ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΕΚΤΕΛΕΣΗ ΤΡΑΠΕΖΙΚΩΝ ΕΡΓΑΣΙΩΝ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΟΝ ΕΛΛΗΝΙΚΟ ΤΡΑΠΕΖΙΚΟ ΤΟΜΕΑ

Διπλωματική Εργασία

της

Μήτια Αικατερίνης

Θεσσαλονίκη, 02/2021

ΕΚΤΕΛΕΣΗ ΤΡΑΠΕΖΙΚΩΝ ΕΡΓΑΣΙΩΝ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΟΝ ΕΛΛΗΝΙΚΟ ΤΡΑΠΕΖΙΚΟ ΤΟΜΕΑ

Μήτια Αικατερίνη

Πτυχίο Νομικής Σχολής, Α.Π.Θ. ,2005

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες Καθηγητές
Κομνηνός Κόμνιος
Χρήστος Μαστροκώστας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

....

Αικατερίνη Μήτια

Περίληψη

Με τη παρούσα Διπλωματική Εργασία επιχειρείται μέσω της μελέτης των αποφάσεων, γνωμοδοτήσεων, οδηγιών και συστάσεων της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σχετικά με τη δραστηριότητα των τραπεζικών ιδρυμάτων συνδυαστικά με την με την μελέτη των διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 να ταξινομηθούν οι πληροφορίες σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα ανά επιμέρους τραπεζική δραστηριότητα. Στη συνέχεια, οι πληροφορίες θα αναλυθούν και θα αξιολογηθούν προκειμένου να αναδειχθούν τα πρακτικά βήματα που θα πρέπει να ακολουθήσει ένας πιστωτικός οργανισμός ως υπεύθυνος επεξεργασίας για την ορθή εφαρμογή της νομοθεσίας περί προστασίας των προσωπικών δεδομένων. Ιδιαίτερη έμφαση θα δοθεί στο ρόλο του Υπεύθυνου Προστασίας Δεδομένων ενός πιστωτικού Ιδρύματος, και στις επιμέρους πτυχές του καθήκοντος για παρακολούθηση της συμμόρφωσης.

Θα αναλυθούν εκτενώς σε δομημένες ενότητες τα παρακάτω θέματα:

Αρχικά, θα παρατεθούν τα νομοθετήματα σχετικά με την προστασία των προσωπικών δεδομένων στον τραπεζικό τομέα, σε εθνικό αλλά και ενωσιακό επίπεδο (PSD2, GDPR), οι σχετικές αποφάσεις και οι γνωμοδοτήσεις της Αρχής Προστασίας Προσωπικών Δεδομένων.

Στη συνέχεια θα εξεταστούν τα θέματα που προκύπτουν ανά επιμέρους τραπεζική δραστηριότητα, ως προς την εναρμόνιση με τις βασικές αρχές επεξεργασίας, με τα στοιχεία προς επεξεργασία, τους σκοπούς της επεξεργασίας, τα πρόσωπα στα οποία θα μπορούν να γνωστοποιηθούν τα προσωπικά δεδομένα. Επίσης, ζητήματα σχετικά με τη διασυνοριακή διαβίβαση δεδομένων, το χρονικό διάστημα τήρησης δεδομένων, τα δικαιώματα των πελατών των τραπεζικών ιδρυμάτων και τις υποχρεώσεις της τράπεζας. Ακόμη, ειδικά θέματα που προκύπτουν από τα κλειστά κυκλώματα τηλεόρασης και καταγραφής συνδιαλέξεων καθώς και κατά την παροχή Ηλεκτρονικών Υπηρεσιών.

Στην τρίτη ενότητα εξετάζεται ο ρόλος του Υπεύθυνου Προστασίας Δεδομένων ενός χρηματοπιστωτικού Οργανισμού. Αναλύεται ο θεσμός του Υπευθύνου Προστασίας Δεδομένων, ο ρόλος του, τα ζητήματα της καταστατικής θέσης του Υπευθύνου Προστασίας Προσωπικών δεδομένων στον οργανισμό που υπηρετεί (ανεξαρτησία και μέτρο ευθύνης). Εξετάζονται τα απαιτούμενα προσόντα, η θέση και τα καθήκοντα του (καθήκον λογοδοσίας, καθήκον τήρησης απορρήτου και εμπιστευτικότητας, συμβουλευτικός και ενημερωτικός ρόλος). Οι αρμοδιότητες του Υπευθύνου Προστασίας Δεδομένων, με ιδιαίτερη κι εκτενή ανάλυση της αρμοδιότητας που αφορά στην παρακολούθηση της συμμόρφωσης προς τον Γενικό Κανονισμό Προστασίας Δεδομένων, καθώς και των αρμοδιοτήτων σχετικά με τη διαβούλευση με την Αρχή Προστασίας δεδομένων προσωπικού χαρακτήρα και

σχετικά με την εκτίμηση αντικτύπου.
Τέλος, θα παρατεθούν συμπερασματικές κρίσεις σχετικά με τις δράσεις στις οποίες θα πρέπει να προβεί ένας χρηματοπιστωτικός οργανισμός ως υπεύθυνος επεξεργασίας για την ορθή εφαρμογή της νομοθεσίας περί προστασίας των προσωπικών δεδομένων.

Λέξεις Κλειδιά: προσωπικά δεδομένα, προστασία προσωπικών δεδομένων, Υπεύθυνος Προστασίας Δεδομένων (Υ.Π.Δ.), προσωπικά δεδομένα στον τραπεζικό χώρο, Γενικός Κανονισμός Προστασίας Δεδομένων (Γ.Κ.Π.Δ.), Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.)

Abstract

This Diploma Thesis will attempt to classify the information about the personal data processing on any stage of banking activity, through the study of the Hellenic Data Protection Authority (DPA) Decisions, Opinions, Directives, Guidelines, Recommendations that are relevant to the banking activity in combination with the study of the General Regulation of Data Protection of the EU. 679/2016 (G.D.P.R.). The information will be analyzed and evaluated in order to highlight the processes that a bank should practice as a controller for the compliance with the Data Protection legislation and the proper G.D.P.R. implementation. Particular emphasis will be laid on the role of a bank's Data Protection Officer, and especially on the task to monitor and promote the controller's compliance.

The following topics will be analyzed in detail in structured sections:

At the first chapter a series of national and European Union legislation on Data Protection in the banking sector will be mentioned (PSD2, GDPR), as well as relevant Decisions and Recommendations of the Hellenic Data Protection Authority (DPA).

At the second chapter the data protection issues that arise during the stages of banking activity will be examined in terms of harmonization with the key principles of Data Processing, with the the concept of Personal Data, with the Rules on lawful processing, with the users of the Personal Data. Additionally, issues related to transborder data flows, to the time limitation for storing personal data, to the rights of data subjects/ bank's customers and to the obligations of the bank as Controller will be examined. Furthermore, issues related to C.C.T.V, conversation recording and issues that arise during the provision of electronic Services will be examined.

