Κατευθυντήριες γραμμές 06/2020 σχετικά με την αλληλεπίδραση μεταξύ της δεύτερης οδηγίας για τις υπηρεσίες πληρωμών και του ΓΚΠΔ

Έκδοση 2.0

Εγκρίθηκε στις 15 Δεκεμβρίου 2020

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

Ιστορικό εκδόσεων

Έκδοση 2.0	15.12.2020	Έγκριση των κατευθυντήριων γραμμών μετά από δημόσια διαβούλευση
Έκδοση 1.0	17.7.2020	Έγκριση των κατευθυντήριων γραμμών για δημόσια διαβούλευση

Πίνακας περιεχομένων

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 (στο εξής: ΓΚΠΔ),

Έχοντας υπόψη τη συμφωνία για τον ΕΟΧ, και ιδίως το παράρτημα XI και το πρωτόκολλο 37 αυτής, όπως τροποποιήθηκαν με την απόφαση αριθ. 154/2018 της Μεικτής Επιτροπής του ΕΟΧ της 6ης Ιουλίου 2018[1],

Έχοντας υπόψη τα άρθρα 12 και 22 του εσωτερικού κανονισμού του,

Εκτιμώντας τα ακόλουθα:

1) Ο γενικός κανονισμός για την προστασία δεδομένων προβλέπει ένα συνεκτικό σύνολο κανόνων για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την ΕΕ.

2) Η δεύτερη οδηγία για τις υπηρεσίες πληρωμών [οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Δεκεμβρίου 2015, στο εξής: PSD2] καταργεί την οδηγία 2007/64/ΕΚ και προβλέπει νέους κανόνες για τη διασφάλιση της ασφάλειας δικαίου για τους καταναλωτές, τους εμπόρους και τις επιχειρήσεις εντός της αλυσίδας πληρωμών και τον εκσυγχρονισμό του νομικού πλαισίου για την αγορά υπηρεσιών πληρωμών[2]. Τα κράτη μέλη όφειλαν να μεταφέρουν την οδηγία PSD2 στο εθνικό τους δίκαιο πριν από τις 13 Ιανουαρίου 2018.

3) Ένα σημαντικό χαρακτηριστικό της PSD2 είναι η θέσπιση νομικού πλαισίου για νέες υπηρεσίες εκκίνησης πληρωμών και υπηρεσίες πληροφοριών λογαριασμού. Η PSD2 επιτρέπει στους εν λόγω νέους παρόχους υπηρεσιών πληρωμών να αποκτούν πρόσβαση σε λογαριασμούς πληρωμών των υποκειμένων των δεδομένων για τους σκοπούς της παροχής των υπηρεσιών αυτών.

4) Όσον αφορά την προστασία των δεδομένων, σύμφωνα με το άρθρο 94 παράγραφος 1 της PSD2, κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της παροχής πληροφοριών σχετικά με την επεξεργασία, για τους σκοπούς της PSD2 πραγματοποιείται σύμφωνα με τον ΓΚΠΔ[3] και τον κανονισμό (ΕΕ) 2018/1725.

5) Σύμφωνα με την αιτιολογική σκέψη 89 της PSD2, όταν δεδομένα προσωπικού χαρακτήρα αποτελούν αντικείμενο επεξεργασίας για τους σκοπούς της PSD2, θα πρέπει να προσδιορίζεται ο ακριβής σκοπός της επεξεργασίας, να αναφέρεται η σχετική νομική βάση και να εφαρμόζονται οι σχετικές απαιτήσεις ασφαλείας του ΓΚΠΔ, θα πρέπει δε να τηρούνται οι αρχές της αναγκαιότητας, της αναλογικότητας, του περιορισμού του σκοπού και της αναλογικής περιόδου διατήρησης δεδομένων. Επίσης, η προστασία των δεδομένων ήδη από τον σχεδιασμό και η προστασία των δεδομένων εξ

[1] Οι αναφορές στα «κράτη μέλη» στο παρόν έγγραφο θα πρέπει να νοούνται ως αναφορές στα «κράτη μέλη του ΕΟΧ».
[2] Αιτιολογική σκέψη 6 της PSD2.
[3] Δεδομένου ότι η PSD2 είναι προγενέστερη του ΓΚΠΔ, εξακολουθεί να παραπέμπει στην οδηγία 95/46. Το άρθρο 94 του ΓΚΠΔ ορίζει ότι οι παραπομπές στην καταργούμενη οδηγία 95/46 θεωρούνται παραπομπές στον ΓΚΠΔ.

ορισμού θα πρέπει να ενσωματωθούν σε όλα τα συστήματα επεξεργασίας δεδομένων που αναπτύσσονται και χρησιμοποιούνται στο πλαίσιο της PSD2[4].

6) Η αιτιολογική σκέψη 93 της PSD2 ορίζει ότι οι πάροχοι υπηρεσιών εκκίνησης πληρωμών και οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού αφενός και ο πάροχος υπηρεσιών πληρωμών εξυπηρέτησης λογαριασμού, αφετέρου, θα πρέπει να τηρούν τις αναγκαίες απαιτήσεις σχετικά με την προστασία των δεδομένων και την ασφάλεια, οι οποίες καθορίζονται από την παρούσα οδηγία ή αναφέρονται σε αυτήν ή περιλαμβάνονται στα ρυθμιστικά τεχνικά πρότυπα.

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ

1. ΕΙΣΑΓΩΓΗ

1. Η δεύτερη οδηγία για τις υπηρεσίες πληρωμών (στο εξής: PSD2) εισήγαγε ορισμένες καινοτομίες στον τομέα των υπηρεσιών πληρωμών. Παρότι δημιουργεί νέες ευκαιρίες για τους καταναλωτές και ενισχύει τη διαφάνεια στον τομέα αυτόν, η εφαρμογή της PSD2 εγείρει ορισμένα ερωτήματα και ανησυχίες όσον αφορά την ανάγκη τα υποκείμενα των δεδομένων να διατηρούν τον πλήρη έλεγχο των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Ο γενικός κανονισμός για την προστασία δεδομένων (στο εξής: ΓΚΠΔ) εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των δραστηριοτήτων επεξεργασίας που διεξάγονται στο πλαίσιο υπηρεσιών πληρωμών, όπως ορίζονται στην PSD2[5]. Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας που δραστηριοποιούνται στον τομέα που καλύπτεται από την PSD2 πρέπει πάντα να διασφαλίζουν τη συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ, συμπεριλαμβανομένων των αρχών της προστασίας των δεδομένων που ορίζονται στο άρθρο 5 του ΓΚΠΔ, καθώς και με τις σχετικές διατάξεις της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[6]. Παρότι η PSD2[7] και τα ρυθμιστικά τεχνικά πρότυπα για την αυστηρή εξακρίβωση της ταυτότητας του πελάτη και τα κοινά και ασφαλή ανοικτά πρότυπα επικοινωνίας (στο εξής: ΡΤΠ[8]) περιέχουν ορισμένες διατάξεις σχετικά με την προστασία και την ασφάλεια των δεδομένων, έχει προκύψει αβεβαιότητα όσον αφορά την ερμηνεία των εν λόγω διατάξεων, καθώς και όσον αφορά την αλληλεπίδραση μεταξύ του γενικού πλαισίου προστασίας δεδομένων και της PSD2.

2. Στις 5 Ιουλίου 2018 το ΕΣΠΔ εξέδωσε επιστολή σχετικά με την PSD2, στην οποία το ΕΣΠΔ παρείχε διευκρινίσεις σχετικά με ζητήματα που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα σε σχέση με την PSD2, ιδιαίτερα όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα μη συμβαλλομένων μερών [τα λεγόμενα «δεδομένα σιωπηλά

[4] Αιτιολογική σκέψη 89 της PSD2.
[5] Άρθρο 1 παράγραφος 1 του ΓΚΠΔ.
[6] 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).
[7] Άρθρο 94 της δεύτερης οδηγίας για τις υπηρεσίες πληρωμών κ.λπ.
[8] Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2018/389 της Επιτροπής, της 27ης Νοεμβρίου 2017, για τη συμπλήρωση της οδηγίας (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά ρυθμιστικά τεχνικά πρότυπα για την αυστηρή εξακρίβωση ταυτότητας πελάτη και τα κοινά και ασφαλή ανοικτά πρότυπα επικοινωνίας (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)· C(2017)7782· ΕΕ L 69 της 13.3.2018, σ. 23-43· διατίθεται στη διεύθυνση https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32018R0389&from=EN

μετεχόντων» (silent party data)] από παρόχους υπηρεσιών πληροφοριών λογαριασμού (στο εξής: AISP) και παρόχους υπηρεσιών εκκίνησης πληρωμών (στο εξής: PISP), τις διαδικασίες για τη χορήγηση και την ανάκληση συγκατάθεσης, τα ΡΤΠ και τη συνεργασία μεταξύ παρόχων υπηρεσιών πληρωμών εξυπηρέτησης λογαριασμού (στο εξής: ASPSP) σε σχέση με τα μέτρα ασφαλείας. Στο πλαίσιο των προπαρασκευαστικών εργασιών για τις εν λόγω κατευθυντήριες γραμμές συλλέχθηκαν στοιχεία από τα ενδιαφερόμενα μέρη, τόσο γραπτώς όσο και σε εκδήλωση με τα ενδιαφερόμενα μέρη, προκειμένου να προσδιοριστούν οι πλέον πιεστικές προκλήσεις.

3. Οι παρούσες κατευθυντήριες γραμμές αποσκοπούν στην παροχή περαιτέρω καθοδήγησης σχετικά με πτυχές της προστασίας δεδομένων στο πλαίσιο της PSD2, ιδιαίτερα όσον αφορά τη σχέση μεταξύ των σχετικών διατάξεων του ΓΚΠΔ και της PSD2. Οι παρούσες κατευθυντήριες γραμμές εστιάζουν κυρίως στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από τους AISP και τους PISP. Ως εκ τούτου, το παρόν έγγραφο εξετάζει τις προϋποθέσεις για τη χορήγηση πρόσβασης σε πληροφορίες λογαριασμού πληρωμών από τους ASPSP και για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τους PISP και τους AISP, συμπεριλαμβανομένων των απαιτήσεων και εγγυήσεων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τους PISP και τους AISP για σκοπούς άλλους από τους αρχικούς σκοπούς για τους οποίους συλλέχθηκαν τα δεδομένα, ιδιαίτερα όταν έχουν συλλεχθεί στο πλαίσιο της παροχής υπηρεσίας πληροφοριών λογαριασμού[9]. Το παρόν έγγραφο εξετάζει επίσης διάφορες έννοιες της ρητής συγκατάθεσης στο πλαίσιο της PSD2 και του ΓΚΠΔ, την επεξεργασία των «δεδομένων σιωπηλά μετεχόντων», την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα από PISP και AISP, την εφαρμογή των βασικών αρχών προστασίας δεδομένων που ορίζονται στον ΓΚΠΔ, συμπεριλαμβανομένων της ελαχιστοποίησης των δεδομένων, της διαφάνειας, της λογοδοσίας και των μέτρων ασφάλειας. Η PSD2 περιλαμβάνει διαλειτουργικές αρμοδιότητες στους τομείς, μεταξύ άλλων, της προστασίας των καταναλωτών και του δικαίου του ανταγωνισμού. Ζητήματα που αφορούν αυτούς τους τομείς του δικαίου είναι εκτός του πεδίου εφαρμογής των παρουσών κατευθυντήριων γραμμών.

4. Για να διευκολυνθεί η ανάγνωση των κατευθυντήριων γραμμών, παρατίθενται κατωτέρω οι βασικοί ορισμοί που χρησιμοποιούνται στο παρόν έγγραφο.

1.1 Ορισμοί

«Πάροχος υπηρεσίας πληροφοριών λογαριασμού» («AISP»): ο πάροχος διαδικτυακής υπηρεσίας για την παροχή συγκεντρωτικών πληροφοριών σχετικά με έναν ή περισσότερους λογαριασμούς πληρωμών που τηρεί ο χρήστης υπηρεσιών πληρωμών είτε σε άλλο πάροχο υπηρεσιών πληρωμών είτε σε περισσότερους του ενός παρόχους υπηρεσιών πληρωμών·

«Πάροχος υπηρεσιών πληρωμών εξυπηρέτησης λογαριασμού» («ASPSP»): ο πάροχος υπηρεσιών πληρωμών ο οποίος παρέχει και τηρεί λογαριασμό πληρωμής για πληρωτή·

«Ελαχιστοποίηση των δεδομένων»: η αρχή προστασίας δεδομένων, σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία·

[9] Υπηρεσία πληροφοριών λογαριασμού είναι η διαδικτυακή υπηρεσία για την παροχή συγκεντρωτικών πληροφοριών σχετικά με έναν ή περισσότερους λογαριασμούς πληρωμών που τηρεί ο χρήστης υπηρεσιών πληρωμών είτε σε άλλο πάροχο υπηρεσιών πληρωμών είτε σε περισσότερους του ενός παρόχους υπηρεσιών πληρωμών.

