την πιστωτική κάρτα που χρησιμοποιεί ο πελάτης για να πληρώσει είναι απαραίτητη για την εκτέλεση της σύμβασης, ενεργοποιώντας την περίπτωση του άρθρου 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ, η αποθήκευση αυτών των δεδομένων είναι χρήσιμη μόνο για τη διευκόλυνση πιθανών επόμενων συναλλαγών και για τη διευκόλυνση των πωλήσεων. Ο σκοπός αυτός δεν μπορεί να θεωρηθεί απολύτως αναγκαίος για την εκτέλεση σύμβασης πώλησης αγαθού ή παροχής υπηρεσίας που το υποκείμενο των δεδομένων έχει ήδη πληρώσει[3].

7. Όταν η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος[4], το ΕΣΠΔ επισημαίνει ότι για να μπορεί ο υπεύθυνος επεξεργασίας να βασιστεί στο άρθρο 6 παράγραφος 1 στοιχείο στ) του ΓΚΠΔ θα πρέπει να πληρούνται οι τρεις προϋποθέσεις που θέτει το άρθρο αυτό[5]. Αυτή η νομική βάση απαιτεί, πρώτον, τον προσδιορισμό και την αξιολόγηση του εννόμου συμφέροντος που επιδιώκεται από τον υπεύθυνο επεξεργασίας ή από τρίτο. Το έννομο συμφέρον του υπεύθυνου

άλλο σκοπό, επί παραδείγματι για τη συμμόρφωση προς κάποια νομική υποχρέωση ή για την πραγματοποίηση επαναλαμβανόμενων πληρωμών σε περιπτώσεις διαρκών συμβάσεων ή συμβάσεων συνδρομής για την παροχή μακροχρόνιας υπηρεσίας (π.χ. σύμβασης που προβλέπει την παροχή συγκεκριμένου αγαθού σε μηνιαία βάση ή συνδρομή για την παροχή υπηρεσιών συνεχούς ροής που αφορούν μουσικά ή κινηματογραφικά έργα).

[3] Βλ. επίσης τις κατευθυντήριες γραμμές του ΕΣΠΔ 2/2019 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ στο πλαίσιο της παροχής επιγραμμικών υπηρεσιών σε υποκείμενα δεδομένων, ιδίως τη σελίδα 10.

[4] Βλ. γνώμη της ομάδας εργασίας του άρθρου 29 σχετικά με την έννοια των εννόμων συμφερόντων του υπεύθυνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ, η οποία ήδη τελεί υπό αναθεώρηση από το ΕΣΠΔ (βλ. πρόγραμμα εργασίας 2021/2022 του ΕΣΠΔ, το οποίο εγκρίθηκε στις 16 Μαρτίου 2021).

[5] Βλ. απόφαση του Δικαστηρίου της 4ης Μαΐου 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde κατά Rīgas pašvaldības SIA 'Rīgas satiksme', υπόθεση C-13/16, ECLI:EU:C:2017:336, σκέψη 28.

επεξεργασίας ή του τρίτου μπορεί να υπερβαίνει τον σκοπό της επεξεργασίας και πρέπει να είναι γεγενημένο και ενεστώς κατά την ημερομηνία της επεξεργασίας των δεδομένων[6].

8. Δεύτερον, η νομική βάση του εννόμου συμφέροντος απαιτεί να παρίσταται ανάγκη επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για τους σκοπούς του επιδιωκόμενου εννόμου συμφέροντος. Όσον αφορά την τελευταία προϋπόθεση, εφόσον ο υπεύθυνος επεξεργασίας έχει έννομο συμφέρον κατά τα ανωτέρω, δεν είναι προφανές ότι η αποθήκευση των δεδομένων πιστωτικών καρτών για τη διευκόλυνση μελλοντικών αγορών είναι αναγκαία για την επιδίωξη του εν λόγω εννόμου συμφέροντος. Πράγματι, η πραγματοποίηση άλλης αγοράς εξαρτάται από την απόφαση του καταναλωτή και δεν καθορίζεται από τη δυνατότητα πραγματοποίησής της «με ένα κλικ».