At the third chapter the role of the Data Protection Officer (D.P.O) in a bank will be examined. The D.P.O. institution, the role of a D.P.O., the position in the Organization he serves (independence and responsibility) will be analyzed. In addition, the required qualification, position and duties (loyalty and accountability duty, confidentiality and secrecy duty, duty to inform and advise) will be examined. Furthermore, the tasks of the D.P.O will be studied, including the task of monitoring the G.D.P.R compliance, as well as the task to cooperate with the supervisory authority (Hellenic Data Protection Authority) and the tasks associated with data protection impact assessment.

This Thesis concludes the presentation of the actions that should be taken by a bank in order to achieve the proper data protection legislation implementation and G.D.P.R. compliance.

Keywords: personal data, personal data protection, Data protection Officer (D.P.O.), personal data in the banking sector, General Regulation of Data Protection of the EU.679/2016 (G.D.P.R.), Hellenic Data Protection Authority

(D.P.A)

Πρόλογος

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 θεωρείται ορόσημο στη νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα. Προκειμένου να επιτύχουν τη συμμόρφωση, τα τραπεζικά ιδρύματα χρειάζεται να αναπτύξουν σαφές σχέδιο και στρατηγική, ώστε να εφαρμόζεται η νομοθεσία. Η τράπεζα ως υπεύθυνος επεξεργασίας πρέπει να αποδεικνύει τη συμμόρφωση, ειδάλλως θα αντιμετωπίσει την επιβολή προστίμων σημαντικού ύψους ή ακόμη και περιορισμών στην πρόσβαση στις διεθνείς αγορές, για πολύ σοβαρές παραβιάσεις. Στον αντίποδα εάν μία Τράπεζα μετασχηματιστεί ριζικά, ώστε να συμπεριλάβει πρόβλεψη για εφαρμογή των βασικών Αρχών προστασίας προσωπικών δεδομένων από την έναρξη του σχεδιασμού των συστημάτων αντί να επιχειρήσει να τροποποιήσει τα ήδη υπάρχοντα, και εάν αυτός ο μετασχηματισμός εφαρμοστεί με διαλειτουργικότητα[1] σε όλο το εύρος των υπηρεσιών και των λειτουργιών της (και όχι μόνο στο νομικό τμήμα της) θα αποκομίσει επιπλέον οφέλη, όπως η αριστεία, η καλή φήμη για την ασφάλεια και την ακεραιότητα που αποτελεί ανταγωνιστικό πλεονέκτημα καθώς και περεταίρω ευκαιρίες για ομαλή ψηφιοποίηση του χρηματοπιστωτικού Οργανισμού. Πλέον οι Τράπεζες στρέφονται σε μία πελατοκεντρική πολιτική, που διευκολύνει τη διαχείριση του πελατολογίου αλλά και των κινδύνων, με καλά δομημένες βάσεις δεδομένων και νεα λειτουργικά συστήματα (fintech και ψηφιακές λύσεις) που αλληλεπιδρούν αποτελεσματικά μεταξύ τους, ώστε να αποφεύγονται οι διπλές διαδικασίες, τα δεδομένα να ρέουν πιο ομαλά, να αυξάνεται η αποδοτικότητα των εργαζομένων και να μειώνεται το κόστος. [2]

Προκειμένου να γίνει πρόβλεψη για την ορθή εφαρμογή της ισχύουσας νομοθεσίας περί προσωπικών δεδομένων θα προβούμε στη μελέτη δυο ενοτήτων.

Στην πρώτη ενότητα θα γίνει μία παράθεση των νομοθετημάτων που ισχύουν στον ελληνικό τραπεζικό τομέα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, τόσο σε ευρωπαϊκό όσο και σε Εθνικό Επίπεδο. Στη συνέχεια θα παρατεθούν οι αποφάσεις και οι γνωμοδοτήσεις της Αρχής Προστασίας Προσωπικών δεδομένων, που αφορούν σε θέματα που άπτονται της δραστηριοτήτων των τραπεζών και των χρηματοπιστωτικών οργανισμών, προκειμένου να επισημανθούν τα μελανά σημεία όπου στο παρελθόν διαπιστώθηκε παραβίαση της νομοθεσίας περί δεδομένων προσωπικού

[1] Ως διαλειτουργικότητα ορίζεται η δυνατότητα της επικοινωνίας και ανταλλαγής δεδομένων μεταξύ διαφορετικών λειτουργικών συστημάτων. (Παράρτημα Σύστασης Cm/Rec (2019)2 των Υπουργών Εξωτερικών προς τα κράτη μέλη) σύμφωνα με : Σωτηρόπουλος Β., «Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019, σελ.228

[2] Khiar I., Trautwein K., Huber A. and Stamm J. (2018), The EU General Data Protection Regulation (GDPR) in the banking industry https://www.pwc.ch/en/publications/2017/gdpr_banking_industry_report_en.pdf (23/1/2019)

χαρακτήρα, αλλά και οι περιπτώσεις όπου υπήρξε αμφιβολία για το εάν ερμηνεύτηκαν ορθώς οι διατάξεις και δόθηκε απάντηση από την αρμόδια εποπτική Αρχή.

Στη δεύτερη ενότητα θα εξεταστούν τα θέματα που προκύπτουν εάν εφαρμόσουμε τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 στο πλαίσιο εκτέλεσης των τραπεζικών εργασιών και υπηρεσιών. Θα γίνει συστηματική ανάλυση των άρθρων του Γ.Κ.Π.Δ. που αφορούν στις βασικές Αρχές, τα στοιχεία προς επεξεργασία, τον υπεύθυνο επεξεργασίας, τους νόμιμους σκοπούς επεξεργασίας και τα πρόσωπα στα οποία θα μπορούν να γνωστοποιηθούν τα προσωπικά δεδομένα, υπό το πρίσμα του τραπεζικών εργασιών και διαδικασιών. Ακόμη, θα γίνει συστηματική ανάλυση των άρθρων σχετικά με τη διασυνοριακή διαβίβαση δεδομένων, το χρονικό διάστημα τήρησης δεδομένων, τα δικαιώματα των πελατών των τραπεζικών ιδρυμάτων και τις υποχρεώσεις της τράπεζας, ως υπεύθυνου επεξεργασίας των δεδομένων.

Ακολουθεί η τρίτη ενότητα, στην οποία γίνεται ανάλυση του ρόλου του Υπευθύνου Προστασίας Δεδομένων, της καταστατικής του θέσης και των καθηκόντων του. Ο Υπεύθυνος Προστασίας Δεδομένων της Τράπεζας, ο «ακρογωνιαίος λίθος λογοδοσίας»[3] θα διευκολύνει τη συμμόρφωση, θα παρέχει συμβουλές , θα ενεργήσει ως ενδιάμεσος μεταξύ της Τράπεζας, της εποπτικής Αρχής και των υποκειμένων των δεδομένων και θα αποτελέσει το πρόσωπο που θα διαμορφώσει την πολιτική της Τράπεζας για την ορθή εφαρμογή της νομοθεσίας και την υλοποίηση του επιθυμητού μετασχηματισμού της.

Εν κατακλείδι, θα παρατεθούν κάποιες συμπερασματικές κρίσεις σχετικά με τις δράσεις στις οποίες πρέπει να προβεί η Τράπεζα ως υπεύθυνος επεξεργασίας για την ορθή εφαρμογή της νομοθεσίας περι προστασίας δεδομένων προσωπικού χαρακτήρα.