«Πληρωτής»: το φυσικό ή νομικό πρόσωπο το οποίο διατηρεί λογαριασμό πληρωμών και επιτρέπει εντολή πληρωμής από αυτόν τον λογαριασμό ή, εάν δεν υπάρχει λογαριασμός πληρωμών, το φυσικό ή νομικό πρόσωπο που δίνει εντολή πληρωμής·

«Δικαιούχος»: το φυσικό ή νομικό πρόσωπο που είναι ο τελικός αποδέκτης των χρηματικών ποσών τα οποία αποτελούν αντικείμενο της πράξης πληρωμής·

«Λογαριασμός πληρωμών»: ο λογαριασμός που τηρείται στο όνομα ενός ή περισσότερων χρηστών υπηρεσιών πληρωμών και χρησιμοποιείται για την εκτέλεση πράξεων πληρωμής·

«Πάροχος υπηρεσίας εκκίνησης πληρωμής» («PISP»): ο πάροχος υπηρεσίας για την έναρξη εντολής πληρωμής κατόπιν αιτήματος του χρήστη υπηρεσιών πληρωμών σε σχέση με λογαριασμό πληρωμών που τηρείται σε άλλο πάροχο υπηρεσιών πληρωμών·

«Πάροχος υπηρεσιών πληρωμών»: μία από τις οντότητες που αναφέρονται στο άρθρο 1 παράγραφος 1 της PSD2[10] ή φυσικό ή νομικό πρόσωπο που τυγχάνει εξαίρεσης δυνάμει του άρθρου 32 ή 33 της PSD2·

«Χρήστης υπηρεσιών πληρωμών»: το φυσικό ή νομικό πρόσωπο που χρησιμοποιεί μια υπηρεσία πληρωμών ως πληρωτής, δικαιούχος, ή και με τις δύο ιδιότητες·

«Δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας, ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου·

«Προστασία των δεδομένων ήδη από τον σχεδιασμό»: τεχνικά και οργανωτικά μέτρα ενσωματωμένα σε προϊόν ή υπηρεσία, τα οποία έχουν σχεδιαστεί για την αποτελεσματική εφαρμογή των αρχών προστασίας των δεδομένων και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία,

[10] Το άρθρο 1 παράγραφος 1 της PSD2 ορίζει ότι η PSD2 θεσπίζει τους κανόνες διά των οποίων τα κράτη μέλη διακρίνουν μεταξύ των ακόλουθων κατηγοριών *παρόχων υπηρεσιών πληρωμών*:
α) πιστωτικά ιδρύματα όπως ορίζονται στο άρθρο 4 παράγραφος 1 σημείο 1) του κανονισμού (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (1), περιλαμβανομένων των υποκαταστημάτων τους όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 17) του εν λόγω κανονισμού, όταν τα εν λόγω υποκαταστήματα βρίσκονται στην Ένωση, είτε η έδρα τους βρίσκεται εντός της Ένωσης είτε, σύμφωνα με το άρθρο 47 της οδηγίας 2013/36/ΕΕ και με το εθνικό δίκαιο, εκτός της Ένωσης·
β) ιδρύματα ηλεκτρονικού χρήματος όπως ορίζονται στο άρθρο 2 σημείο 1) της οδηγίας 2009/110/ΕΚ, περιλαμβανομένων, σύμφωνα με το άρθρο 8 της εν λόγω οδηγίας και το εθνικό δίκαιο, των υποκαταστημάτων τους, όταν τα εν λόγω υποκαταστήματα βρίσκονται στην Ένωση και η έδρα τους βρίσκεται εκτός της Ένωσης, και μόνο στον βαθμό που οι υπηρεσίες πληρωμών τις οποίες προσφέρουν τα εν λόγω υποκαταστήματα συνδέονται με την έκδοση ηλεκτρονικού χρήματος·
γ) γραφεία ταχυδρομικών επιταγών τα οποία εξουσιοδοτούνται βάσει του εθνικού δικαίου να παρέχουν υπηρεσίες πληρωμών·
δ) ιδρύματα πληρωμών·
ε) η ΕΚΤ και οι εθνικές κεντρικές τράπεζες όταν δεν ενεργούν υπό την ιδιότητά τους ως νομισματικών ή άλλων δημόσιων αρχών·
στ) τα κράτη μέλη ή οι περιφερειακές ή τοπικές αρχές τους όταν δεν ενεργούν υπό την ιδιότητά τους ως δημόσιων αρχών.

ώστε να πληρούνται οι απαιτήσεις του ΓΚΠΔ και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων·

«Προστασία των δεδομένων εξ ορισμού»: κατάλληλα τεχνικά και οργανωτικά μέτρα τα οποία εφαρμόζονται σε προϊόν ή υπηρεσία και τα οποία διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας·

«ΡΤΠ»: ο κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2018/389 της Επιτροπής, της 27ης Νοεμβρίου 2017, για τη συμπλήρωση της οδηγίας (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά ρυθμιστικά τεχνικά πρότυπα για την αυστηρή εξακρίβωση ταυτότητας πελάτη και τα κοινά και ασφαλή ανοικτά πρότυπα επικοινωνίας·

«Τρίτοι πάροχοι» (στο εξής: TPP»): τόσο οι PISP όσο και οι AISP.

1.2 Υπηρεσίες στο πλαίσιο της PSD2

5. Η PSD2 εισάγει δύο νέα είδη (παρόχους) υπηρεσιών πληρωμών: τους PISP και τους AISP. Το παράρτημα I της PSD2 περιλαμβάνει τις οκτώ υπηρεσίες πληρωμών που καλύπτονται από την PSD2.

6. Οι PISP παρέχουν υπηρεσίες για την έναρξη εντολής πληρωμής κατόπιν αιτήματος του χρήστη υπηρεσιών πληρωμών σε σχέση με λογαριασμό πληρωμών χρήστη που τηρείται σε άλλο πάροχο υπηρεσιών πληρωμών[11]. Ένας PISP μπορεί να ζητήσει από έναν ASPSP (συνήθως τράπεζα) να εκκινήσει συναλλαγή για λογαριασμό του χρήστη υπηρεσιών πληρωμών. Ο χρήστης (υπηρεσιών πληρωμών) μπορεί να είναι φυσικό πρόσωπο (υποκείμενο των δεδομένων) ή νομικό πρόσωπο.

7. Οι AISP παρέχουν διαδικτυακές υπηρεσίες για την παροχή συγκεντρωτικών πληροφοριών σχετικά με έναν ή περισσότερους λογαριασμούς πληρωμών που τηρεί ο χρήστης υπηρεσιών πληρωμών είτε σε άλλο πάροχο υπηρεσιών πληρωμών είτε σε περισσότερους του ενός παρόχους υπηρεσιών πληρωμών[12]. Σύμφωνα με την αιτιολογική σκέψη 28 της PSD2, ο χρήστης των υπηρεσιών πληρωμών έχει τη δυνατότητα να έχει αμέσως, σε οποιαδήποτε δεδομένη στιγμή, μία συνολική εικόνα της οικονομικής του κατάστασης.

8. Όσον αφορά τις υπηρεσίες πληροφοριών λογαριασμού, θα μπορούσαν να παρέχονται διάφορα είδη υπηρεσιών, με έμφαση σε διαφορετικά χαρακτηριστικά και σκοπούς. Για παράδειγμα, ορισμένοι πάροχοι μπορεί να προσφέρουν στους χρήστες υπηρεσίες, όπως ο δημοσιονομικός προγραμματισμός και η παρακολούθηση των δαπανών. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο αυτών των υπηρεσιών καλύπτεται από την PSD2. Οι υπηρεσίες που συνεπάγονται αξιολογήσεις πιστοληπτικής ικανότητας του χρήστη υπηρεσιών πληρωμών ή ελεγκτικές υπηρεσίες που διενεργούνται βάσει της συλλογής πληροφοριών μέσω υπηρεσίας πληροφοριών λογαριασμού δεν εμπίπτουν στο πεδίο εφαρμογής της PSD2 και, ως εκ τούτου, εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ. Επιπλέον, οι λογαριασμοί εκτός από τους λογαριασμούς πληρωμών (π.χ. ταμιευτηρίου, επενδύσεων) επίσης δεν καλύπτονται από την PSD2. Σε κάθε περίπτωση, ο ΓΚΠΔ αποτελεί το εφαρμοστέο νομικό πλαίσιο για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Παράδειγμα 1:

[11] Άρθρο 4 σημείο 15 της PSD2.
[12] Άρθρο 4 σημείο 16 της PSD2.

Η HappyPayments είναι μια εταιρεία που προσφέρει διαδικτυακή υπηρεσία η οποία συνίσταται στην παροχή πληροφοριών για έναν ή περισσότερους λογαριασμούς πληρωμών μέσω εφαρμογής για κινητές συσκευές με σκοπό την παροχή οικονομικού ελέγχου (υπηρεσία πληροφοριών λογαριασμού). Με την υπηρεσία αυτή, ο χρήστης υπηρεσιών πληρωμών μπορεί να δει με μια ματιά το υπόλοιπο και τις πρόσφατες συναλλαγές σε δύο ή περισσότερους λογαριασμούς πληρωμών που τηρούνται σε διαφορετικές τράπεζες. Παρέχει επίσης, όταν ο χρήστης υπηρεσιών πληρωμών το επιλέγει, κατηγοριοποίηση των δαπανών και των εσόδων ανάλογα με τις διάφορες τυπολογίες (μισθός, αναψυχή, ενέργεια, υποθήκη κ.λπ.), βοηθώντας έτσι τον χρήστη υπηρεσιών πληρωμών στον οικονομικό σχεδιασμό. Στο πλαίσιο αυτής της εφαρμογής, η HappyPayments προσφέρει επίσης μια υπηρεσία για την έναρξη πληρωμών απευθείας από τον/τους λογαριασμό/-ούς πληρωμών που έχουν οριστεί από τους χρήστες (υπηρεσία εκκίνησης πληρωμών).

9. Για την παροχή των υπηρεσιών αυτών, η PSD2 ρυθμίζει τις νομικές προϋποθέσεις υπό τις οποίες οι PISP και οι AISP μπορούν να έχουν πρόσβαση σε λογαριασμούς πληρωμών για την παροχή υπηρεσίας στον χρήστη υπηρεσιών πληρωμών.

10. Το άρθρο 66 παράγραφος 1 και το άρθρο 67 παράγραφος 1 της PSD2 ορίζουν ότι η πρόσβαση και η χρήση των υπηρεσιών πληρωμών και πληροφοριών λογαριασμού αποτελούν δικαιώματα του χρήστη υπηρεσιών πληρωμών. Αυτό σημαίνει ότι ο χρήστης υπηρεσιών πληρωμών θα πρέπει να διατηρεί πλήρη ελευθερία όσον αφορά την άσκηση του εν λόγω δικαιώματος και δεν μπορεί να υποχρεώνεται να κάνει χρήση του δικαιώματος αυτού.

11. Η πρόσβαση σε λογαριασμούς πληρωμών και η χρήση πληροφοριών λογαριασμού πληρωμών ρυθμίζονται εν μέρει στα άρθρα 66 και 67 της PSD2, τα οποία περιέχουν εγγυήσεις όσον αφορά την προστασία των δεδομένων (προσωπικού χαρακτήρα). Το άρθρο 66 παράγραφος 3 στοιχείο στ) της PSD2 ορίζει ότι ο PISP δεν ζητεί από τον χρήστη υπηρεσιών πληρωμών κανένα άλλο στοιχείο πέραν αυτών που είναι αναγκαία για την παροχή της υπηρεσίας εκκίνησης πληρωμών, και το άρθρο 66 παράγραφος 3 στοιχείο ζ) της PSD2 προβλέπει ότι οι PISP αποφεύγουν τη χρήση, πρόσβαση και αποθήκευση δεδομένων για σκοπούς άλλους από την εκτέλεση της υπηρεσίας εκκίνησης πληρωμών που ζητεί ρητά ο χρήστης υπηρεσιών πληρωμών. Επιπλέον, το άρθρο 67 παράγραφος 2 στοιχείο δ) της PSD2 περιορίζει την πρόσβαση των AISP στις πληροφορίες από καθορισμένους λογαριασμούς πληρωμών και τις συναφείς πράξεις πληρωμής, ενώ το άρθρο 67 παράγραφος 2 στοιχείο στ) της PSD2 ορίζει ότι οι AISP αποφεύγουν τη χρήση, πρόσβαση ή αποθήκευση δεδομένων για σκοπούς άλλους από την εκτέλεση της υπηρεσίας πληροφοριών λογαριασμού που έχει ζητήσει ρητά ο χρήστης υπηρεσιών πληρωμών, σύμφωνα με τους κανόνες προστασίας των δεδομένων. Οι εν λόγω κανόνες τονίζουν ότι, στο πλαίσιο των υπηρεσιών πληροφοριών λογαριασμού, τα δεδομένα προσωπικού χαρακτήρα μπορούν να συλλέγονται μόνο για καθορισμένους, ρητούς και νόμιμους σκοπούς. Ως εκ τούτου, οι AISP θα πρέπει να αναφέρουν ρητά στη σύμβαση τους συγκεκριμένους σκοπούς για τους οποίους πρόκειται να υποβληθούν σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα που περιέχονται σε πληροφορίες λογαριασμού, στο πλαίσιο της υπηρεσίας πληροφοριών λογαριασμού που παρέχουν. Σύμφωνα με το άρθρο 5 του ΓΚΠΔ, η σύμβαση θα πρέπει να είναι σύννομη, θεμιτή και διαφανής, καθώς και να συνάδει με άλλες νομοθετικές διατάξεις για την προστασία των καταναλωτών.

12. Ανάλογα με τις συγκεκριμένες περιστάσεις, οι πάροχοι υπηρεσιών πληρωμών θα μπορούσαν να είναι υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία βάσει του ΓΚΠΔ. Στις παρούσες κατευθυντήριες γραμμές, ως «υπεύθυνος επεξεργασίας» νοείται ο πάροχος υπηρεσιών πληρωμών ο οποίος, μόνος ή από κοινού με άλλους, καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Περισσότερες οδηγίες σχετικά με το θέμα

αυτό παρέχονται στις κατευθυντήριες γραμμές 07/2020 του ΕΣΠΔ σχετικά με τις έννοιες του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία στον ΓΚΠΔ.

2 ΝΟΜΙΜΟΙ ΛΟΓΟΙ ΚΑΙ ΠΕΡΑΙΤΕΡΩ ΕΠΕΞΕΡΓΑΣΙΑ ΒΑΣΕΙ ΤΗΣ PSD2

2.1 Νόμιμοι λόγοι επεξεργασίας

13. Σύμφωνα με τον ΓΚΠΔ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπευθύνους επεξεργασίας πρέπει να έχει νομική βάση. Το άρθρο 6 παράγραφος 1 του ΓΚΠΔ περιλαμβάνει εξαντλητικό και περιοριστικό κατάλογο έξι νομικών βάσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα βάσει του ΓΚΠΔ[13]. Εναπόκειται στον υπεύθυνο επεξεργασίας να καθορίσει την κατάλληλη νομική βάση και να διασφαλίσει ότι πληρούνται όλες οι προϋποθέσεις για αυτή τη νομική βάση. Ο καθορισμός της βάσης που είναι έγκυρη και καταλληλότερη σε μια συγκεκριμένη περίπτωση εξαρτάται από τις περιστάσεις υπό τις οποίες πραγματοποιείται η επεξεργασία, συμπεριλαμβανομένου του σκοπού της επεξεργασίας και της σχέσης μεταξύ του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων.