9. Τέλος, η τρίτη προϋπόθεση απαιτεί την εκτέλεση σταθμίσεως: το έννομο συμφέρον του υπεύθυνου επεξεργασίας ή του τρίτου πρέπει να σταθμίζεται έναντι των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, συμπεριλαμβανομένων των δικαιωμάτων του υποκειμένου των δεδομένων στην προστασία των δεδομένων και στην ιδιωτική ζωή. Η στάθμιση πρέπει να λαμβάνει υπόψη τις ειδικές περιστάσεις της επεξεργασίας[7]. Ένα ουσιώδες στοιχείο της στάθμισης είναι ο πιθανός αντίκτυπος που έχει η επεξεργασία στα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων[8]. Ο αντίκτυπος αυτός μπορεί να εξαρτάται από τη φύση των δεδομένων, τη μέθοδο επεξεργασίας και την πρόσβαση τρίτων στα εν λόγω δεδομένα. Όσον αφορά τη φύση του κριτηρίου για τα δεδομένα, επισημαίνεται ότι η ομάδα του άρθρου 29 έχει αξιολογήσει τα οικονομικά δεδομένα ως δεδομένα εξαιρετικά προσωπικού χαρακτήρα επειδή η παραβίασή τους σαφώς επηρεάζει σημαντικά την καθημερινή ζωή του υποκειμένου των δεδομένων[9]. Ως εκ τούτου, ανεξαρτήτως της υποχρέωσης του υπεύθυνου επεξεργασίας να εφαρμόζει τεχνικά και οργανωτικά μέτρα που θα διασφαλίζουν κατάλληλο επίπεδο ασφάλειας των δεδομένων πιστωτικών καρτών σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο στ) του ΓΚΠΔ και του ότι τα εν λόγω δεδομένα ενδέχεται να αποθηκευθούν για άλλους σκοπούς, η επεξεργασία τους για τη διευκόλυνση περαιτέρω αγορών ενδεχομένως ενέχει έναν ολοένα αυξανόμενο κίνδυνο παραβιάσεων της ασφάλειας των δεδομένων πιστωτικών καρτών, καθόσον συνεπάγεται την επεξεργασία σε άλλα συστήματα. Ένα άλλο σημαντικό στοιχείο της στάθμισης που θα μπορούσε να ληφθεί υπόψη για την αξιολόγηση του αντικτύπου της επεξεργασίας στα υποκείμενα των δεδομένων είναι οι εύλογες προσδοκίες των υποκειμένων των δεδομένων βάσει της σχέσης τους με τον υπεύθυνο επεξεργασίας, καθώς και του πλαισίου και του σκοπού της συλλογής των δεδομένων προσωπικού χαρακτήρα[10].

[6] Βλ. απόφαση του Δικαστηρίου της 11ης Δεκεμβρίου 2019, TK κατά Asociaţia de Proprietari bloc M5A-ScaraA, υπόθεση C-708/18, ECLI:EU:C:2019:1064, σκέψη 44.

[7] Βλ. απόφαση του Δικαστηρίου της 24ης Νοεμβρίου 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECEMD) κατά Administración del Estado, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, ECLI:EU:C:2011:777, σκέψεις 47 και 48· απόφαση του Δικαστηρίου της 19ης Οκτωβρίου 2016, Patrick Breyer κατά Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779, σκέψη 62.

[8] Βλ. απόφαση του Δικαστηρίου της 24ης Νοεμβρίου 2011 ανωτέρω, σημείο 44· απόφαση του Δικαστηρίου της 11ης Δεκεμβρίου 2019 ανωτέρω, σημείο 56.

[9] ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ - Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.

[10] Βλ. αιτιολογική σκέψη 47 του ΓΚΠΔ.