[3] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, «Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων» , Έκδοση 2018

Περιεχόμενα:

Συμβολισμοί :

Α.Π.Δ.Π.Χ.: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Αρ. :αριθμός
Αιτιολ.σκ. :αιτιολογική σκέψη
Γ.Κ.Π.Δ.: Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)
Ε.Ε: Ευρωπαϊκή ένωση
Ε.Ο.Χ.: Ευρωπαϊκός Οικονομικός Χώρος
Ν. : Νόμος
Παρ.: παράγραφος
Περ.: περίπτωση
Σελ. : σελίδα
Στοιχ.: στοιχείο
Υ.Π.Δ. : Υπεύθυνος Προστασίας Δεδομένων
D.P.O.: Data Protection Officer
F.A.T.C.A.: Foreign Account Tax Compliance Act (FATCA) είναι οι Κανόνες για την Φορολογική Συμμόρφωση που σχεδιάστηκαν από τις φορολογικές αρχές των ΗΠΑ (Internal Revenue Service “IRS”), με σκοπό την πρόληψη και πάταξη της φοροδιαφυγής των Αμερικανών προσώπων που διατηρούν λογαριασμούς σε χρηματοπιστωτικά ιδρύματα εκτός ΗΠΑ.
G.D.P.R.: General Data Protection Regulation
I.T.: Information Technology (ΤΠΕ) τεχνολογίες πληροφοριών και επικοινωνίας ή τεχνολογία της πληροφορίας είναι το σύνολο των επαγγελματικών χώρων οι οποίοι σχετίζονται με τη μελέτη, σχεδίαση, ανάπτυξη, υλοποίηση, συντήρηση και διαχείριση υπολογιστικών πληροφοριακών συστημάτων, κυρίως όσον αφορά εφαρμογές λογισμικού και υλικού υπολογιστών

1.Η προστασία των προσωπικών δεδομένων στον τραπεζικό τομέα

1.1 Σε επίπεδο Ευρωπαϊκής Ένωσης

Η Ευρώπη βρίσκεται στην πρώτη γραμμή της προστασίας δεδομένων παγκοσμίως. Τα πρότυπα της ΕΕ για την προστασία δεδομένων βασίζονται στη Σύμβαση 108 του Συμβουλίου της Ευρώπης, σε νομοθετικές πράξεις της ΕΕ – μεταξύ άλλων στον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ) και στην Οδηγία για την Προστασία Δεδομένων 95/46/ΕΚ που χρησιμοποιούνται από τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης– καθώς και στη σχετική νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου και του Δικαστηρίου της Ευρωπαϊκής Ένωσης. Οι μεταρρυθμίσεις στον τομέα της προστασίας δεδομένων που πραγματοποιήθηκαν από την Ευρωπαϊκή Ένωση και το Συμβούλιο της Ευρώπης είναι εκτεταμένες και ενίοτε σύνθετες, με ποικίλα οφέλη και συνέπειες για τα άτομα και τις επιχειρήσεις.[4]

Επιγραμματικά αναφέρονται παρακάτω οι βασικές νομικές διατάξεις που ρυθμίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα, γενικότερα. Βάσει του άρθρου 8 της ΕΣΔΑ, το δικαίωμα προσώπου σε προστασία σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα περιλαμβάνεται στο δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας του. Η Σύμβαση 108 του Συμβουλίου της Ευρώπης είναι η πρώτη, και μέχρι στιγμής η μόνη, διεθνής νομικά δεσμευτική πράξη που αφορά την προστασία των δεδομένων. Η Σύμβαση υποβλήθηκε σε διαδικασία εκσυγχρονισμού το 2018, η οποία ολοκληρώθηκε με την υιοθέτηση του τροποποιητικού πρωτοκόλλου CETS αριθ. 223. Βάσει του δικαίου της ΕΕ, η προστασία δεδομένων αναγνωρίζεται ως διακριτό θεμελιώδες δικαίωμα. Προβλέπεται στο άρθρο 16 της Συνθήκης για τη λειτουργία της ΕΕ καθώς και στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ε.Ε. Στο πλαίσιο του δικαίου της Ε.Ε., η προστασία δεδομένων ρυθμίστηκε για πρώτη φορά με την Οδηγία για την Προστασία Δεδομένων το 1995.

Λαμβανομένων υπόψη των ραγδαίων τεχνολογικών εξελίξεων, η Ε.Ε. θέσπισε νέα νομοθεσία το 2016 για την προσαρμογή των κανόνων για την προστασία δεδομένων στην ψηφιακή εποχή. Μαζί με τον Γενικό Κανονισμό για την Προστασία Δεδομένων Ε.Ε. 679/2016, η Ε.Ε. θέσπισε νομοθεσία για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από κρατικές αρχές για σκοπούς επιβολής του νόμου. Η Οδηγία (ΕΕ) 2016/680 θεσπίζει τους κανόνες και τις αρχές προστασίας δεδομένων που διέπουν την επεξεργασία

[4]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.[5] Ο Γενικός Κανονισμός για την Προστασία Δεδομένων Ε.Ε. 679/2016 τέθηκε σε εφαρμογή τον Μάιο του 2018, καταργώντας την Οδηγία για την Προστασία Δεδομένων 95/46/ΕΚ.

Το 2018, ο Οργανισμός Θεμελιωδών Δικαιωμάτων της Ε.Ε., σε συνεργασία με το Συμβούλιο της Ευρώπης και τον Ευρωπαίο Επόπτη Προστασίας Δικαιωμάτων δημοσίευσαν το «Εγχειρίδιο για το Ευρωπαϊκό Δίκαιο Προστασίας Δεδομένων», όπου παρουσιάζεται ο τρόπος με τον οποίο θα συνεφαρμοστούν οι κανόνες του Γενικού κανονισμού προστασίας Δεδομένων με τους κανόνες της επικαιροποιημένης Σύμβασης 108 και τη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου και του Δικαστηρίου της Ευρωπαϊκής Ένωσης.[6]

Η Οδηγία PSD2

Η 2η Οδηγία της Ευρωπαϊκής Ένωσης για τις πληρωμές (Payment Services Directive 2 – PSD2)[7], σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, ενσωματώθηκε στην ελληνική νομοθεσία με τον ν.4537/2018. Παρέχει τη νομική βάση για την περαιτέρω ανάπτυξη μιας καλύτερα ενοποιημένης εσωτερικής αγοράς για τις ηλεκτρονικές πληρωμές στην Ευρωπαϊκή Ένωση και θέτει σε εφαρμογή περιεκτικούς κανόνες για τις υπηρεσίες πληρωμών, με στόχο να καταστήσει τις διεθνείς πληρωμές (εντός της ΕΕ) εξίσου απλές, αποτελεσματικές και ασφαλείς με τις πληρωμές που διεκπεραιώνονται εντός μίας μόνο χώρας. Αποσκοπεί στο άνοιγμα αγορών πληρωμής σε νεοεισερχόμενους, οδηγώντας στην ενίσχυση του ανταγωνισμού, σε περισσότερες επιλογές και καλύτερες τιμές για τους καταναλωτές.