2.2 Άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ (η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης)

14. Οι υπηρεσίες πληρωμών παρέχονται βάσει σύμβασης μεταξύ του χρήστη υπηρεσιών πληρωμών και του παρόχου υπηρεσιών πληρωμών. Όπως ορίζεται στην αιτιολογική σκέψη 87 της PSD2, «*[Η] παρούσα οδηγία θα πρέπει να αφορά μόνον συμβατικές υποχρεώσεις και ευθύνες μεταξύ του χρήστη υπηρεσιών πληρωμών και του οικείου παρόχου υπηρεσιών πληρωμών.*» Στο πλαίσιο του ΓΚΠΔ, η κύρια νομική βάση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για την παροχή υπηρεσιών πληρωμών είναι το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ, υπό την έννοια ότι η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης.

15. Οι υπηρεσίες πληρωμών στο πλαίσιο της PSD2 ορίζονται στο παράρτημα 1 της PSD2. Η παροχή αυτών των υπηρεσιών, όπως ορίζεται στην PSD2, αποτελεί προϋπόθεση για τη σύναψη σύμβασης με την οποία τα μέρη έχουν πρόσβαση στα δεδομένα λογαριασμού πληρωμών του χρήστη υπηρεσιών πληρωμών. Οι εν λόγω πάροχοι υπηρεσιών πληρωμών πρέπει επίσης να είναι αδειοδοτημένοι φορείς εκμετάλλευσης. Όσον αφορά τις υπηρεσίες εκκίνησης πληρωμών και τις

[13] Σύμφωνα με το άρθρο 6, η επεξεργασία είναι σύννομη μόνον εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,
β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,
γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,
δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,
ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,
στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύουν το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ειδικότερα εάν το υποκείμενο των δεδομένων είναι παιδί.

υπηρεσίες πληροφοριών λογαριασμού στο πλαίσιο της PSD2, οι συμβάσεις μπορούν να περιλαμβάνουν όρους που επιβάλλουν επίσης προϋποθέσεις σχετικά με πρόσθετες υπηρεσίες που δεν ρυθμίζονται από την PSD2. Οι *κατευθυντήριες γραμμές 2/2019 του ΕΣΠΔ 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* καθιστούν σαφές ότι οι υπεύθυνοι επεξεργασίας πρέπει να εκτιμούν ποια επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αντικειμενικά απαραίτητη για την εκτέλεση της σύμβασης. Στις εν λόγω κατευθυντήριες γραμμές επισημαίνεται ότι η αιτιολόγηση της αναγκαιότητας εξαρτάται από τη φύση της υπηρεσίας, τις αμοιβαίες προοπτικές και προσδοκίες των συμβαλλομένων μερών, το σκεπτικό της σύμβασης και τα ουσιώδη στοιχεία της σύμβασης.

16. Οι κατευθυντήριες γραμμές 2/2019 του ΕΣΠΔ καθιστούν επίσης σαφές ότι, βάσει του άρθρου 7 παράγραφος 4 του ΓΚΠΔ, γίνεται διάκριση μεταξύ των δραστηριοτήτων επεξεργασίας που είναι αναγκαίες για την εκτέλεση μιας σύμβασης και των όρων που καθιστούν την παροχή υπηρεσιών εξαρτημένη από ορισμένες δραστηριότητες επεξεργασίας που δεν είναι πράγματι απαραίτητες για την εκτέλεση της σύμβασης. Η διατύπωση «απαραίτητη για την εκτέλεση» απαιτεί σαφώς κάτι περισσότερο από έναν συμβατικό όρο[14]. Ο υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να αποδεικνύει πως το κύριο αντικείμενο της συγκεκριμένης σύμβασης με το υποκείμενο των δεδομένων δεν μπορεί, βάσει πραγματικών στοιχείων, να εκτελεστεί αν δεν διενεργηθεί η συγκεκριμένη επεξεργασία των εν λόγω δεδομένων προσωπικού χαρακτήρα. Η απλή παραπομπή ή αναφορά στην επεξεργασία δεδομένων σε μια σύμβαση δεν επαρκεί για να εντάξει την εν λόγω επεξεργασία στο πεδίο εφαρμογής του άρθρου 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ.

17. Το άρθρο 5 παράγραφος 1 στοιχείο β) του ΓΚΠΔ προβλέπει την αρχή του περιορισμού του σκοπού, σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Κατά την εκτίμηση του εάν το άρθρο 6 παράγραφος 1 στοιχείο β) αποτελεί την κατάλληλη νομική βάση για επεξεργασία στο πλαίσιο μιας σύμβασης επιγραμμικών υπηρεσιών, θα πρέπει να λαμβάνεται υπόψη ο συγκεκριμένος στόχος, σκοπός ή αντικειμενικός σκοπός της υπηρεσίας[15]. Οι σκοποί της επεξεργασίας πρέπει να καθορίζονται με σαφήνεια και να ανακοινώνονται στο υποκείμενο των δεδομένων, σύμφωνα με τις υποχρεώσεις του υπεύθυνου επεξεργασίας για τον περιορισμό του σκοπού και για τη διαφάνεια. Η εκτίμηση του τι είναι «απαραίτητο» περιλαμβάνει μια συνδυαστική, εστιασμένη στα γεγονότα εκτίμηση της επεξεργασίας «για τον στόχο που επιδιώκεται και κατά πόσον είναι λιγότερο επεμβατική συγκρινόμενη με άλλες επιλογές για την επίτευξη του ίδιου στόχου». Το άρθρο 6 παράγραφος 1 στοιχείο β) δεν καλύπτει επεξεργασία που είναι χρήσιμη αλλά όχι αντικειμενικά απαραίτητη για την εκτέλεση της συμβατικής υπηρεσίας ή για τη λήψη σχετικών μέτρων πριν από τη σύναψη σύμβασης κατ' αίτηση του υποκειμένου των δεδομένων, ακόμα κι αν είναι απαραίτητη για άλλους επιχειρηματικούς σκοπούς του υπευθύνου επεξεργασίας[16].

18. Οι κατευθυντήριες γραμμές 2/2019 του ΕΣΠΔ καθιστούν σαφές ότι οι συμβάσεις δεν μπορούν να επεκτείνουν τεχνητά τις κατηγορίες δεδομένων προσωπικού χαρακτήρα ή τους τύπους

[14] Κατευθυντήριες γραμμές 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, ΕΣΠΔ, σ. 10.
[15] Ό.π., σ. 11.
[16] Ό.π., σ. 10.

δραστηριοτήτων επεξεργασίας που ο υπεύθυνος επεξεργασίας είναι απαραίτητο να διενεργήσει για την εκτέλεση της σύμβασης κατά την έννοια του άρθρου 6 παράγραφος 1 στοιχείο β)[17]. Οι παρούσες κατευθυντήριες γραμμές εξετάζουν επίσης περιπτώσεις στις οποίες μπορούν να δημιουργηθούν καταστάσεις «όλα ή τίποτα» για τα υποκείμενα των δεδομένων που μπορεί να ενδιαφέρονται μόνο για μία από τις υπηρεσίες. Αυτό μπορεί να συμβεί όταν ο υπεύθυνος επεξεργασίας επιθυμεί να συνενώσει σε μία μόνο σύμβαση διάφορες ξεχωριστές υπηρεσίες ή στοιχεία υπηρεσιών με διαφορετικούς θεμελιώδεις σκοπούς, χαρακτηριστικά ή σκεπτικό. Όταν η σύμβαση αποτελείται από διάφορες ξεχωριστές υπηρεσίες ή στοιχεία υπηρεσιών που εύλογα μπορούν να εκτελεστούν στην πραγματικότητα ανεξάρτητα το ένα από το άλλο, η εφαρμογή του άρθρου 6 παράγραφος 1 στοιχείο β) θα πρέπει να εκτιμηθεί στο πλαίσιο κάθε μιας από τις υπηρεσίες αυτές ξεχωριστά, εξετάζοντας τι είναι αντικειμενικά απαραίτητο για την εκτέλεση κάθε μιας από τις υπηρεσίες ξεχωριστά που το υποκείμενο των δεδομένων έχει ενεργά αιτηθεί ή συμφωνήσει[18].

19. Σύμφωνα με τις προαναφερθείσες κατευθυντήριες γραμμές, οι υπεύθυνοι επεξεργασίας πρέπει να εκτιμήσουν τι είναι αντικειμενικά απαραίτητο για την εκτέλεση της σύμβασης. Όταν οι υπεύθυνοι επεξεργασίας δεν μπορούν να αποδείξουν ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που περιέχονται σε λογαριασμό πληρωμών είναι αντικειμενικά απαραίτητη για την παροχή καθεμιάς από τις εν λόγω υπηρεσίες χωριστά, το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ δεν αποτελεί έγκυρη νομική βάση για την επεξεργασία. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας θα πρέπει να εξετάζει άλλη νομική βάση για την επεξεργασία.

2.3 Πρόληψη της απάτης

20. Το άρθρο 94 παράγραφος 1 της PSD2 ορίζει ότι τα κράτη μέλη επιτρέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα συστήματα πληρωμών και τους παρόχους υπηρεσιών πληρωμών, όταν χρειάζεται για την πρόληψη, τη διερεύνηση και τον εντοπισμό απάτης στον τομέα των πληρωμών. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα που είναι απολύτως απαραίτητη για την πρόληψη της απάτης θα μπορούσε να συνιστά έννομο συμφέρον του ενδιαφερόμενου παρόχου υπηρεσιών πληρωμών, υπό τον όρο ότι δεν υπερισχύει των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων[19]. Οι δραστηριότητες επεξεργασίας με σκοπό την πρόληψη της απάτης θα πρέπει να βασίζονται σε προσεκτική κατά περίπτωση αξιολόγηση από τον υπεύθυνο επεξεργασίας, σύμφωνα με την αρχή της λογοδοσίας. Επιπλέον, για την πρόληψη της απάτης, οι υπεύθυνοι επεξεργασίας μπορεί επίσης να υπόκεινται σε συγκεκριμένες νομικές υποχρεώσεις που απαιτούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

2.4 Περαιτέρω επεξεργασία (AISP και PISP)

21. Το άρθρο 6 παράγραφος 4 του ΓΚΠΔ καθορίζει τις προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπό άλλον από αυτόν για τον οποίο συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα. Ειδικότερα, η εν λόγω περαιτέρω επεξεργασία μπορεί να πραγματοποιηθεί, όταν βασίζεται στο δίκαιο της Ένωσης ή κράτους μέλους, το οποίο συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των σκοπών που αναφέρονται στο άρθρο 23 παράγραφος 1, όταν το υποκείμενο των δεδομένων έχει συναινέσει

[17] Ό.π., σ. 11.
[18] Ό.π., σ. 13.
[19] Αιτιολογική σκέψη 47 του ΓΚΠΔ.

ή όταν η επεξεργασία για σκοπό άλλον από αυτόν για τον οποίο συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα είναι συμβατή με τον αρχικό σκοπό.

22. Το άρθρο 66 παράγραφος 3 στοιχείο ζ) και το άρθρο 67 παράγραφος 2 στοιχείο στ) της PSD2 πρέπει να λαμβάνονται προσεκτικά υπόψη. Όπως προαναφέρθηκε, το άρθρο 66 παράγραφος 3 στοιχείο ζ) της PSD2 ορίζει ότι ο PISP αποφεύγει τη χρήση, πρόσβαση και αποθήκευση δεδομένων για σκοπούς άλλους από την εκτέλεση της υπηρεσίας εκκίνησης πληρωμών που ζητεί ρητά ο πληρωτής. Το άρθρο 67 παράγραφος 2 στοιχείο στ) της PSD2 ορίζει ότι ο AISP αποφεύγει τη χρήση, πρόσβαση ή αποθήκευση δεδομένων για σκοπούς άλλους από την εκτέλεση της υπηρεσίας πληροφοριών λογαριασμού που έχει ζητήσει ρητά ο χρήστης υπηρεσιών πληρωμών, σύμφωνα με τους κανόνες προστασίας των δεδομένων.

23. Κατά συνέπεια, το άρθρο 66 παράγραφος 3 στοιχείο ζ) και το άρθρο 67 παράγραφος 2 στοιχείο στ) της PSD2 περιορίζουν σημαντικά τις δυνατότητες επεξεργασίας για άλλους σκοπούς, υπό την έννοια ότι η επεξεργασία για άλλον σκοπό δεν επιτρέπεται, εκτός αν το υποκείμενο των δεδομένων έχει συναινέσει σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) του ΓΚΠΔ ή η επεξεργασία βασίζεται στο δίκαιο της Ένωσης ή στο δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, σύμφωνα με το άρθρο 6 παράγραφος 4 του ΓΚΠΔ. Όταν η επεξεργασία για σκοπό άλλον από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή στο δίκαιο κράτους μέλους, οι περιορισμοί που προβλέπονται στο άρθρο 66 παράγραφος 3 στοιχείο ζ) και στο άρθρο 67 παράγραφος 2 στοιχείο στ) της PSD2 καθιστούν σαφές ότι οποιοσδήποτε άλλος σκοπός δεν είναι συμβατός με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα. Το κριτήριο συμβατότητας του άρθρου 6 παράγραφος 4 του ΓΚΠΔ δεν μπορεί να οδηγήσει σε νομική βάση για την επεξεργασία.

24. Το άρθρο 6 παράγραφος 4 του ΓΚΠΔ επιτρέπει την περαιτέρω επεξεργασία όταν βασίζεται στο δίκαιο της Ένωσης ή στο δίκαιο κράτους μέλους. Για παράδειγμα, σύμφωνα με το άρθρο 3 σημείο 2 στοιχείο α) της οδηγίας (ΕΕ) 2015/849 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2015, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, όλοι οι PISP και οι AISP είναι υπόχρεες οντότητες. Ως εκ τούτου, αυτές οι υπόχρεες οντότητες είναι υποχρεωμένες να εφαρμόζουν τα μέτρα δέουσας επιμέλειας ως προς τον πελάτη, όπως ορίζονται στην οδηγία. Κατά συνέπεια, τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στο πλαίσιο υπηρεσίας της PSD2 υποβάλλονται σε περαιτέρω επεξεργασία βάσει τουλάχιστον μίας νομικής υποχρέωσης που βαρύνει τον πάροχο της υπηρεσίας[20].

25. Όπως αναφέρεται στην παράγραφο 20, το άρθρο 6 παράγραφος 4 του ΓΚΠΔ αναφέρει ότι η επεξεργασία για σκοπό άλλον από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα θα μπορούσε να βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων, εφόσον πληρούνται όλες οι προϋποθέσεις για συγκατάθεση βάσει του ΓΚΠΔ. Όπως αναφέρεται ανωτέρω, ο υπεύθυνος επεξεργασίας πρέπει να αποδείξει ότι το υποκείμενο των δεδομένων είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί (αιτιολογική σκέψη 42 του ΓΚΠΔ).