Ωστόσο, φαίνεται ότι κατά τον χρόνο της αγοράς και της παροχής δεδομένων πιστωτικών καρτών για την πληρωμή το υποκείμενο των δεδομένων δεν αναμένει ευλόγως ότι τα δεδομένα των πιστωτικών καρτών του θα αποθηκευθούν για περίοδο μεγαλύτερη από αυτήν που είναι απαραίτητη για την πληρωμή των αγαθών ή των υπηρεσιών που αγοράζει. Κατά συνέπεια, τα θεμελιώδη δικαιώματα και οι ελευθερίες του προσώπου στο οποίο αφορά η προστασία δεδομένων είναι πιθανό να υπερτερούν του εννόμου συμφέροντος του υπεύθυνου επεργασίας στο συγκεκριμένο πλαίσιο.

10. Οι επιμέρους αυτές πτυχές οδηγούν στο συμπέρασμα ότι η συγκατάθεση (άρθρο 6 παράγραφος 1 στοιχείο α) του ΓΚΠΔ) φαίνεται ότι αποτελεί τη μόνη κατάλληλη νομική βάση που καθιστά την προαναφερθείσα επεξεργασία σύννομη. Πράγματι, η ρητή συγκατάθεση του υποκειμένου των δεδομένων πρέπει να παρέχεται πριν από την αποθήκευση των δεδομένων των πιστωτικών καρτών του που έπεται κάποιας αγοράς, ώστε να αντιμετωπισθούν οι κίνδυνοι ασφαλείας και να δοθεί στο υποκείμενο των δεδομένων η δυνατότητα να ασκεί έλεγχο επί των δεδομένων του και να αποφασίζει ενεργά σχετικά με τη χρήση των δεδομένων των πιστωτικών καρτών του. Η συγκατάθεση αυτή θα επιτρέπει στον υπεύθυνο επεξεργασίας να αποδεικνύει την επιθυμία του εκάστοτε φυσικού προσώπου να διευκολύνει τις περαιτέρω αγορές του μέσω του συγκεκριμένου διαδικτυακού τόπου ή της συγκεκριμένης εφαρμογής, η οποία δεν τεκμαίρεται από το απλό γεγονός της σύναψης μίας, ή περισσότερων, μεμονωμένων συναλλαγών.

11. Η συγκατάθεση αυτή πρέπει να είναι ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει[11]. Πρέπει να παρέχεται με σαφή θετική ενέργεια, ενώ θα πρέπει να ζητείται με φιλικό προς τον χρήστη τρόπο, π.χ. μέσω μη προσυμπληρωμένου τετραγωνιδίου[12], απευθείας στο έντυπο που χρησιμοποιείται για τη συλλογή των δεδομένων. Αυτή η ρητή συγκατάθεση θα πρέπει να διακρίνεται από τη συγκατάθεση που παρέχεται για τους όρους παροχής της υπηρεσίας ή για τις πωλήσεις και να μη αποτελεί όρο για την ολοκλήρωση της συναλλαγής.

12. Σύμφωνα με το άρθρο 7 παράγραφος 3 του ΓΚΠΔ, το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει ανά πάσα στιγμή τη συγκατάθεσή του για την αποθήκευση δεδομένων πιστωτικών καρτών για σκοπούς διευκόλυνσης περαιτέρω αγορών. Η ανάκληση της συγκατάθεσης πρέπει να είναι ελεύθερη, απλή και εξίσου εύκολη για το υποκείμενο των δεδομένων με την παροχή της. Πρέπει να οδηγεί στην αποτελεσματική διαγραφή των δεδομένων πιστωτικών καρτών που αποθηκεύτηκαν από τον υπεύθυνο επεξεργασίας για τον αποκλειστικό σκοπό της διευκόλυνσης περαιτέρω συναλλαγών.

Για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η Πρόεδρος

(Andrea Jelinek)

[11] Βλ. κατευθυντήριες γραμμές 05/2020 του ΕΣΠΔ σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679.
[12] Όπ.π.