Η οδηγία αποσκοπεί στη βελτίωση των υφιστάμενων κανόνων της ΕΕ για τις ηλεκτρονικές πληρωμές. Λαμβάνει υπόψη αναδυόμενες και καινοτόμες υπηρεσίες πληρωμών, όπως οι πληρωμές μέσω διαδικτύου και μέσω κινητού. Καθορίζει κανόνες σχετικά με αυστηρές απαιτήσεις ασφαλείας για ηλεκτρονικές πληρωμές και την προστασία των οικονομικών δεδομένων των καταναλωτών, διασφαλίζοντας την ασφαλή εξακρίβωση της ταυτότητας και μειώνοντας τον κίνδυνο απάτης. Επίσης καθορίζει κανόνες σχετικά με τη διαφάνεια των απαιτήσεων των όρων και της ενημέρωσης για τις υπηρεσίες πληρωμών, τα δικαιώματα και τις υποχρεώσεις των χρηστών και

[5]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

[6] Σωτηρόπουλος Β., «Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019, σελ.13

[7]Οδηγία 2015/2366/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου της 25ης Νοεμβρίου 2015 (ΕΕ L 271).
https://eur-lex.europa.eu/legal-content/EL/LSU/?uri=CELEX:32015L2366

των παρόχων υπηρεσιών πληρωμών.

Οι βασικές διατάξεις της εν λόγω Οδηγίας, αφορούν. μεταξύ άλλων, την εισαγωγή δύο νέων κατηγοριών υπηρεσιών πληρωμών, εν προκειμένω τις υπηρεσίες εκκίνησης πληρωμών (PISP) και υπηρεσίες πληροφοριών λογαριασμών (AISP). Την εισαγωγή δύο νέων κατηγοριών φορέων παροχής υπηρεσιών πληρωμών, ήτοι των παρόχων υπηρεσιών εκκίνησης πληρωμών και παρόχων υπηρεσιών πληροφοριών λογαριασμών. Την ενίσχυση της ασφάλειας των ηλεκτρονικών συναλλαγών, απαιτώντας αυστηρή ταυτοποίηση των πελατών για τις πληρωμές τους, και
την περαιτέρω ενίσχυση της προστασίας των καταναλωτών υπηρεσιών πληρωμών.[8]

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων εξέδωσε κατευθυντήριες γραμμές για τη δεύτερη οδηγία για τις υπηρεσίες πληρωμών (PSD2). Σημαντικό είναι ότι η PSD2 εισάγει ένα νομικό πλαίσιο για τις νέες υπηρεσίες εκκίνησης πληρωμής (PISP) και τις υπηρεσίες πληροφοριών λογαριασμού (AISP). Οι χρήστες μπορούν να παρέχουν στους νέους αυτούς παρόχους υπηρεσιών πληρωμών πρόσβαση στους λογαριασμούς πληρωμών τους. Επίσης, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων εκπόνησε κατευθυντήριες γραμμές σχετικά με την εφαρμογή των διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων σε αυτές τις νέες υπηρεσίες πληρωμών.

Στις κατευθυντήριες γραμμές επισημαίνεται ότι στο συγκεκριμένο πλαίσιο η επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα εν γένει απαγορεύεται (σύμφωνα με το άρθρο 9 παρ. 1 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016), εκτός εάν το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση (άρθρο 9 παρ. 2 στ. α' του ΓΚΠΔ) ή η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος (άρθρο 9 παρ. 2 στοιχ.Ζ'του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016).

Στις κατευθυντήριες γραμμές εξετάζονται επίσης οι όροι υπό τους οποίους οι πάροχοι υπηρεσιών πληρωμών εξυπηρέτησης λογαριασμού (ASPSP) παρέχουν στις υπηρεσίες εκκίνησης πληρωμής (PISP) και στις υπηρεσίες πληροφοριών λογαριασμού (AISP)πρόσβαση σε πληροφορίες λογαριασμών πληρωμών, ιδίως μερική πρόσβαση σε λογαριασμούς πληρωμών.

Διευκρινίζεται στις εν λόγω κατευθυντήριες γραμμές ότι ούτε το άρθρο 66 παρ. 3 στοιχ. ζ' ούτε το άρθρο 67 παρ. 2 στοιχ. στ' της οδηγίας PSD2 προβλέπουν τη δυνατότητα περαιτέρω επεξεργασίας, εκτός και εάν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του (σύμφωνα με το άρθρο 6 παρ. 1 στοιχ. α' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε.

[8]Ελληνική Ένωση Τραπεζών
https://www.hba.gr/FinancialLaw/List?type=InternationalPaymentSystems

679/2016) ή εάν η επεξεργασία προβλέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους. [9]

1.2 Σε εθνικό επίπεδο

Με το Ν. 4692/2019 ενσωματώθηκε στην εθνική νομοθεσία η Οδηγία (Ε.Ε.) 2016/680 του Ευρωπαϊκού Κοινοβουλίου, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Με τον ίδιο νόμο και τις διατάξεις «πλαισίωσης»[10] του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε 679/2016 ελήφθησαν μέτρα εφαρμογής του ανωτέρω Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε 679/2016. Με τον ίδιο νόμο καταργήθηκε ο ν.2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

Ο Ν.4537/2018 ενσωματώνει στην ελληνική νομοθεσία την οδηγία (Ε.Ε.) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις υπηρεσίες πληρωμών στην εσωτερική αγορά (Payment Services Directive – PSD2).

Στις 26 Μαρτίου 2019 κατατέθηκε από την Ελληνική Ένωση Τραπεζών προς έγκριση από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ο Κώδικας Δεοντολογίας για την επεξεργασία Προσωπικών Δεδομένων στο τραπεζικό σύστημα. Σύμφωνα με το άρθρο 40 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016, η Ελληνική Ένωση Τραπεζών ως φορέας εκπροσώπησης των ελληνικών και ξένων πιστωτικών ιδρυμάτων που λειτουργούν στην Ελλάδα, έχει την αρμοδιότητα για την εκπόνηση Κώδικα Δεοντολογίας έχοντας αναγνωρίσει τις ιδιαιτερότητες του τραπεζικού κλάδου.[11] Επιδίωξη του Κώδικα Δεοντολογίας είναι να θέσει με σαφήνεια τις βασικές αρχές της διαφάνειας, συνέπειας, υπευθυνότητας και λογοδοσίας, που διέπουν την επεξεργασία των προσωπικών δεδομένων και να συμβάλλει στην ισχυροποίηση της ασφάλειας δικαίου στις σχέσεις των πιστωτικών ιδρυμάτων με τους πολίτες.

1.3 Αποφάσεις της Α.Π.Δ.Π.Χ.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι συνταγματικά

[9] Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0, 15 December 2020.
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

[10] Σωτηρόπουλος Β., «Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019, σελ.12

[11] Ελληνική Ένωση Τραπεζών. https://www.hba.gr/info/gdpr

κατοχυρωμένη ανεξάρτητη Αρχή που ιδρύθηκε με τον νόμο 2472/1997, ο οποίος ενσωμάτωσε στο ελληνικό δίκαιο την ευρωπαϊκή Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Από τις 25/5/2018, οπότε και τέθηκε σε εφαρμογή ο κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός Προστασίας Δεδομένων), η Οδηγία 95/45/ΕΚ καταργήθηκε και η Αρχή, έχει ως αποστολή της την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά[12].