[20] Επισημαίνεται ότι η διεξοδική εξέταση του αν η οδηγία για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες πληροί το κριτήριο του άρθρου 6 παράγραφος 4 του ΓΚΠΔ δεν εμπίπτει στο πεδίο εφαρμογής του παρόντος εγγράφου.

2.5 Νόμιμος λόγος για τη χορήγηση πρόσβασης στον λογαριασμό (ASPSP)

26. Όπως αναφέρεται στην παράγραφο 10, οι χρήστες υπηρεσιών πληρωμών μπορούν να ασκήσουν το δικαίωμά τους να κάνουν χρήση των υπηρεσιών εκκίνησης πληρωμών και πληροφοριών λογαριασμού. Οι υποχρεώσεις που επιβάλλονται στα κράτη μέλη με το άρθρο 66 παράγραφος 1 και το άρθρο 67 παράγραφος 1 της PSD2 θα πρέπει να ενσωματωθούν στο εθνικό δίκαιο, προκειμένου να διασφαλιστεί η αποτελεσματική εφαρμογή του δικαιώματος του χρήστη υπηρεσιών πληρωμών να επωφελείται από τις προαναφερθείσες υπηρεσίες πληρωμών. Η αποτελεσματική εφαρμογή των δικαιωμάτων αυτών δεν θα ήταν δυνατή χωρίς την ύπαρξη αντίστοιχης υποχρέωσης του ASPSP, συνήθως τράπεζας, να παρέχει στον πάροχο υπηρεσιών πληρωμών πρόσβαση στον λογαριασμό, υπό τον όρο ότι πληροί όλες τις προϋποθέσεις για να έχει πρόσβαση στον λογαριασμό του χρήστη υπηρεσιών πληρωμών. Επιπλέον, το άρθρο 66 παράγραφος 5 και το άρθρο 67 παράγραφος 4 της PSD2 ορίζουν σαφώς ότι η παροχή υπηρεσιών εκκίνησης πληρωμών και υπηρεσιών πληροφοριών λογαριασμού δεν εξαρτάται από την ύπαρξη συμβατικής σχέσης μεταξύ του PISP/AISP και του ASPSP.

27. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον ASPSP, η οποία συνίσταται στη χορήγηση πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που ζητούν ο PISP και ο AISP για την παροχή της υπηρεσίας πληρωμών τους στον χρήστη υπηρεσιών πληρωμών, βασίζεται σε νομική υποχρέωση. Προκειμένου να επιτευχθούν οι στόχοι της PSD2, οι ASPSP πρέπει να παρέχουν τα δεδομένα προσωπικού χαρακτήρα για τις υπηρεσίες των PISP και των AISP, γεγονός που αποτελεί απαραίτητη προϋπόθεση για την παροχή υπηρεσιών από τους PISP και τους AISP και, ως εκ τούτου, τη διασφάλιση των δικαιωμάτων που προβλέπονται στο άρθρο 66 παράγραφος 1 και στο άρθρο 67 παράγραφος 1 της PSD2. Ως εκ τούτου, η εφαρμοστέα νομική βάση στην προκειμένη περίπτωση είναι το άρθρο 6 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ.

28. Δεδομένου ότι στον ΓΚΠΔ διευκρινίζεται ότι η επεξεργασία βάσει νομικής υποχρέωσης θα πρέπει να ορίζεται σαφώς σύμφωνα με το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους (βλ. άρθρο 6 παράγραφος 3 του ΓΚΠΔ), η υποχρέωση των ASPSP να χορηγούν πρόσβαση θα πρέπει να απορρέει από την εθνική νομοθεσία για τη μεταφορά της PSD2.

3 ΡΗΤΗ ΣΥΓΚΑΤΑΘΕΣΗ

3.1 Συγκατάθεση βάσει του ΓΚΠΔ

29. Σύμφωνα με τον ΓΚΠΔ, η συγκατάθεση αποτελεί μία από τις έξι νομικές βάσεις για τη νομιμότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Το άρθρο 4 σημείο 11 του ΓΚΠΔ ορίζει τη συγκατάθεση ως «κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν», Αυτές οι τέσσερις προϋποθέσεις, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, είναι απαραίτητες για την εγκυρότητα της συγκατάθεσης. Σύμφωνα με τις κατευθυντήριες γραμμές 05/2020 του ΕΣΠΔ σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, η συγκατάθεση μπορεί να αποτελεί κατάλληλη νόμιμη βάση μόνο εάν στο υποκείμενο των δεδομένων παρέχεται έλεγχος και πραγματική επιλογή όσον αφορά την αποδοχή ή την απόρριψη των προσφερόμενων όρων ή την απόρριψη αυτών χωρίς ζημία. Όταν ο υπεύθυνος επεξεργασίας ζητεί συγκατάθεση, πρέπει να εξετάζει αν πληρούνται όλες οι απαιτήσεις για την εξασφάλιση έγκυρης συγκατάθεσης. Εάν η συγκατάθεση αποκτηθεί με πλήρη συμμόρφωση προς τον ΓΚΠΔ, αποτελεί εργαλείο το οποίο παρέχει στα υποκείμενα των δεδομένων έλεγχο σχετικά με το αν τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν θα υποβληθούν σε επεξεργασία. Σε αντίθετη περίπτωση, ο έλεγχος του υποκειμένου των δεδομένων καθίσταται πλασματικός και η συγκατάθεση δεν αποτελεί έγκυρη νομική βάση για την επεξεργασία, με αποτέλεσμα η πράξη επεξεργασίας να καθίσταται παράνομη[21].

30. Ο ΓΚΠΔ περιλαμβάνει επίσης περαιτέρω εγγυήσεις στο άρθρο 7, το οποίο ορίζει ότι ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να είναι σε θέση να αποδείξει ότι υπήρξε έγκυρη συγκατάθεση κατά τον χρόνο της επεξεργασίας. Επιπλέον, το αίτημα για συγκατάθεση πρέπει να υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Επιπροσθέτως, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται σχετικά με το δικαίωμα να ανακαλέσει τη συγκατάθεση ανά πάσα στιγμή, με τον ίδιο απλό τρόπο όπως και για την παροχή της συγκατάθεσης.

31. Σύμφωνα με το άρθρο 9 του ΓΚΠΔ, η συγκατάθεση αποτελεί μία από τις εξαιρέσεις από τη γενική απαγόρευση επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Ωστόσο, στην περίπτωση αυτή, η συγκατάθεση του υποκειμένου των δεδομένων πρέπει να είναι «ρητή»[22].

32. Σύμφωνα με τις κατευθυντήριες γραμμές 05/2020 του ΕΣΠΔ σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, η ρητή συγκατάθεση βάσει του ΓΚΠΔ αναφέρεται στον τρόπο με τον οποίο το υποκείμενο των δεδομένων εκφράζει τη συγκατάθεση. Σημαίνει ότι το υποκείμενο των δεδομένων πρέπει να προβεί σε ρητή δήλωση συγκατάθεσης για συγκεκριμένο σκοπό ή σκοπούς επεξεργασίας. Ένας προφανής τρόπος για να διασφαλίζεται ότι η συγκατάθεση είναι ρητή είναι να επιβεβαιώνεται ρητώς σε γραπτή δήλωση. Όταν ενδείκνυται, ο υπεύθυνος επεξεργασίας μπορεί να διασφαλίζει ότι το υποκείμενο των δεδομένων υπογράφει τη γραπτή δήλωση, προκειμένου να αρθεί κάθε ενδεχόμενη αμφιβολία και δυνητική έλλειψη αποδείξεων στο μέλλον.

[21] Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, ΕΣΠΔ, παράγραφος 3.

[22] Βλ. επίσης γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης (WP187), σ. 7-9, και/ή γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ (WP217), σ. 11, 12, 17 και 18.

33. Σε καμία περίπτωση δεν μπορεί να προκύπτει συγκατάθεση από δυνητικά διφορούμενες δηλώσεις ή ενέργειες. Ο υπεύθυνος επεξεργασίας πρέπει επίσης να μεριμνά ώστε η συγκατάθεση να μην εξασφαλίζεται με την ίδια ενέργεια με την οποία παρέχεται η συμφωνία σε σύμβαση ή γίνονται αποδεκτοί γενικοί όροι και προϋποθέσεις υπηρεσίας.

3.2 Συγκατάθεση βάσει της PSD2

34. Το ΕΣΠΔ επισημαίνει ότι το νομικό πλαίσιο σχετικά με τη ρητή συγκατάθεση είναι πολύπλοκο, δεδομένου ότι τόσο η PSD2 όσο και ο ΓΚΠΔ περιλαμβάνουν την έννοια της «ρητής συγκατάθεσης». Αυτό οδηγεί στο ερώτημα αν η «ρητή συγκατάθεση», όπως αναφέρεται στο άρθρο 94 παράγραφος 2 της PSD2, θα πρέπει να ερμηνεύεται με τον ίδιο τρόπο όπως η ρητή συγκατάθεση βάσει του ΓΚΠΔ.

3.2.1 Ρητή συγκατάθεση βάσει του άρθρου 94 παράγραφος 2 της PSD2

35. Η PSD2 περιλαμβάνει σειρά ειδικών κανόνων σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, κυρίως στο άρθρο 94 παράγραφος 1 της PSD2, το οποίο ορίζει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της PSD2 πρέπει να πραγματοποιείται σύμφωνα με τη νομοθεσία της ΕΕ για την προστασία των δεδομένων. Επιπλέον, σύμφωνα με το άρθρο 94 παράγραφος 2 της PSD2, οι πάροχοι υπηρεσιών πληρωμών έχουν πρόσβαση, επεξεργάζονται και διατηρούν τα προσωπικά δεδομένα που είναι απαραίτητα για την παροχή των υπηρεσιών πληρωμών, μόνο με τη ρητή συγκατάθεση του χρήστη υπηρεσιών πληρωμών. Σύμφωνα με το άρθρο 33 παράγραφος 2 της PSD2, αυτή η απαίτηση ρητής συγκατάθεσης του χρήστη υπηρεσιών πληρωμών δεν ισχύει για τους AISP. Ωστόσο, το άρθρο 67 παράγραφος 2 στοιχείο α) της PSD2 εξακολουθεί να προβλέπει τη ρητή συγκατάθεση των AISP για την παροχή της υπηρεσίας.

36. Όπως προαναφέρθηκε, ο κατάλογος των νομικών βάσεων για την επεξεργασία βάσει του ΓΚΠΔ είναι εξαντλητικός. Όπως αναφέρεται στην παράγραφο 14, η νομική βάση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για την παροχή υπηρεσιών πληρωμών είναι, κατ' αρχήν, το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ, υπό την έννοια ότι η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης. Επομένως, το άρθρο 94 παράγραφος 2 της PSD2 δεν μπορεί να θεωρηθεί ως πρόσθετη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το ΕΣΠΔ θεωρεί ότι, βάσει των ανωτέρω, η παρούσα παράγραφος θα πρέπει να ερμηνεύεται, αφενός, σύμφωνα με το ισχύον νομικό πλαίσιο για την προστασία των δεδομένων και, αφετέρου, κατά τρόπο που να διαφυλάσσεται η πρακτική αποτελεσματικότητά της. Ως εκ τούτου, η ρητή συγκατάθεση βάσει του άρθρου 94 παράγραφος 2 της PSD2 θα πρέπει να θεωρείται πρόσθετη απαίτηση συμβατικής φύσης[23] σε σχέση με την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και την επακόλουθη επεξεργασία και αποθήκευση δεδομένων προσωπικού χαρακτήρα με σκοπό την παροχή υπηρεσιών πληρωμών και, ως εκ τούτου, διαφέρει από τη (ρητή) συγκατάθεση βάσει του ΓΚΠΔ.

37. Η «ρητή συγκατάθεση» που αναφέρεται στο άρθρο 94 παράγραφος 2 της PSD2 είναι συμβατική συγκατάθεση. Αυτό σημαίνει ότι το άρθρο 94 παράγραφος 2 της PSD2 θα πρέπει να ερμηνεύεται υπό την έννοια ότι, κατά τη σύναψη σύμβασης με πάροχο υπηρεσιών πληρωμών βάσει της PSD2, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται πλήρως για τις συγκεκριμένες κατηγορίες δεδομένων προσωπικού χαρακτήρα που θα υποβληθούν σε επεξεργασία. Επιπλέον, πρέπει να ενημερώνονται για τον συγκεκριμένο σκοπό (υπηρεσίας πληρωμών) για τον οποίο θα υποβληθούν σε επεξεργασία τα οικεία δεδομένα προσωπικού χαρακτήρα και πρέπει να

[23] Επιστολή του ΕΣΠΔ σχετικά με την οδηγία PSD2, 5 Ιουλίου 2018, σ. 4.

συμφωνήσουν ρητά με αυτές τις ρήτρες. Οι ρήτρες αυτές θα πρέπει να είναι σαφώς διακριτές από τα άλλα θέματα που εξετάζονται στη σύμβαση και θα πρέπει να γίνονται ρητώς δεκτές από το υποκείμενο των δεδομένων.

38. Κεντρικό στοιχείο της έννοιας της «ρητής συγκατάθεσης» σύμφωνα με το άρθρο 94 παράγραφος 2 της PSD2 είναι η απόκτηση πρόσβασης σε δεδομένα προσωπικού χαρακτήρα για τη μεταγενέστερη επεξεργασία και αποθήκευση των δεδομένων αυτών με σκοπό την παροχή υπηρεσιών πληρωμών. Αυτό σημαίνει ότι ο πάροχος υπηρεσιών πληρωμών[24] δεν επεξεργάζεται ακόμη τα δεδομένα προσωπικού χαρακτήρα, αλλά χρειάζεται πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που έχουν υποβληθεί σε επεξεργασία υπό την ευθύνη οποιουδήποτε άλλου υπευθύνου επεξεργασίας. Αν ένας χρήστης υπηρεσιών πληρωμών συνάψει σύμβαση, για παράδειγμα, με πάροχο υπηρεσιών εκκίνησης πληρωμών, ο εν λόγω πάροχος πρέπει να αποκτήσει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα του χρήστη υπηρεσιών πληρωμών τα οποία υποβάλλονται σε επεξεργασία υπό την ευθύνη του παρόχου υπηρεσιών πληρωμών εξυπηρέτησης λογαριασμού. Αντικείμενο της ρητής συγκατάθεσης βάσει του άρθρου 94 παράγραφος 2 της PSD2 είναι η άδεια πρόσβασης στα εν λόγω δεδομένα προσωπικού χαρακτήρα, ώστε να είναι δυνατή η επεξεργασία και αποθήκευση αυτών των δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητα για την παροχή της υπηρεσίας πληρωμών. Αν το υποκείμενο των δεδομένων δώσει ρητή συγκατάθεση, ο πάροχος υπηρεσιών πληρωμών εξυπηρέτησης λογαριασμού υποχρεούται να παράσχει πρόσβαση στα αναφερόμενα δεδομένα προσωπικού χαρακτήρα.

39. Παρότι η συγκατάθεση του άρθρου 94 παράγραφος 2 της PSD2 δεν αποτελεί νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, η συγκατάθεση αυτή αφορά ειδικά τα δεδομένα προσωπικού χαρακτήρα και την προστασία των δεδομένων και εξασφαλίζει διαφάνεια και έναν βαθμό ελέγχου για τον χρήστη υπηρεσιών πληρωμών[25]. Μολονότι η PSD2 δεν προσδιορίζει τις ουσιαστικές προϋποθέσεις για τη συγκατάθεση βάσει του άρθρου 94 παράγραφος 2 της PSD2, θα πρέπει, όπως προαναφέρθηκε, να ερμηνεύεται σύμφωνα με το εφαρμοστέο νομικό πλαίσιο για την προστασία των δεδομένων και κατά τρόπο που να διαφυλάσσεται η πρακτική αποτελεσματικότητά της.

40. Όσον αφορά τις πληροφορίες που πρέπει να παρέχονται από τους υπευθύνους επεξεργασίας και την απαίτηση διαφάνειας, οι κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 σχετικά με τη διαφάνεια ορίζουν ότι «*Σύμφωνα με μια κεντρική θεώρηση της αρχής της διαφάνειας που σκιαγραφείται σε αυτές τις διατάξεις, το υποκείμενο των δεδομένων θα πρέπει να είναι σε θέση να προσδιορίζει εκ των προτέρων το πεδίο εφαρμογής της επεξεργασίας και τις συνέπειες που αυτή συνεπάγεται και δεν θα πρέπει να εκπλήσσεται σε μεταγενέστερο στάδιο όσον αφορά τους τρόπους με τους οποίους έχουν χρησιμοποιηθεί τα δεδομένα προσωπικού χαρακτήρα τους*»[26].

41. Επιπλέον, όπως απαιτείται από την αρχή του περιορισμού του σκοπού, τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς [άρθρο 5 παράγραφος 1 στοιχείο β) του ΓΚΠΔ]. Όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται για περισσότερους από έναν σκοπούς, «*οι υπεύθυνοι επεξεργασίας θα πρέπει να αποφεύγουν να*

[24] Αυτό ισχύει για τις υπηρεσίες 1 έως 7 του παραρτήματος 1 της PSD2.
[25] Το άρθρο 94 παράγραφος 2 της PSD2 εμπίπτει στο κεφάλαιο 4 «Προστασία δεδομένων».
[26] Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, παράγραφος 10 (εκδόθηκαν στις 11 Απριλίου 2018) — εγκρίθηκαν από το ΕΣΠΔ.

προσδιορίζουν έναν μόνο ευρύ σκοπό προκειμένου να δικαιολογήσουν διάφορες δραστηριότητες περαιτέρω επεξεργασίας οι οποίες στην πραγματικότητα έχουν ελάχιστη μόνο σχέση με τον πραγματικό αρχικό σκοπό»[27]. Πρόσφατα, στο πλαίσιο των συμβάσεων για επιγραμμικές υπηρεσίες, το ΕΣΠΔ επισήμανε τον κίνδυνο συμπερίληψης ρητρών γενικής επεξεργασίας στις συμβάσεις και δήλωσε ότι ο σκοπός της συλλογής πρέπει να καθορίζεται με σαφήνεια και ακρίβεια: πρέπει να είναι αρκετά λεπτομερής, ώστε να προσδιορίζει το είδος της επεξεργασίας που περιλαμβάνεται και δεν περιλαμβάνεται στο πλαίσιο του καθορισμένου σκοπού και να επιτρέπει την εκτίμηση της συμμόρφωσης με το δίκαιο και την εφαρμογή των εγγυήσεων προστασίας των δεδομένων[28].

42. Όταν εξετάζεται στο πλαίσιο της πρόσθετης απαίτησης ρητής συγκατάθεσης σύμφωνα με το άρθρο 94 παράγραφος 2 της PSD2, αυτό συνεπάγεται ότι οι υπεύθυνοι επεξεργασίας πρέπει να παρέχουν στα υποκείμενα των δεδομένων ακριβείς και σαφείς πληροφορίες σχετικά με τους συγκεκριμένους σκοπούς που καθορίζονται από τον υπεύθυνο επεξεργασίας για τους οποίους παρέχεται δυνατότητα πρόσβασης, επεξεργασίας και διατήρησης των οικείων δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με το άρθρο 94 παράγραφος 2 της PSD2, τα υποκείμενα των δεδομένων πρέπει να αποδέχονται ρητά αυτούς τους συγκεκριμένους σκοπούς.

43. Επιπλέον, όπως αναφέρεται ανωτέρω στην παράγραφο 10, το ΕΣΠΔ επισημαίνει ότι ο χρήστης υπηρεσιών πληρωμών πρέπει να είναι σε θέση να επιλέξει αν θα χρησιμοποιήσει ή όχι την υπηρεσία και δεν μπορεί να υποχρεωθεί να το πράξει. Ως εκ τούτου, η συγκατάθεση βάσει του άρθρου 94 παράγραφος 2 της PSD2 πρέπει επίσης να είναι ελεύθερη.

3.3 Συμπέρασμα

44. Η ρητή συγκατάθεση βάσει της PSD2 διαφέρει από τη (ρητή) συγκατάθεση βάσει του ΓΚΠΔ. Η ρητή συγκατάθεση βάσει του άρθρου 94 παράγραφος 2 της PSD2 αποτελεί πρόσθετη απαίτηση συμβατικής φύσης. Όταν ένας πάροχος υπηρεσιών πληρωμών χρειάζεται πρόσβαση σε δεδομένα προσωπικού χαρακτήρα για την παροχή υπηρεσίας πληρωμών, απαιτείται ρητή συγκατάθεση του χρήστη υπηρεσιών πληρωμών σύμφωνα με το άρθρο 94 παράγραφος 2 της PSD2.

[27] Ομάδα εργασίας του άρθρου 29, Γνώμη 03/2013 σχετικά με τον περιορισμό του σκοπού (WP203), σ. 16.
[28] Κατευθυντήριες γραμμές 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, παράγραφος 16 (έκδοση δημόσιας διαβούλευσης) και γνώμη 03/2013 της ομάδας εργασίας του άρθρου 29 σχετικά με τον περιορισμό του σκοπού (WP203), σ. 15-16.

4 ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΣΙΩΠΗΛΑ ΜΕΤΕΧΟΝΤΩΝ

4.1 Δεδομένα σιωπηλά μετεχόντων

45. Ένα ζήτημα προστασίας δεδομένων που χρήζει προσεκτικής εξέτασης είναι η επεξεργασία των λεγόμενων «δεδομένων σιωπηλά μετεχόντων» (silent party data). Στο πλαίσιο του παρόντος εγγράφου, τα δεδομένα σιωπηλά μετεχόντων είναι δεδομένα προσωπικού χαρακτήρα που αφορούν υποκείμενο δεδομένων το οποίο δεν είναι χρήστης συγκεκριμένου παρόχου υπηρεσιών πληρωμών, αλλά του οποίου τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία από τον συγκεκριμένο πάροχο υπηρεσιών πληρωμών για την εκτέλεση σύμβασης μεταξύ του παρόχου και του χρήστη υπηρεσιών πληρωμών. Αυτό συμβαίνει, για παράδειγμα, όταν ένας χρήστης υπηρεσιών πληρωμών, το υποκείμενο δεδομένων Α, χρησιμοποιεί τις υπηρεσίες ενός AISP, και το υποκείμενο δεδομένων Β έχει προβεί σε σειρά πράξεων πληρωμής στον λογαριασμό πληρωμών του υποκειμένου δεδομένων Α. Στην περίπτωση αυτή, το υποκείμενο δεδομένων Β θεωρείται ως «σιωπηλά μετέχων» και τα δεδομένα προσωπικού χαρακτήρα (όπως ο αριθμός λογαριασμού του υποκειμένου δεδομένων Β και το χρηματικό ποσό που σχετιζόταν με τις εν λόγω πράξεις) που αφορούν το υποκείμενο δεδομένων Β θεωρούνται «δεδομένα σιωπηλά μετεχόντων».

4.2 Έννομο συμφέρον του υπευθύνου επεξεργασίας:

46. Το άρθρο 5 παράγραφος 1 στοιχείο β) του ΓΚΠΔ ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται μόνο για καθορισμένους, σαφείς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Επιπλέον, ο ΓΚΠΔ ορίζει ότι κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι τόσο απαραίτητη όσο και αναλογική και σύμφωνη με τις αρχές προστασίας των δεδομένων, όπως οι αρχές του περιορισμού του σκοπού και της ελαχιστοποίησης των δεδομένων.

47. Ο ΓΚΠΔ μπορεί να επιτρέπει την επεξεργασία των δεδομένων σιωπηλά μετεχόντων όταν η εν λόγω επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος [άρθρο 6 παράγραφος 1 στοιχείο στ) του ΓΚΠΔ]. Ωστόσο, η εν λόγω επεξεργασία μπορεί να πραγματοποιηθεί μόνον όταν του έννομου συμφέροντος του υπευθύνου επεξεργασίας δεν «υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα».

48. Ως εκ τούτου, νόμιμη βάση για την επεξεργασία των δεδομένων σιωπηλά μετεχόντων από τους PISP και τους AISP —στο πλαίσιο της παροχής υπηρεσιών πληρωμών βάσει της PSD2— θα μπορούσε να είναι το έννομο συμφέρον ενός υπευθύνου επεξεργασίας ή ενός τρίτου για την εκτέλεση της σύμβασης με τον χρήστη υπηρεσιών πληρωμών. Η ανάγκη επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του σιωπηλά μετέχοντος είναι περιορισμένη και καθορίζεται από τις εύλογες προσδοκίες των εν λόγω υποκειμένων των δεδομένων. Στο πλαίσιο της παροχής υπηρεσιών πληρωμών που καλύπτονται από την PSD2, πρέπει να θεσπιστούν αποτελεσματικά και κατάλληλα μέτρα προκειμένου να διασφαλιστεί ότι υπερισχύουν τα συμφέροντα ή τα θεμελιώδη δικαιώματα και οι ελευθερίες των σιωπηλά μετεχόντων και ότι γίνονται σεβαστές οι εύλογες προσδοκίες των εν λόγω υποκειμένων των δεδομένων όσον αφορά την επεξεργασία των οικείων δεδομένων προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, ο υπεύθυνος επεξεργασίας (AISP ή PISP) πρέπει να θεσπίσει τις αναγκαίες εγγυήσεις για την επεξεργασία με σκοπό την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων. Στις εγγυήσεις αυτές περιλαμβάνονται τεχνικά μέτρα για να διασφαλιστεί ότι τα δεδομένα των σιωπηλά μετεχόντων δεν υποβάλλονται σε επεξεργασία για σκοπό άλλον από τον σκοπό για τον οποίο τα δεδομένα προσωπικού

χαρακτήρα συλλέχθηκαν αρχικά από τους PISP και τους AISP. Εάν είναι εφικτό, θα πρέπει να χρησιμοποιείται επίσης κρυπτογράφηση ή να εφαρμόζονται άλλες τεχνικές για την επίτευξη κατάλληλου επιπέδου ασφάλειας και ελαχιστοποίησης των δεδομένων.

4.3 Περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα του σιωπηλά μετέχοντος

49. Όπως αναφέρεται στην παράγραφο 29, τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στο πλαίσιο υπηρεσίας πληρωμών που ρυθμίζεται από την PSD2 θα μπορούσαν να υποβληθούν σε περαιτέρω επεξεργασία βάσει νομικών υποχρεώσεων που βαρύνουν τον πάροχο υπηρεσιών. Αυτές οι νομικές υποχρεώσεις θα μπορούσαν να αφορούν δεδομένα προσωπικού χαρακτήρα του σιωπηλά μετέχοντος.

50. Όσον αφορά την περαιτέρω επεξεργασία δεδομένων του σιωπηλά μετέχοντος βάσει έννομου συμφέροντος, το ΕΣΠΔ είναι της γνώμης ότι τα εν λόγω δεδομένα δεν μπορούν να χρησιμοποιούνται για σκοπό άλλον από αυτόν για τον οποίο έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα, βάσει του δικαίου της ΕΕ ή του δικαίου κράτους μέλους. Η συγκατάθεση του σιωπηλά μετέχοντος δεν είναι νομικά εφικτή, διότι, προκειμένου να εξασφαλιστεί συγκατάθεση, θα έπρεπε να συλλέγονται ή να υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα του σιωπηλά μετέχοντος, για τα οποία δεν υπάρχει νομική βάση βάσει του άρθρου 6 του ΓΚΠΔ. Ούτε το κριτήριο συμβατότητας του άρθρου 6 παράγραφος 4 του ΓΚΠΔ μπορεί να αποτελέσει βάση για την επεξεργασία για άλλους σκοπούς (π.χ. δραστηριότητες άμεσης εμπορικής προώθησης). Τα δικαιώματα και οι ελευθερίες αυτών των υποκειμένων των δεδομένων-σιωπηλά μετεχόντων δεν θα γίνονται σεβαστά αν ο νέος υπεύθυνος επεξεργασίας δεδομένων χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα για άλλους σκοπούς, λαμβανομένων υπόψη του πλαισίου στο οποίο έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα, ιδιαίτερα της απουσίας οποιασδήποτε σχέσης με τα υποκείμενα των δεδομένων που είναι σιωπηλά μετέχοντες[29]· της απουσίας οποιασδήποτε σύνδεσης μεταξύ οποιουδήποτε άλλου σκοπού και του σκοπού για τον οποίο συλλέχθηκαν αρχικά τα δεδομένα προσωπικού χαρακτήρα (δηλαδή του γεγονότος ότι οι PSP χρειάζονται τα δεδομένα σιωπηλά μετεχόντων μόνο για την εκτέλεση σύμβασης με το άλλο συμβαλλόμενο μέρος)· της φύσης των σχετικών δεδομένων προσωπικού χαρακτήρα[30], του γεγονότος ότι τα υποκείμενα των δεδομένων δεν είναι σε θέση να αναμένουν ευλόγως οποιαδήποτε περαιτέρω επεξεργασία ή ακόμη και να γνωρίζουν ποιος υπεύθυνος επεξεργασίας μπορεί να επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα τους και δεδομένα των νομικών περιορισμών στην επεξεργασία που προβλέπονται στο άρθρο 66 παράγραφος 3 στοιχείο ζ) και στο άρθρο 67 παράγραφος 2 στοιχείο στ) της PSD2.