Η Αρχή είναι επιφορτισμένη με την παρακολούθηση της εφαρμογής των διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ), με σκοπό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων που τα αφορούν και τη διευκόλυνση της ελεύθερης κυκλοφορίας των δεδομένων στην Ένωση.[13] Συμβάλλει στη συνεκτική εφαρμογή του ΓΚΠΔ σε ολόκληρη την Ένωση και για το σκοπό αυτό συνεργάζεται με την Επιτροπή και τις εποπτικές αρχές των κρατών μελών της ΕΕ. [14]

Η Αρχή είναι αρμόδια να εκτελεί τα καθήκοντά της, βάσει του άρθρου 57 του ΓΚΠΔ, και να ασκεί τις εξουσίες που της ανατίθενται, βάσει του άρθρου 58 του ΓΚΠΔ, στο έδαφός της (άρθρο 55 παρ. 1, αιτ. 122, 129 του ΓΚΠΔ) με πλήρη ανεξαρτησία (άρθρο 52, αιτ. 117-118, 121 του ΓΚΠΔ).

Ειδικότερα, η Αρχή είναι επιφορτισμένη μεταξύ άλλων να παρακολουθεί και επιβάλλει την εφαρμογή του ΓΚΠΔ, να προωθεί την ευαισθητοποίηση του κοινού στα ζητήματα προστασίας προσωπικών δεδομένων και των υπευθύνων και εκτελούντων επεξεργασία σχετικά με τις υποχρεώσεις τους δυνάμει του ΓΚΠΔ. Συμβουλεύει το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα και οργανισμούς για νομοθετικά και διοικητικά μέτρα που σχετίζονται με την προστασία των προσωπικών δεδομένων. Παρέχει κατόπιν αιτήματος πληροφορίες στα υποκείμενα των δεδομένων σχετικά με την άσκηση των δικαιωμάτων τους. Χειρίζεται τις υποβληθείσες για παράβαση διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 καταγγελίες, διενεργεί έρευνες σχετικά με την εφαρμογή του ΓΚΠΔ. Καταρτίζει και διατηρεί κατάλογο σε σχέση με την απαίτηση για διενέργεια εκτίμησης αντικτύπου (άρθρο 35 παρ. 4 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016) και να παρέχει συμβουλές σχετικά με τις πράξεις

[12] Ετήσια έκθεση της Αρχής 2018
https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/FILES%20ANNUAL%20REPORTS/ANNUAL%202018%20V3.0%20WEBPAGE_0.PDF
[13] Άρθρο 51 παρ. 1, αιτ. 123 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[14] Άρθρο 51 παρ. 2, αιτ. 123 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

επεξεργασίας του άρθρου 36 παρ. 2 του ΓΚΠΔ. Συνεργάζεται με άλλες εποπτικές αρχές μέσω ανταλλαγής πληροφοριών και να παρέχει αμοιβαία συνδρομή σε αυτές με σκοπό τη διασφάλιση της συνεκτικότητας εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 .[15] Επίσης, η Αρχή διαθέτει εξουσίες ελέγχου, καθώς και διορθωτικές, συμβουλευτικές και αδειοδοτικές εξουσίες, όπως αυτές εξειδικεύονται και αναλύονται στο άρθρο 58 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016.

Πριν την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016, η Αρχή, σύμφωνα με την ισχύουσα έως τις 25 Μαΐου 2018 νομοθεσία (άρθρο 19 του ν. 2472/1997), είχε μια σειρά αρμοδιοτήτων, τόσο ρυθμιστικών εν ευρεία εννοία όσο και ελεγκτικών. Η Αρχή, στο πλαίσιο των ρυθμιστικών της αρμοδιοτήτων, εξέδιδε οδηγίες προς τον σκοπό ενιαίας εφαρμογής των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων. Εξέταζε αιτήσεις του υπευθύνου επεξεργασίας, με τις οποίες ζητούνταν ο έλεγχος και η εξακρίβωση της νομιμότητας της επεξεργασίας και απηύθυνε συστάσεις και υποδείξεις στους υπευθύνους επεξεργασίας. Επίσης, η Αρχή γνωμοδοτούσε για κάθε νομοθετική ή κανονιστική ρύθμιση που αφορούσε την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα. Στο πλαίσιο των ελεγκτικών της αρμοδιοτήτων, η Αρχή εξέταζε προσφυγές, καταγγελίες, αντιρρήσεις και παράπονα των υποκειμένων των δεδομένων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων τους.[16]

Το ζήτημα της προστασίας των δεδομένων προσωπικού χαρακτήρα στον τραπεζικό χώρο απασχόλησε την Αρχή τόσο προληπτικά, με τη μορφή κανονιστικών πράξεων, γνωμοδοτήσεων και αποφάσεων, όσο και κατασταλτικά συνεπεία προσφυγών, καταγγελιών και παραπόνων που υπεβλήθησαν.[17] Κατά τη διάρκεια της λειτουργίας της η Αρχή εξέδωσε πλήθος αποφάσεων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα με υπεύθυνο επεξεργασίας κάποιο πιστωτικό ίδρυμα. Παρακάτω αναφέρονται ενδεικτικά κάποιες αποφάσεις της Αρχής, κατηγοριοποιημένες ανά αντικείμενο συζήτησης ή τραπεζική δραστηριότητα που αφορούν.

1.3.1 Στοιχεία ταυτοποίησης που ζητούν οι τράπεζες.

Η Αρχή απάντησε[18] ότι σύμφωνα με τις με αριθ. 281/17.3.2009, 2652/29.02.2012 και 94/15.11.2013 Πράξεις της ΕΤΠΘ της Τράπεζας της

[15] Άρθρο 57 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679
[16] Ετήσια έκθεση της Αρχής Προστασίας Δεδομένων προσωπικού Χαρακτήρα 2018 https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/FILES%20ANNUAL%20REPORTS/ANNUAL%202018%20V3.0%20WEBPAGE_0.PDF
[17] Αλεξανδροπούλου – Αιγυπτιάδου Ε.: «Ηλεκτρονική επεξεργασία προσωπικών δεδομένων στο πεδίο της Τραπεζικής Δραστηριότητας (Νομικό Πλαίσιο) Αρμ. ΝΗ' (2004)1337–1395
[18] Ενημερωτικό δελτίο (newsletter) της Αρχής Τεύχος 12 / Ιούλιος 2015 (https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/NEWSMAIN/INFORMATIONAL/JULY2015.PDF#12o)