[29] Σύμφωνα με την αιτιολογική σκέψη 87 της PSD2, η PSD2 αφορά μόνον συμβατικές υποχρεώσεις και ευθύνες μεταξύ του χρήστη υπηρεσιών πληρωμών και του οικείου παρόχου υπηρεσιών πληρωμών. Ως εκ τούτου, τα δεδομένα σιωπηλά μετεχόντων δεν εμπίπτουν στο πεδίο εφαρμογής της PSD2.

[30] Ιδιαίτερη προσοχή θα πρέπει να δίνεται κατά την επεξεργασία οικονομικών δεδομένων προσωπικού χαρακτήρα, δεδομένου ότι η επεξεργασία μπορεί να θεωρηθεί ότι αυξάνει τον πιθανό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, σύμφωνα με τις κατευθυντήριες γραμμές για την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ).

5 Η ΕΠΕΞΕΡΓΑΣΙΑ ΕΙΔΙΚΩΝ ΚΑΤΗΓΟΡΙΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΒΑΣΕΙ ΤΗΣ PSD2

5.1 Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα

51. Σύμφωνα με το άρθρο 9 παράγραφος 1 του ΓΚΠΔ, απαγορεύεται η επεξεργασία «δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό».

52. Θα πρέπει να τονιστεί ότι σε ορισμένα κράτη μέλη οι ηλεκτρονικές πληρωμές είναι ήδη πανταχού παρούσες και πολλοί άνθρωποι τις προτιμούν στις καθημερινές συναλλαγές τους έναντι των μετρητών. Ταυτόχρονα, οι χρηματοοικονομικές συναλλαγές μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες σχετικά με ένα μεμονωμένο υποκείμενο δεδομένων, συμπεριλαμβανομένων πληροφοριών που σχετίζονται με ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα. Για παράδειγμα, ανάλογα με τις λεπτομέρειες της συναλλαγής, οι δωρεές προς πολιτικά κόμματα ή οργανώσεις, εκκλησίες ή κοινότητες ενδέχεται να αποκαλύπτουν πολιτικά φρονήματα και θρησκευτικές πεποιθήσεις. Η αφαίρεση της ετήσιας συνδρομής μέλους από τον τραπεζικό λογαριασμό ενός προσώπου μπορεί να αποκαλύψει τη συμμετοχή του σε συνδικαλιστική οργάνωση. Δεδομένα προσωπικού χαρακτήρα που αφορούν την υγεία μπορούν να συλλεχθούν από την ανάλυση των ιατρικών λογαριασμών που πληρώνει το υποκείμενο των δεδομένων σε επαγγελματία του τομέα της υγείας (για παράδειγμα, ψυχίατρο). Τέλος, οι πληροφορίες για ορισμένες αγορές μπορεί να αποκαλύψουν πληροφορίες σχετικά με τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό ενός ατόμου. Όπως φαίνεται από τα παραδείγματα αυτά, ακόμη και μεμονωμένες συναλλαγές μπορεί να περιέχουν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα. Επιπλέον, οι υπηρεσίες πληροφοριών λογαριασμού μπορεί να βασίζονται στην κατάρτιση προφίλ, όπως ορίζεται στο άρθρο 4 σημείο 4 του ΓΚΠΔ. Όπως ήδη επισημάνθηκε στις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, όπως εγκρίθηκαν από το ΕΣΠΔ, «η κατάρτιση προφίλ μπορεί να δημιουργήσει δεδομένα ειδικών κατηγοριών διά της συναγωγής από δεδομένα που δεν ανήκουν σε ειδική κατηγορία καθαυτά, αλλά τα οποία καθίστανται δεδομένα ειδικών κατηγοριών όταν συνδυάζονται με άλλα δεδομένα.»[31] Αυτό σημαίνει ότι μέσω του συνόλου των χρηματοοικονομικών συναλλαγών μπορούν να αποκαλυφθούν διάφορα είδη μοντέλων συμπεριφοράς, τα οποία μπορεί να περιλαμβάνουν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα. Ως εκ τούτου, υπάρχουν σημαντικές πιθανότητες ένας πάροχος υπηρεσιών που επεξεργάζεται πληροφορίες σχετικά με χρηματοοικονομικές συναλλαγές υποκειμένων δεδομένων να επεξεργάζεται επίσης ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα.

53. Όσον αφορά τον όρο «ευαίσθητα δεδομένα πληρωμών», το ΕΣΠΔ επισημαίνει τα εξής. Ο ορισμός των ευαίσθητων δεδομένων πληρωμών στην PSD2 διαφέρει σημαντικά από τον τρόπο με τον οποίο χρησιμοποιείται ευρέως ο όρος «ευαίσθητα δεδομένα προσωπικού χαρακτήρα» στο πλαίσιο του ΓΚΠΔ και (του δικαίου) προστασίας των δεδομένων. Ενώ η PSD2 ορίζει τα «ευαίσθητα

[31] Ομάδα εργασίας για την προστασία δεδομένων του άρθρου 29, κατευθυντήριες γραμμές για την αυτοματοποιημένη ατομική λήψη αποφάσεων και την κατάρτιση προφίλ
για τους σκοπούς του κανονισμού 2016/679, WP251rev.01, σ. 18.

δεδομένα πληρωμών» ως «δεδομένα τα οποία συμπεριλαμβάνουν τα εξατομικευμένα διαπιστευτήρια ασφάλειας και τα οποία μπορούν να χρησιμοποιηθούν για διάπραξη απάτης», ο ΓΚΠΔ τονίζει την ανάγκη ειδικής προστασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα τα οποία, βάσει του άρθρου 9 του ΓΚΠΔ, είναι από τη φύση τους ιδιαίτερα ευαίσθητα σε σχέση με τα θεμελιώδη δικαιώματα και τις ελευθερίες, όπως οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα[32]. Στο πλαίσιο αυτό, συνιστάται τουλάχιστον να χαρτογραφηθεί και να κατηγοριοποιηθεί με ακρίβεια το είδος των δεδομένων προσωπικού χαρακτήρα που θα υποβληθούν σε επεξεργασία. Πιθανότατα θα απαιτηθεί εκτίμηση επιπτώσεων σχετικά με την προστασία δεδομένων (ΕΑΠΔ) σύμφωνα με το άρθρο 35 του ΓΚΠΔ, η οποία θα συμβάλει στην εν λόγω διαδικασία χαρτογράφησης. Περισσότερες οδηγίες σχετικά με τις ΕΑΠΔ παρέχονται στο έγγραφο της ομάδας εργασίας του άρθρου 29 «Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 [Κατευθυντήριες γραμμές για την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να οδηγήσει σε υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679], όπως εγκρίθηκε από το ΕΣΠΔ.

5.2 Πιθανές παρεκκλίσεις

54. Η απαγόρευση του άρθρου 9 του ΓΚΠΔ δεν είναι απόλυτη. Ειδικότερα, ενώ οι παρεκκλίσεις του άρθρου 9 παράγραφος 2 στοιχεία β) έως στ) και η) έως ι) του ΓΚΠΔ προδήλως δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της PSD2, θα μπορούσαν να εξεταστούν οι ακόλουθες δύο παρεκκλίσεις του άρθρου 9 παράγραφος 2 του ΓΚΠΔ:

α) Η απαγόρευση δεν εφαρμόζεται αν το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς [άρθρο 9 παράγραφος 2 στοιχείο α) του ΓΚΠΔ].

β) Η απαγόρευση δεν εφαρμόζεται αν η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων [άρθρο 9 παράγραφος 2 στοιχείο ζ) του ΓΚΠΔ].

55. Θα πρέπει να επισημανθεί ότι ο κατάλογος των παρεκκλίσεων στο άρθρο 9 παράγραφος 2 του ΓΚΠΔ είναι εξαντλητικός. Ο πάροχος υπηρεσιών πρέπει να αναγνωρίζει τη δυνατότητα να περιλαμβάνονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα στα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για την παροχή οποιασδήποτε από τις υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής της PSD2. Δεδομένου ότι η απαγόρευση του άρθρου 9 παράγραφος 1 του ΓΚΠΔ εφαρμόζεται στους εν λόγω παρόχους υπηρεσιών, πρέπει να διασφαλίζουν ότι εφαρμόζεται σ’ αυτούς μία από τις εξαιρέσεις του άρθρου 9 παράγραφος 2 του ΓΚΠΔ. Θα πρέπει να τονιστεί ότι, όταν ο πάροχος υπηρεσιών δεν μπορεί να αποδείξει ότι πληρούται μία από τις προϋποθέσεις των παρεκκλίσεων, εφαρμόζεται η απαγόρευση του άρθρου 9 παράγραφος 1.

[32] Για παράδειγμα, στην αιτιολογική σκέψη 10 του ΓΚΠΔ, ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα αναφέρονται ως «ευαίσθητα δεδομένα».

5.3 Ουσιαστικό δημόσιο συμφέρον

56. Οι υπηρεσίες πληρωμών μπορούν να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών για λόγους ουσιαστικού δημόσιου συμφέροντος, αλλά μόνο όταν πληρούνται όλες οι προϋποθέσεις του άρθρου 9 παράγραφος 2 στοιχείο ζ) του ΓΚΠΔ. Αυτό σημαίνει ότι η επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα πρέπει να εξετάζεται στο πλαίσιο ειδικής παρέκκλισης από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ στο δίκαιο της Ένωσης ή κράτους μέλους. Η διάταξη αυτή θα πρέπει να εξετάζει την αναλογικότητα σε σχέση με τον επιδιωκόμενο στόχο της επεξεργασίας και να περιέχει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων. Επιπλέον, η διάταξη αυτή βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους θα πρέπει να σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων. Τέλος, πρέπει επίσης να αποδεικνύεται ότι η επεξεργασία των ειδικών κατηγοριών δεδομένων είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, συμπεριλαμβανομένων συμφερόντων συστημικής σημασίας. Μόνο όταν πληρούνται πλήρως όλες αυτές οι προϋποθέσεις,θα μπορούσε η παρέκκλιση αυτή να εφαρμοστεί σε καθορισμένα είδη υπηρεσιών πληρωμών.

5.4 Ρητή συγκατάθεση

57. Στις περιπτώσεις στις οποίες δεν εφαρμόζεται η παρέκκλιση του άρθρου 9 παράγραφος 2 στοιχείο ζ) του ΓΚΠΔ, η εξασφάλιση ρητής συγκατάθεσης σύμφωνα με τις προϋποθέσεις έγκυρης συγκατάθεσης που προβλέπονται στον ΓΚΠΔ φαίνεται να παραμένει η μόνη δυνατή νόμιμη παρέκκλιση για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα από τους ΤΡΡ. Σύμφωνα με τις κατευθυντήριες γραμμές 5/2020 του ΕΣΠΔ σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679[33]: «Το άρθρο 9 παράγραφος 2 δεν αναγνωρίζει την περίπτωση να είναι η επεξεργασία “απαραίτητη για την εκτέλεση σύμβασης” ως εξαίρεση στη γενική απαγόρευση επεξεργασίας ειδικών κατηγοριών δεδομένων. Επομένως, οι υπεύθυνοι επεξεργασίας και τα κράτη μέλη που αντιμετωπίζουν μια τέτοια περίπτωση θα πρέπει να εξετάζουν τις ειδικές εξαιρέσεις που προβλέπονται στο άρθρο 9 παράγραφος 2 στοιχεία β) έως ι). Όταν οι πάροχοι υπηρεσιών βασίζονται στο άρθρο 9 παράγραφος 2 στοιχείο α) του ΓΚΠΔ, πρέπει να διασφαλίζουν, πριν ξεκινήσουν την επεξεργασία, ότι έχουν λάβει ρητή συγκατάθεση.» Η ρητή συγκατάθεση όπως ορίζεται στο άρθρο 9 παράγραφος 2 στοιχείο α) του ΓΚΠΔ πρέπει να πληροί όλες τις απαιτήσεις του ΓΚΠΔ.

5.5 Απουσία κατάλληλης παρέκκλισης

58. Όπως προαναφέρθηκε, όταν ο πάροχος υπηρεσιών δεν μπορεί να αποδείξει ότι πληρούται μία από τις προϋποθέσεις των παρεκκλίσεων, εφαρμόζεται η απαγόρευση του άρθρου 9 παράγραφος 1. Στην περίπτωση αυτή θα μπορούσαν να τεθούν σε εφαρμογή τεχνικά μέτρα για την πρόληψη της επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, για παράδειγμα με την πρόληψη της επεξεργασίας ορισμένων σημείων δεδομένων. Στο πλαίσιο αυτό, οι πάροχοι υπηρεσιών πληρωμών μπορούν να διερευνήσουν τις τεχνικές δυνατότητες για τον αποκλεισμό ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και να επιτρέψουν επιλεγμένη πρόσβαση που θα εμπόδιζε την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα που σχετίζονται με σιωπηλά μετέχοντες από ΤΡΡ.

[33] Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, ΕΣΠΔ, παράγραφος 99.