Ελλάδος τα χρηματοπιστωτικά ιδρύματα και άλλα υπόχρεα πρόσωπα οφείλουν (στο μέτρο της δέουσας επιμέλειας σύμφωνα με τα προβλεπόμενα στον ν. 3691/2008 για την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες, όπως τροποποιήθηκε και ισχύει) να εξακριβώνουν και να ελέγχουν την ταυτότητα του πελάτη τους ή του συναλλασσόμενου και να ζητούν έγγραφα που να πιστοποιούν τα συγκεκριμένα στοιχεία του φυσικού προσώπου. Ειδικότερα, τα στοιχεία που απαιτούνται κατ' ελάχιστον για την πιστοποίηση της ταυτότητας των φυσικών προσώπων είναι: ονοματεπώνυμο και πατρώνυμο, ΑΔΤ ή διαβατήριο, εκδούσα αρχή, ημερομηνία και τόπος γέννησης, παρούσα διεύθυνση κατοικίας, τηλέφωνο επικοινωνίας, ασκούμενο επάγγελμα και παρούσα επαγγελματική διεύθυνση, ΑΦΜ και δείγμα υπογραφής πελάτη. Τα ανωτέρω στοιχεία επαληθεύονται από έγγραφα τα οποία είναι δύσκολο να παραποιηθούν ή να αποκτηθούν με παράνομο τρόπο, όπως ενδεικτικά αναφέρονται πρόσφατο λογαριασμό οργανισμού κοινής ωφέλειας, αντίγραφο μισθοδοσίας. Η τράπεζα μπορεί επίσης να ζητήσει, σύμφωνα με το ανωτέρω κανονιστικό πλαίσιο, κατ' εφαρμογή των μέτρων δέουσας επιμέλειας[19] κάθε στοιχείο συναφές με το αντικείμενο και τη φύση της συναλλαγής, όπως στοιχεία σχετικά με την επαγγελματική και οικονομική κατάσταση των πελατών τους (παρούσα διεύθυνση κατοικίας, ασκούμενο επάγγελμα και επαγγελματική διεύθυνση, ΑΦΜ, εισόδημα από άλλες πηγές, κ.λπ.). Οι διαδικασίες πιστοποίησης και τα μέτρα δέουσας επιμέλειας προβλέπουν ότι οι τράπεζες ασκούν συνεχή εποπτεία καθ' όλη τη διάρκεια της συναλλακτικής σχέσης με ενδελεχή εξέταση κάθε συναλλαγής ως προς το ζήτημα αν συνάδει με τη γνώση που έχει η τράπεζα για τον συγκεκριμένο πελάτη της και τις επαγγελματικές δραστηριότητές του. Ειδικότερα, τα μέτρα της συνήθους δέουσας επιμέλειας, τα οποία εφαρμόζουν τα πιστωτικά ιδρύματα που λειτουργούν στη χώρα μας, ως προς τον πελάτη, περιλαμβάνουν τη συλλογή πληροφοριών για τον σκοπό και τη σκοπούμενη φύση της επιχειρηματικής σχέσης ή σημαντικών συναλλαγών ή δραστηριοτήτων του πελάτη ή του πραγματικού δικαιούχου και την επαλήθευση από τα πιστωτικά ιδρύματα των εισοδημάτων των ανωτέρω με βάση προσκομιζόμενο πρόσφατο εκκαθαριστικό σημείωμα φορολογίας εισοδήματος, πλην των περιπτώσεων, στις οποίες ο πελάτης δεν υποχρεούται να υποβάλει δήλωση φόρου εισοδήματος[20].

1.3.2 Θύρες εισόδου ασφαλείας

Σχετικά με τις θύρες εισόδου ασφαλείας που τοποθετήθηκαν σε καταστήματα Τράπεζας, που διαθέτουν σύστημα που συλλέγει και αποθηκεύει δεδομένα εικόνας αλλά ουσιαστικά επεξεργάζεται δεδομένα της γεωμετρίας του προσώπου, που εντάσσονται στην κατηγορία των βιομετρικών δεδομένων, η Αρχή εξέδωσε την απόφαση 194/2012. Σύμφωνα με την απόφαση, δεν

[19] παρ. 5.4 της με αριθ. 281/17.3.2009 Πράξης της ΕΤΠΘ της Τράπεζας της Ελλάδος
[20] Άρθρο 13 παρ. 1 στοιχ. γ΄ του ν. 3691/2008

πραγματοποιείται καμία περαιτέρω χρήση των βιομετρικών δεδομένων, ούτε είναι δυνατό σε κάποιον χρήστη του συστήματος να εξαγάγει εκ νέου αυτά τα χαρακτηριστικά για όλες τις αποθηκευμένες φωτογραφίες. Επίσης, σκοπός της επεξεργασίας είναι η πρόληψη και αποτροπή εγκληματικών ενεργειών καθώς και προστασία του συναλλακτικού κοινού και του προσωπικού, σκοπός που παρίσταται νόμιμος. Προκειμένου η λειτουργία του συστήματος ασφαλείας να είναι σύμφωνη με την αρχή της αναλογικότητας, υπό την ειδικότερη έκφανση της αναγκαιότητας, αυτή θα πρέπει να επιτρέπεται μόνο μετά από ειδικά αιτιολογημένη απόφαση του Διευθυντή της οικείας Διεύθυνσης Ασφαλείας ή Αστυνομικής Διεύθυνσης, η οποία θα λαμβάνει ιδίως υπόψη την εγκληματικότητα, την πραγματοποίηση συναθροίσεων ή συγκεντρώσεων στην περιοχή, τη διάπραξη στο συγκεκριμένο κατάστημα φθορών ή ληστείας κατά το παρελθόν, την απόστασή του από το πλησιέστερο αστυνομικό τμήμα, καθώς και τη διακίνηση από το συγκεκριμένο κατάστημα μεγάλων χρηματικών ποσών ή τη φύλαξη σε αυτό αντικειμένων σημαντικής αξίας.

1.3.3 Διατήρηση και επεξεργασία των δεδομένων που βιντεοσκοπούνται από τα εγκατεστημένα κλειστά κυκλώματα βιντεοσκόπησης στις Τράπεζες

Η λήψη και επεξεργασία δεδομένων προσωπικού χαρακτήρα με συστήματα βιντεοεπιτήρησης συνιστά περιορισμό του ατομικού δικαιώματος προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μεσα, των προσωπικών δεδομένων, το οποίο καθιερώνεται από το άρθρο 9Α του Συντάγματος. Έτσι η εγκατάσταση και λειτουργία συστημάτων βιντεοεπιτήρησης σε χώρους που δεν είναι δημόσιοι αλλά είναι προσβάσιμοι στο κοινό πρέπει να γίνεται μετά από ουσιαστική αξιολόγηση της αναγκαιότητας της συγκεκριμένης επεξεργασίας σε σχέση (α) με τον κίνδυνο που ο υπεύθυνος επεξεργασίας επιδιώκει να αντιμετωπίσει και (β) με το μέγεθος της επίπτωσης στην ιδιωτική ζωή των προσώπων που αφορά. Η αξιολόγηση αυτή θα πρέπει να περιλαμβάνει και τη διερεύνηση ηπιότερων μέσων ασφάλειας προσώπων και αγαθών[21].

Με την απόφασή της 40/2001 η Αρχή αποφάσισε να επιτρέψει στα τραπεζικά ιδρύματα να διατηρούν τα αρχεία που προκύπτουν από εγκατάσταση κλειστών κυκλωμάτων, για χρονικό διάστημα όχι μεγαλύτερο των σαράντα πέντε (45) ημερολογιακών ημερών, αντί των 15 ημερών, που προβλεπόταν αρχικά στην 1122 (Φ.Ε.Κ. αρ. 1234/9-10-2000) Οδηγία της, λαμβάνοντας υπόψη την αναγκαιότητα πρόληψης και αποτροπής εγκλημάτων, καθώς και την ανάγκη επίλυσης διενέξεων που αφορούν αμφισβητήσεις οικονομικών συναλλαγών, τροποποιώντας κατά τούτο την ανωτέρω Οδηγία. Η Οδηγία αυτή (1122/2000) καταργήθηκε με την Οδηγία 1/2011 σχετικά με τη χρήση

[21] Άρθρο 1 της Οδηγίας 1/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών.