6 ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ, ΑΣΦΑΛΕΙΑ, ΔΙΑΦΑΝΕΙΑ, ΛΟΓΟΔΟΣΙΑ ΚΑΙ ΚΑΤΑΡΤΙΣΗ ΠΡΟΦΙΛ

6.1 Ελαχιστοποίηση των δεδομένων και προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

59. Η αρχή της ελαχιστοποίησης των δεδομένων κατοχυρώνεται στο άρθρο 5 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ: «Τα δεδομένα προσωπικού χαρακτήρα […] είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία». Ουσιαστικά, σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, οι υπεύθυνοι επεξεργασίας δεν θα πρέπει να επεξεργάζονται περισσότερα δεδομένα προσωπικού χαρακτήρα από ό, τι είναι αναγκαίο για την επίτευξη του εν λόγω συγκεκριμένου σκοπού. Όπως επισημαίνεται στο κεφάλαιο 2, η ποσότητα και το είδος των δεδομένων προσωπικού χαρακτήρα που απαιτούνται για την παροχή της υπηρεσίας πληρωμών καθορίζονται από τον αντικειμενικό και αμοιβαία κατανοητό συμβατικό σκοπό[34]. Η ελαχιστοποίηση των δεδομένων εφαρμόζεται σε κάθε επεξεργασία (π.χ. κάθε συλλογή ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και αίτηση για δεδομένα προσωπικού χαρακτήρα). Οι κατευθυντήριες γραμμές 4/2019 του ΕΣΠΔ σχετικά με το άρθρο 25 «Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού» (DPbDD) αναφέρουν ότι «οι εκτελούντες την επεξεργασία και οι πάροχοι τεχνολογίας αναγνωρίζονται επίσης ως βασικοί παράγοντες διευκόλυνσης της DPbDD, θα πρέπει επίσης να γνωρίζουν ότι οι υπεύθυνοι επεξεργασίας υποχρεούνται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μόνο με συστήματα και τεχνολογίες με ενσωματωμένη προστασία δεδομένων[35]».

60. Το άρθρο 25 του ΓΚΠΔ περιλαμβάνει τις υποχρεώσεις για την εφαρμογή της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Οι υποχρεώσεις αυτές έχουν ιδιαίτερη σημασία για την αρχή της ελαχιστοποίησης των δεδομένων. Το εν λόγω άρθρο ορίζει ότι οι υπεύθυνοι επεξεργασίας εφαρμόζουν αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του ΓΚΠΔ και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων. Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Τα μέτρα αυτά μπορούν να περιλαμβάνουν την κρυπτογράφηση, τη ψευδωνυμοποίηση και άλλα τεχνικά μέτρα.

61. Όταν εφαρμόζεται η υποχρέωση του άρθρου 25 του ΓΚΠΔ, τα στοιχεία που πρέπει να λαμβάνονται υπόψη είναι οι τελευταίες εξελίξεις, το κόστος εφαρμογής και η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας, καθώς και οι κίνδυνοι διαφορετικής πιθανότητας επέλευσης και σοβαρότητας κινδύνων που ενέχει η επεξεργασία για τα δικαιώματα

[34] Κατευθυντήριες γραμμές 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, ΕΣΠΔ, παράγραφος 32.
[35] Κατευθυντήριες γραμμές 4/2019 σχετικά με το άρθρο 25 «Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού», σ. 29.

και τις ελευθερίες των φυσικών προσώπων. Περαιτέρω διευκρινίσεις σχετικά με την εν λόγω υποχρέωση παρέχονται στις προαναφερθείσες κατευθυντήριες γραμμές 4/2019 του ΕΣΠΔ σχετικά με το άρθρο 25 «Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού».

6.2 Μέτρα ελαχιστοποίησης των δεδομένων

62. Οι TPP που έχουν πρόσβαση σε δεδομένα λογαριασμού πληρωμών για την παροχή των ζητούμενων υπηρεσιών πρέπει επίσης να λαμβάνουν υπόψη την αρχή της ελαχιστοποίησης των δεδομένων και πρέπει να συλλέγουν μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για την παροχή των συγκεκριμένων υπηρεσιών πληρωμών που ζητούνται από τον χρήστη υπηρεσιών πληρωμών. Κατ' αρχήν, η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα θα πρέπει να περιορίζεται στο αναγκαίο για την παροχή υπηρεσιών πληρωμών. Όπως καταδείχθηκε στο κεφάλαιο 2, η PSD2 απαιτεί από τους ASPSP να ανταλλάσσουν πληροφορίες σχετικά με τον χρήστη υπηρεσιών πληρωμών κατόπιν αιτήματος του χρήστη υπηρεσιών πληρωμών, όταν ο χρήστης υπηρεσιών πληρωμών επιθυμεί να χρησιμοποιήσει υπηρεσία εκκίνησης πληρωμών ή υπηρεσία πληροφοριών λογαριασμού.

63. Όταν δεν είναι όλα τα δεδομένα λογαριασμού πληρωμών απαραίτητα για την εκτέλεση της σύμβασης, πριν από τη συλλογή των δεδομένων ο AISP θα πρέπει να επιλέγει τις σχετικές κατηγορίες δεδομένων. Για παράδειγμα, οι κατηγορίες δεδομένων που μπορεί να μην είναι απαραίτητες μπορεί να περιλαμβάνουν την ταυτότητα του σιωπηλά μετέχοντος και τα χαρακτηριστικά της συναλλαγής. Επίσης, εκτός αν απαιτείται από το δίκαιο κράτους μέλους ή το δίκαιο της ΕΕ, ενδέχεται να μη χρειάζεται να εμφανίζεται ο IBAN του τραπεζικού λογαριασμού του σιωπηλά μετέχοντος.

64. Στο πλαίσιο αυτό, θα μπορούσε να εξεταστεί το ενδεχόμενο εφαρμογής τεχνικών μέτρων που επιτρέπουν ή υποστηρίζουν τους TPP στην υποχρέωσή τους να έχουν πρόσβαση και να ανακτούν μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για την παροχή των υπηρεσιών τους, στο πλαίσιο της εφαρμογής κατάλληλων πολιτικών προστασίας των δεδομένων, σύμφωνα με το άρθρο 24 παράγραφος 2 του ΓΚΠΔ. Στο πλαίσιο αυτό, το ΕΣΠΔ συνιστά τη χρήση ψηφιακών εργαλείων για την υποστήριξη των AISP στην υποχρέωσή τους να συλλέγουν μόνο δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Για παράδειγμα, όταν ένας πάροχος υπηρεσιών δεν χρειάζεται τα χαρακτηριστικά της συναλλαγής (στο πεδίο περιγραφής των αρχείων συναλλαγών) για την παροχή της υπηρεσίας του, ένα ψηφιακό εργαλείο επιλογής θα μπορούσε να λειτουργήσει ως μέσο εξαίρεσης από τους TPP αυτού του πεδίου από τις συνολικές πράξεις επεξεργασίας του TPP.

Παράδειγμα 2:

Η HappyPayments, ο πάροχος υπηρεσιών πληροφοριών λογαριασμού του παραδείγματος 1, επιθυμεί να διασφαλίσει ότι επεξεργάζεται μόνο τα δεδομένα προσωπικού χαρακτήρα που περιέχονται σε λογαριασμό πληρωμών για τα οποία ενδιαφέρονται οι χρήστες του. Η αναζήτηση πρόσβασης σε περισσότερα δεδομένα λογαριασμών πληρωμών δεν θα ήταν απαραίτητη για την παροχή της υπηρεσίας. Ως εκ τούτου, δίνει τη δυνατότητα στους χρήστες να επιλέγουν τα συγκεκριμένα είδη πληροφοριών για τα οποία ενδιαφέρονται.

Ο χρήστης Α επιθυμεί να συμβουλευτεί την επισκόπηση των δαπανών του για τους δύο τελευταίους μήνες. Ως εκ τούτου, ζητεί τους δύο τραπεζικούς λογαριασμούς του, οι οποίοι τηρούνται από δύο διαφορετικούς ASPSP, τις πληροφορίες για όλες τις συναλλαγές των τελευταίων δύο μηνών, το ποσό της συναλλαγής, την ημερομηνία εκτέλεσης και το όνομα του αποδέκτη, και επιλέγει τα αντίστοιχα τετραγωνίδια στη διεπαφή χρήστη της HappyPayments.

Στη συνέχεια, η HappyPayments ζητεί από τους αντίστοιχους ASPSP μόνο τις πληροφορίες που αντιστοιχούν στα πεδία που έχει ορίσει ο χρήστης Α και μόνο για την περίοδο των δύο τελευταίων μηνών. Πληροφορίες όπως η «κοινοποίηση» της μεταφοράς ή ακόμη και ο IBAN δεν ζητούνται, καθώς ο χρήστης Α δεν ζήτησε τις πληροφορίες αυτές.

Για να δώσουν τη δυνατότητα στη HappyPayments να συμμορφωθεί με τις υποχρεώσεις ελαχιστοποίησης των δεδομένων, οι ASPSP επιτρέπουν στη HappyPayments να ζητήσει συγκεκριμένα πεδία για μια σειρά ημερομηνιών.

65. Θα πρέπει επίσης να σημειωθεί εν προκειμένω ότι, σύμφωνα με την PSD2, οι ASPSP επιτρέπεται να παρέχουν πρόσβαση μόνο σε πληροφορίες λογαριασμού πληρωμών. Δεν υπάρχει νομική βάση στο πλαίσιο της PSD2 για την παροχή πρόσβασης σε δεδομένα προσωπικού χαρακτήρα που περιέχονται σε άλλους λογαριασμούς, όπως λογαριασμοί ταμιευτηρίου, ενυπόθηκων δανείων ή επενδύσεων. Ως εκ τούτου, σύμφωνα με την PSD2, πρέπει να εφαρμοστούν τεχνικά μέτρα για να εξασφαλιστεί ότι η πρόσβαση περιορίζεται στις απαραίτητες πληροφορίες λογαριασμού πληρωμών.

66. Εκτός από τη συλλογή όσο το δυνατό λιγότερων δεδομένων, ο πάροχος υπηρεσιών πρέπει επίσης να εφαρμόζει περιορισμένες περιόδους διατήρησης. Ο πάροχος υπηρεσιών δεν θα πρέπει να αποθηκεύει τα δεδομένα προσωπικού χαρακτήρα για χρονικό διάστημα μεγαλύτερο από το αναγκαίο σε σχέση με τους σκοπούς που έχει ζητήσει ο χρήστης υπηρεσιών πληρωμών.

67. Αν η σύμβαση μεταξύ του υποκειμένου των δεδομένων και του AISP απαιτεί τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτους, μπορούν να διαβιβαστούν μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για την εκτέλεση της σύμβασης. Τα υποκείμενα των δεδομένων θα πρέπει επίσης να ενημερώνονται ειδικά για τη διαβίβαση και τα δεδομένα προσωπικού χαρακτήρα που πρόκειται να διαβιβαστούν στον εν λόγω τρίτο.

6.3 Ασφάλεια

68. Το ΕΣΠΔ έχει ήδη επισημάνει ότι η παραβίαση των χρηματοοικονομικών δεδομένων προσωπικού χαρακτήρα «*συνεπάγεται σαφώς σοβαρές επιπτώσεις στην καθημερινή ζωή του υποκειμένου των δεδομένων*» και παραθέτει ως παράδειγμα τους κινδύνους απάτης στον τομέα των πληρωμών[36].

69. Όταν η παραβίαση δεδομένων αφορά χρηματοοικονομικά δεδομένα, το υποκείμενο των δεδομένων μπορεί να εκτεθεί σε σημαντικούς κινδύνους. Ανάλογα με τις πληροφορίες που διαρρέουν, τα υποκείμενα των δεδομένων ενδέχεται να εκτίθενται σε κίνδυνο κλοπής ταυτότητας, κλοπής κεφαλαίων από τους λογαριασμούς τους και άλλων περιουσιακών στοιχείων. Επιπλέον, υπάρχει το ενδεχόμενο η έκθεση των δεδομένων συναλλαγών να συνδέεται με σημαντικούς κινδύνους για την ιδιωτική ζωή, καθώς τα δεδομένα συναλλαγών μπορεί να περιέχουν αναφορές σε όλες τις πτυχές της ιδιωτικής ζωής του υποκειμένου των δεδομένων. Ταυτόχρονα, τα χρηματοοικονομικά δεδομένα είναι προφανώς πολύτιμα για τους εγκληματίες και, ως εκ τούτου, αποτελούν ελκυστικό στόχο.

70. Ως υπεύθυνοι επεξεργασίας, οι πάροχοι υπηρεσιών πληρωμών υποχρεούνται να λαμβάνουν κατάλληλα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων (άρθρο 24 παράγραφος 1 του ΓΚΠΔ). Όσο υψηλότεροι είναι οι κίνδυνοι που συνδέονται με τη δραστηριότητα επεξεργασίας που ασκεί ο υπεύθυνος επεξεργασίας τόσο υψηλότερα είναι τα πρότυπα ασφαλείας που πρέπει να εφαρμόζονται. Δεδομένου ότι η

[36] Κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να οδηγήσει σε υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679, WP248 rev.01 — εγκρίθηκαν από το ΕΣΠΔ.

επεξεργασία χρηματοοικονομικών δεδομένων συνδέεται με διάφορους σοβαρούς κινδύνους, τα μέτρα ασφαλείας θα πρέπει να είναι αντιστοίχως ενισχυμένα.

71. Οι πάροχοι υπηρεσιών θα πρέπει να τηρούν υψηλά πρότυπα, συμπεριλαμβανομένων μηχανισμών αυστηρής εξακρίβωσης της ταυτότητας του πελάτη και υψηλών προτύπων ασφαλείας για τον τεχνικό εξοπλισμό[37]. Άλλες διαδικασίες, όπως ο έλεγχος των εκτελούντων την επεξεργασία για τα πρότυπα ασφαλείας και οι διαδικασίες εφαρμογής κατά της μη εξουσιοδοτημένης πρόσβασης, είναι επίσης σημαντικές.

6.4 Διαφάνεια και λογοδοσία

72. Η διαφάνεια και η λογοδοσία αποτελούν δύο θεμελιώδεις αρχές του ΓΚΠΔ.

73. Όσον αφορά τη διαφάνεια [άρθρο 5 παράγραφος 1 στοιχείο α) του ΓΚΠΔ], το άρθρο 12 του ΓΚΠΔ ορίζει ότι οι υπεύθυνοι επεξεργασίας λαμβάνουν τα κατάλληλα μέτρα για να παρέχουν κάθε πληροφορία που αναφέρεται στα άρθρα 13 και 14 του ΓΚΠΔ. Επιπλέον, απαιτεί οι πληροφορίες ή οι ανακοινώσεις σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα να είναι συνοπτικές, διαφανείς, κατανοητές και εύκολα προσβάσιμες. Οι πληροφορίες πρέπει να παρέχονται γραπτώς «ή με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς». Οι «κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679» της ομάδας εργασίας του άρθρου 29, όπως εγκρίθηκαν από το ΕΣΠΔ, παρέχουν ειδική καθοδήγηση για τη συμμόρφωση με την αρχή της διαφάνειας σε ψηφιακά περιβάλλοντα.