Πλέον ισχύει η Οδηγία 1/2011, οι διατάξεις της οποίας πρέπει να εφαρμόζονται σε συνδυασμό με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) και του ν.4624/2019, με οδηγό το κείμενο κατευθυντήριων γραμμών 3/2019 του ΕΣΠΔ.

Στην Οδηγία συγκεκριμένα για τις Τράπεζες και τα λοιπά χρηματοπιστωτικά ιδρύματα, υπάρχει ειδική πρόβλεψη[22] ότι η εγκατάσταση συστημάτων βιντεοεπιτήρησης επιτρέπεται σε όλους τους χώρους των τραπεζών εκτός από τους χώρους, όπου η βιντεοεπιτήρηση προσβάλλει τον σκληρό πυρήνα του δικαιώματος στην ιδιωτική ζωή (παρ. 3 του άρθρου 6 της Οδηγίας1/2011), όπως είναι οι χώροι και οι προθάλαμοι τουαλετών. Σε διατήρηση του περιεχομένου της παλαιότερης απόφασης 40/2001 της Αρχής ορίζεται ότι ειδικά οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα δύνανται να διατηρούν τα δεδομένα για χρονικό διάστημα όχι μεγαλύτερο των 45 ημερών (ενώ η γενική πρόβλεψη του άρθρου 8 ορίζει διάστημα 15 ημερών). Αν κατά το χρονικό αυτό διάστημα καταγραφούν περιστατικά οργανωμένης οικονομικής απάτης ή αμφισβήτησης οικονομικής συναλλαγής, τα σχετικά τμήματα των δεδομένων του συστήματος βιντεοεπιτήρησης δύναται να διατηρηθούν σε ξεχωριστό αρχείο με ανάλογα μέτρα ασφαλείας για όσο διάστημα απαιτείται για τη διερεύνηση και την πειθαρχική ή δικαστική δίωξη των περιστατικών αυτών.

Η Αρχή επισημαίνει[23] ιδιαίτερα την υποχρέωση για αυξημένη διαφάνεια, όπως απορρέει από τον ΓΚΠΔ. Οι υπεύθυνοι επεξεργασίας που χρησιμοποιούν συστήματα βιντεοεπιτήρησης οφείλουν να φροντίζουν για την ικανοποίηση των επαυξημένων δικαιωμάτων που προβλέπει ο ΓΚΠΔ., δεν έχουν πλέον την πρότερη υποχρέωση γνωστοποίησης της επεξεργασίας στην Αρχή, αλλά οφείλουν να παρέχουν πλήρη ενημέρωση για τη λειτουργία καμερών, πριν κάποιος εισέλθει στον επιτηρούμενο χώρο.[24] Για τον σκοπό αυτό είναι, κατά κανόνα, προσφορότερο να ακολουθείται πολυεπίπεδη προσέγγιση, δηλαδή να υπάρχουν ενημερωτικές πινακίδες για την άμεση ενημέρωση όσων εισέρχονται στον χώρο, οι οποίες να παραπέμπουν σε εύκολα προσβάσιμη αναλυτική ενημέρωση. Πριν ένα πρόσωπο εισέλθει στην εμβέλεια του συστήματος βιντεοεπιτήρησης, ο υπεύθυνος επεξεργασίας οφείλει να το ενημερώνει, με τρόπο εμφανή και κατανοητό, ότι πρόκειται να εισέλθει σε χώρο που βιντεοσκοπείται. Προς τούτο, πρέπει να αναρτώνται σε επαρκή αριθμό και εμφανές μέρος ευδιάκριτες πινακίδες, όπου θα αναγράφεται το πρόσωπο για λογαριασμό του οποίου γίνεται η βιντεοσκόπηση (υπεύθυνος επεξεργασίας), ο σκοπός, καθώς και το άτομο με το οποίο οι ενδιαφερόμενοι

[22] Άρθρο 16 της Οδηγίας 1/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[23] Δελτίο Τύπου της 9/6/2020 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[24] Άρθρα 10 έως 13 της Οδηγίας 1/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

μπορούν να επικοινωνήσουν για να ασκήσουν τα δικαιώματά τους.[25]

1.3.4 Χορήγηση οικονομικών στοιχείων της Τράπεζας σε Τρίτους

Η Αρχή έκρινε[26] ότι είναι νόμιμη η χορήγηση σε τρίτο αντιγράφων επιταγών, που η Τράπεζα διατηρεί και αποτελούν το μόνο τρόπο απόδειξης δικαιώματος του αιτούντος /τρίτου ενώπιον Δικαστηρίου. Σύμφωνα με την Απόφαση 22/2004 της Αρχής: «κατά εφαρμογή του άρθρου 7 παρ.2 εδ. γ του Ν.2472/1997, η επεξεργασία ευαίσθητων προσωπικών δεδομένων επιτρέπεται όταν είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου. Κατ' αναλογία, αφού η επεξεργασία είναι επιτρεπτή για το μείζον, δηλαδή για τα ευαίσθητα, επιτρέπεται και για το έλασσον, δηλαδή τα μη ευαίσθητα δεδομένα.

1.3.5 Σχετικά με τη συγκατάθεση υποκειμένου δικαιωμάτων.

Η Αρχή με την απόφαση 18/2007 απεφάνθη ότι η υπογραφή από πελάτη εντύπου της Τράπεζας σχετικά με την επεξεργασία προσωπικών δεδομένων δεν στοιχειοθετεί και τη συγκατάθεσή του για επεξεργασία των δεδομένων του από όλες τις Διευθύνσεις της Τράπεζας ή και τις εταιρίες του ίδιου Ομίλου για σκοπούς άσχετους με το αντικείμενο της συναλλακτικής σχέσης. Στην περίπτωση που εξετάστηκε σε προεκτυπωμένη αίτηση για χορήγηση χρεωστικής κάρτας από Χρηματοπιστωτικό Ίδρυμα υπήρχε όρος, με τον οποίο παρέχεται εκ των προτέρων η συγκατάθεση του υποκειμένου στην τράπεζα προς επεξεργασία των προσωπικών του δεδομένων για διαφημιστικούς σκοπούς ή για προώθηση πωλήσεων προϊόντων και υπηρεσιών. Ο όρος αυτός της αιτήσεως για χορήγηση χρεωστικής κάρτας, είναι διατυπωμένος εκ των προτέρων και ο καταναλωτής είναι υποχρεωμένος, πιεζόμενος από την ανάγκη λήψεως της συγκεκριμένης παροχής του Χρηματοπιστωτικού Ιδρύματος να αποδεχθεί τον όρο αυτό ή να μην τον αποδεχθεί, αλλά τότε δεν θα γίνει κάτοχος της χρεωστικής κάρτας και δεν θα απολαμβάνει των ωφελειών και προνομίων που η κάρτα αυτή παρέχει και στην οποία απέβλεπε με τη σύμβαση. Έτσι επέρχεται περιορισμός του δικαιώματος της συμβατικής του ελευθερίας. Ο παραπάνω όρος εκρίθη από την Αρχή ότι είναι παράνομος, διότι η επεξεργασία γίνεται για άλλους πλην της εκτέλεσης της σύμβασης σκοπούς, η συγκατάθεση δεν είναι ειδική και ελεύθερη και δεν είχε προηγηθεί η απαιτούμενη από τις διατάξεις του ν. 2472/1997 ενημέρωση.[27]