74. Σύμφωνα με τις προαναφερθείσες κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, το άρθρο 11 του ΓΚΠΔ θα πρέπει να ερμηνεύεται ως ένας τρόπος επιβολής ουσιαστικής ελαχιστοποίησης των δεδομένων χωρίς να παρεμποδίζεται η άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, καθώς και ότι η άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων θα πρέπει να γίνεται με τη βοήθεια πρόσθετων πληροφοριών που παρέχει το υποκείμενο των δεδομένων. Ενδέχεται να υπάρχουν περιπτώσεις στις οποίες ο υπεύθυνος επεξεργασίας δεδομένων επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για τα οποία δεν απαιτείται η ταυτοποίηση του υποκειμένου των δεδομένων (για παράδειγμα με ψευδωνυμοποιημένα δεδομένα). Στις περιπτώσεις αυτές, το άρθρο 11 παράγραφος 1 μπορεί επίσης να είναι συναφές, καθώς ορίζει ότι ο υπεύθυνος επεξεργασίας δεδομένων δεν υποχρεούται να διατηρεί, να αποκτά ή να επεξεργάζεται συμπληρωματικές πληροφορίες για την εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων αποκλειστικά και μόνο για τον σκοπό της συμμόρφωσης προς τον ΓΚΠΔ.

75. Όσον αφορά τις υπηρεσίες στο πλαίσιο της PSD2, το άρθρο 13 του ΓΚΠΔ εφαρμόζεται για τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται από το υποκείμενο των δεδομένων και το άρθρο 14 εφαρμόζεται όταν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεχθεί από το υποκείμενο των δεδομένων.

76. Ειδικότερα, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται σχετικά με την περίοδο αποθήκευσης των δεδομένων προσωπικού χαρακτήρα ή, αν αυτό δεν είναι εφικτό, σχετικά με τα κριτήρια που χρησιμοποιούνται για τον καθορισμό της εν λόγω περιόδου και, κατά περίπτωση, σχετικά με τα έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή δυνητικός τρίτος. Όταν η επεξεργασία βασίζεται σε συγκατάθεση όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο α) του ΓΚΠΔ ή σε ρητή συγκατάθεση όπως αναφέρεται στο άρθρο 9 παράγραφος 2

[37] Βλ. ΡΤΠ.

στοιχείο α) του ΓΚΠΔ, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται σχετικά με την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε.

77. Ο υπεύθυνος επεξεργασίας παρέχει τις πληροφορίες στο υποκείμενο των δεδομένων, λαμβάνοντας υπόψη τις ειδικές περιστάσεις υπό τις οποίες τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία. Εάν τα δεδομένα προσωπικού χαρακτήρα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο των δεδομένων[38], κάτι που πιθανόν να συμβεί στην περίπτωση των AISP, οι πληροφορίες πρέπει να παρέχονται το αργότερο κατά την πρώτη επικοινωνία με το εν λόγω υποκείμενο των δεδομένων. Εάν τα δεδομένα προσωπικού χαρακτήρα πρόκειται να γνωστοποιηθούν σε άλλον αποδέκτη, οι πληροφορίες πρέπει να παρέχονται το αργότερο όταν τα δεδομένα προσωπικού χαρακτήρα γνωστοποιούνται για πρώτη φορά.

78. Όσον αφορά τις επιγραμμικές υπηρεσίες πληρωμών, οι προαναφερθείσες κατευθυντήριες γραμμές διευκρινίζουν ότι οι υπεύθυνοι επεξεργασίας δεδομένων μπορούν να ακολουθούν μια προσέγγιση πολλαπλών επιπέδων όταν επιλέγουν να χρησιμοποιήσουν έναν συνδυασμό μεθόδων για την εξασφάλιση διαφάνειας. Συνιστάται ειδικότερα οι δηλώσεις πολλαπλών επιπέδων για την προστασία της ιδιωτικής ζωής να χρησιμοποιούνται για την παραπομπή στις διάφορες κατηγορίες πληροφοριών που πρέπει να παρέχονται στο υποκείμενο των δεδομένων, αντί όλες αυτές οι πληροφορίες να εμφανίζονται σε μία μόνο δήλωση στην οθόνη, ώστε να αποφεύγεται η δημιουργία κούρασης λόγω της παροχής πληροφοριών και ταυτόχρονα να διασφαλίζεται η αποτελεσματικότητα των πληροφοριών.

79. Οι προαναφερθείσες κατευθυντήριες γραμμές διευκρινίζουν επίσης ότι οι υπεύθυνοι επεξεργασίας μπορούν να επιλέξουν να χρησιμοποιήσουν πρόσθετα εργαλεία για την παροχή πληροφοριών στο υποκείμενο των δεδομένων, όπως πίνακες για την προστασία της ιδιωτικής ζωής. Ο πίνακας για την προστασία της ιδιωτικής ζωής είναι ένα ενιαίο σημείο από το οποίο τα υποκείμενα των δεδομένων μπορούν να προβάλλουν «πληροφορίες σχετικά με την προστασία της ιδιωτικής ζωής» και να διαχειρίζονται τις σχετικές προτιμήσεις τους επιτρέποντας ή εμποδίζοντας τη χρήση των δεδομένων τους με ορισμένους τρόπους από τον εν λόγω υπεύθυνο επεξεργασίας[39]. Ο πίνακας για την προστασία της ιδιωτικής ζωής θα μπορούσε να παρέχει επισκόπηση των TPP που έχουν λάβει τη ρητή συγκατάθεση των υποκειμένων των δεδομένων και θα μπορούσε επίσης να παρέχει σχετικές πληροφορίες σχετικά με τη φύση και την ποσότητα των δεδομένων προσωπικού χαρακτήρα στα οποία έχουν πρόσβαση οι TPP. Κατ' αρχήν, ο ASPSP μπορεί να προσφέρει στον χρήστη τη δυνατότητα να ανακαλέσει συγκεκριμένη ρητή συγκατάθεση[40] βάσει της PSD2 μέσω της επισκόπησης, γεγονός που θα είχε ως αποτέλεσμα την άρνηση πρόσβασης στους λογαριασμούς πληρωμών του σε έναν ή περισσότερους TPP. Ο χρήστης

[38] Άρθρο 14 παράγραφος 3 στοιχείο β) του ΓΚΠΔ.

[39] Σύμφωνα με τις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679 — που εγκρίθηκαν από το ΕΣΠΔ, οι πίνακες για την προστασία της ιδιωτικής ζωής είναι ιδιαίτερα χρήσιμοι όταν η ίδια υπηρεσία χρησιμοποιείται από τα υποκείμενα των δεδομένων σε ποικίλες συσκευές, καθώς τους παρέχουν πρόσβαση στα δεδομένα προσωπικού τους χαρακτήρα και τους επιτρέπουν να τα ελέγχουν ανεξάρτητα από τον τρόπο με τον οποίο χρησιμοποιούν την υπηρεσία. Η δυνατότητα που παρέχεται στα υποκείμενα των δεδομένων να προσαρμόζουν τις ρυθμίσεις τους για την προστασία της ιδιωτικής ζωής μέσω ενός πίνακα για την προστασία της ιδιωτικής ζωής μπορεί επίσης να διευκολύνει την εξατομίκευση μιας δήλωσης για την προστασία της ιδιωτικής ζωής ώστε να αντανακλά μόνο τα είδη επεξεργασίας που πραγματοποιούνται για το συγκεκριμένο υποκείμενο δεδομένων.

[40] Βλ. για παράδειγμα τη «ρητή συναίνεση» που αναφέρεται στο άρθρο 67 παράγραφος 2 στοιχείο α) της PSD2.

θα μπορούσε επίσης να ζητήσει από έναν ASPSP να αρνηθεί την πρόσβαση στον ή στους λογαριασμούς πληρωμών του σε έναν ή περισσότερους συγκεκριμένους TPP[41], δεδομένου ότι ο χρήστης έχει το δικαίωμα να (μη) χρησιμοποιήσει μια υπηρεσία πληροφοριών λογαριασμού. Αν οι πίνακες για την προστασία της ιδιωτικής ζωής χρησιμοποιούνται για την παροχή ή την ανάκληση ρητής συγκατάθεσης, θα πρέπει να σχεδιάζονται και να εφαρμόζονται νόμιμα και ιδιαίτερα κατά τρόπο που να αποτρέπεται η δημιουργία εμποδίων στο δικαίωμα των TPP να παρέχουν υπηρεσίες σύμφωνα με την PSD2. Στο πλαίσιο αυτό και σύμφωνα με τις εφαρμοστέες διατάξεις της PSD2, ένας TPP έχει τη δυνατότητα να λάβει εκ νέου ρητή συγκατάθεση από τον χρήστη μετά την ανάκληση της εν λόγω συγκατάθεσης.

80. Σύμφωνα με τις αρχές λογοδοσίας, ο υπεύθυνος επεξεργασίας πρέπει να καθορίζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ, ιδιαίτερα με τις βασικές αρχές προστασίας δεδομένων που προβλέπονται στο άρθρο 5 παράγραφος 1. Τα εν λόγω μέτρα θα πρέπει να λαμβάνουν υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας και τον κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, και πρέπει να επανεξετάζονται και να επικαιροποιούνται όταν κρίνεται απαραίτητο[42].

6.5 Κατάρτιση προφίλ

81. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από παρόχους υπηρεσιών πληρωμών μπορεί να περιλαμβάνει «κατάρτιση προφίλ», όπως αναφέρεται στο άρθρο 4 σημείο 4 του ΓΚΠΔ. Για παράδειγμα, οι AISP, για να αξιολογήσουν ορισμένες προσωπικές πτυχές που αφορούν ένα φυσικό πρόσωπο, θα μπορούσαν να βασιστούν στην αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Θα μπορούσε να αξιολογηθεί η προσωπική οικονομική κατάσταση ενός υποκειμένου δεδομένων, ανάλογα με τα συγκεκριμένα χαρακτηριστικά της υπηρεσίας. Οι υπηρεσίες πληροφοριών λογαριασμού, που πρέπει να παρέχονται κατόπιν αιτήματος των χρηστών, μπορεί να περιλαμβάνουν εκτενή αξιολόγηση των δεδομένων προσωπικού χαρακτήρα που περιέχονται σε λογαριασμούς πληρωμών.

82. Ο υπεύθυνος επεξεργασίας πρέπει επίσης να ενημερώνει σαφώς το υποκείμενο των δεδομένων σχετικά με την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας πρέπει να παρέχει σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της επεξεργασίας αυτής για το υποκείμενο των δεδομένων [άρθρο 13 παράγραφος 2 στοιχείο στ) και άρθρο 14 παράγραφος 2 στοιχείο ζ) και αιτιολογική σκέψη 60][43]. Ομοίως, σύμφωνα με το άρθρο 15 του ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητεί και να λαμβάνει πληροφορίες από τον υπεύθυνο επεξεργασίας σχετικά με την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένων της κατάρτισης προφίλ, της λογικής που ακολουθείται και των συνεπειών για το υποκείμενο των δεδομένων, και, σε ορισμένες περιπτώσεις, το δικαίωμα να αντιτάσσεται στην κατάρτιση προφίλ, ανεξάρτητα από το αν λαμβάνει χώρα διαδικασία αποκλειστικά αυτοματοποιημένης ατομικής λήψης αποφάσεων βάσει κατάρτισης προφίλ[44].

[41] Βλ. επίσης EBA/OP/2020/10, παράγραφος 45.
[42] Άρθρο 5 παράγραφος 2 και άρθρο 24 του ΓΚΠΔ.
[43] Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, WP 260 rev.01 — εγκρίθηκαν από το ΕΣΠΔ.
[44] Κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, WP251rev.01.

83. Επιπλέον, αυτό που έχει επίσης σημασία στο πλαίσιο αυτό είναι το δικαίωμα του υποκειμένου των δεδομένων να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζουν σημαντικά με παρόμοιο τρόπο, όπως προβλέπεται στο άρθρο 22 του ΓΚΠΔ. Ο κανόνας αυτός περιλαμβάνει επίσης, σε ορισμένες περιπτώσεις, την ανάγκη οι υπεύθυνοι επεξεργασίας δεδομένων να εφαρμόζουν κατάλληλα μέτρα για την προστασία των δικαιωμάτων του υποκειμένου των δεδομένων, όπως η ειδική ενημέρωση του υποκειμένου των δεδομένων, το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης κατά τη λήψη αποφάσεων, έκφρασης άποψης και αμφισβήτησης της απόφασης. Όπως αναφέρεται επίσης στην αιτιολογική σκέψη 71 του ΓΚΠΔ, αυτό σημαίνει, μεταξύ άλλων, ότι τα υποκείμενα των δεδομένων έχουν το δικαίωμα να μην υπόκεινται σε απόφαση, όπως η αυτόματη άρνηση ηλεκτρονικής αίτησης πίστωσης χωρίς ανθρώπινη παρέμβαση[45].

84. Η αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που περιλαμβάνει ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο βάσει των ακόλουθων σωρευτικών προϋποθέσεων του άρθρου 22 παράγραφος 4 του ΓΚΠΔ:

- υφίσταται εφαρμοστέα εξαίρεση από το άρθρο 22 παράγραφος 2·
- και εφαρμόζεται το άρθρο 9 παράγραφος 2 στοιχεία α) ή ζ) του ΓΚΠΔ. Και στις δύο ανωτέρω περιπτώσεις, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων[46].

85. Θα πρέπει επίσης να τηρούνται οι απαιτήσεις για περαιτέρω επεξεργασία, όπως αναφέρονται στις παρούσες κατευθυντήριες γραμμές. Οι διευκρινίσεις και οι οδηγίες σχετικά με την αυτοματοποιημένη ατομική λήψη αποφάσεων και την κατάρτιση προφίλ που παρέχονται από τις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για την αυτοματοποιημένη ατομική λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, όπως εγκρίθηκαν από το ΕΣΠΔ, είναι πλήρως συναφείς στο πλαίσιο των υπηρεσιών πληρωμών και, ως εκ τούτου, θα πρέπει να ληφθούν δεόντως υπόψη.

Για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η Πρόεδρος

(Andrea Jelinek)

[45] Αιτιολογική σκέψη 71 του ΓΚΠΔ.

[46] Κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, Wp251rev.01, σ. 24.