Επίσης σχετικά με τη συγκατάθεση του υποκειμένου των δεδομένων παραθέτουμε και την απόφαση 39/2015 της Αρχής, σχετικά με υπηρεσία τράπεζας, όπου μέσω ιστοσελίδας ο επισκέπτης της εν λόγω ιστοσελίδας εισαγάγει τα στοιχεία μιας οποιασδήποτε πιστωτικής κάρτας που έχει

[25] Άρθρο 12 της Οδηγίας 1/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[26] Απόφαση 22/2004 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[27] Απόφαση 18/2007 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

χορηγήσει η Τράπεζα σε κάποιον πελάτη της, καθώς επίσης και την ημερομηνία γέννησης του κατόχου αυτής της κάρτας, και μπορεί να λάβει πληροφορίες περί των κινήσεων της κάρτας (αγορές/χρεώσεις και πληρωμές), χωρίς να είναι σε εφαρμογή άλλος μηχανισμός αυθεντικοποίησης του χρήστη και χωρίς να έχει λάβει τη συναίνεση του πελάτη. Η εν λόγω υπηρεσία αποσκοπούσε στην αμεσότερη πληροφόρηση των πελατών-κατόχων πιστωτικών καρτών που δεν επιθυμούσαν να είναι εγγεγραμμένοι χρήστες στις υπηρεσίες ηλεκτρονικής τραπεζικής σχετικά με την κίνηση των καρτών τους και ήταν διαθέσιμη για οποιονδήποτε κάτοχο πιστωτικής κάρτας, εκτός αν ο ίδιος δήλωνε ρητώς ότι δεν την επιθυμεί (σύστημα “opt-out”).

Κρίθηκε από την Αρχή[28] ότι η εν λόγω επεξεργασία δεν μπορεί να εκληφθεί ως απολύτως απαραίτητη στο πλαίσιο των συμβατικών σχέσεων μεταξύ του υπευθύνου επεξεργασίας και των υποκειμένων των δεδομένων ώστε να τύχει εφαρμογής η εξαίρεση του άρ. 5 παρ. 2 στοιχ. α) του ν. 2472/1997, αλλά θα πρέπει να παρέχεται σε κάθε πελάτη του υπευθύνου επεξεργασίας μόνο κατόπιν συγκατάθεσής του, μετά από επαρκή και σαφή ενημέρωση. Η Αρχή απεφάνθη πως δεν μπορεί να υπαχθεί στην περίπτωση όπου η επεξεργασία επιτρέπεται και χωρίς τη συγκατάθεση όταν είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία το συμβαλλόμενο μέρος είναι υποκείμενο των δεδομένων, αφού η συγκεκριμένη πληροφόρηση για τις κινήσεις των καρτών μπορεί να παρέχεται και με άλλους τρόπους όπως λ.χ. μέσω ταχυδρομείου, οπότε και δεν συντρέχει το στοιχείο της αναγκαιότητας της επεξεργασίας. Ενόψει των ανωτέρω, η Αρχή κάλεσε την Τράπεζα να διασφαλίσει ότι, για τους νέους πελάτες-κατόχους πιστωτικών καρτών, η συγκεκριμένη υπηρεσία θα παρέχεται μόνο εφόσον δηλώσουν ρητώς και ειδικώς ότι την επιθυμούν, αφού προηγουμένως ενημερωθούν για τα βασικά χαρακτηριστικά αυτής. Η δήλωση συγκατάθεσης θα πρέπει να παρέχεται από τους πελάτες, με φυσική τους παρουσία, σε κατάστημα της Τράπεζας ή ηλεκτρονικά, με τρόπο τέτοιο που να διασφαλίζεται η πιστοποίηση της ταυτότητας του αιτούντος. Επίσης κάλεσε την Τράπεζα να φροντίσει αμελλητί, για τους νυν πελάτες-κατόχους πιστωτικών καρτών της Τράπεζας, που δεν είχαν δηλώσει την αντίρρησή τους για την εν λόγω υπηρεσία, να υπάρξει σχετική ατομική ενημέρωση , στην οποία θα αναφέρεται ότι η υπηρεσία είναι ήδη ενεργή, θα περιγράφονται τα χαρακτηριστικά αυτής αλλά και ο τρόπος με τον οποίο μπορεί κάποιος να ζητήσει τη διακοπή της. Η Τράπεζα υποχρεώθηκε όπως τροποποιήσει, εντός τριών μηνών, την υπηρεσία ως προς τα μέτρα ασφάλειας αυτής, έτσι ώστε να υλοποιείται στο πλαίσιο αυτής ισχυρός μηχανισμός αυθεντικοποίησης των χρηστών της, όπως είναι ο κωδικός πρόσβασης (συνθηματικό) από τον κάθε χρήστη, κατά τρόπο τέτοιο ώστε αυτό να είναι εις γνώσιν μόνο του ιδίου. Τέλος η Τράπεζα κλήθηκε να διασφαλίζει ότι, για κάθε τυχόν μελλοντική τροποποίηση της εν λόγω υπηρεσίας, θα παρέχεται πρόσφορη σχετική

[28] Απόφαση 39/2015 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

ενημέρωση στους χρήστες της.[29]

1.3.6 Ασφαλής καταστροφή προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας.

Η Αρχή εξέδωσε δύο αποφάσεις (1/2007 και 76/2012) σε δύο περιπτώσεις που διαπιστώθηκε ότι δεν τηρήθηκαν από Τραπεζικά Ιδρύματα επαρκή μέτρα ασφαλείας για την προστασία των δεδομένων και την πρόληψη κινδύνων όπως απώλεια, μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη. Τα περιστατικά αφορούσαν ανεύρεση τραπεζικών παραστατικών και εγγράφων πελατών, μεταξύ των οποίων αναλύσεις τραπεζικών λογαριασμών, μηνιαίοι λογαριασμοί πιστωτικών καρτών, αιτήσεις δανείων και πιστωτικών καρτών αλληλογραφία με προσωπικά δεδομένα πελατών, φωτοτυπίες αστυνομικής ταυτότητας πελατών, εσωτερικά υπηρεσιακά έγγραφα της τράπεζας, που περιείχαν προσωπικά δεδομένα πελατών και υπαλλήλων της Τράπεζας, τα οποία δεν καταστράφηκαν με προσήκοντα τρόπο και ανευρέθηκαν εγκαταλελειμμένα σε δημόσιο χώρο, έξω από το κατάστημα της τράπεζας. Στην πρώτη περίπτωση απεύθυνε αυστηρή προειδοποίηση προς τον υπεύθυνο επεξεργασίας, στη δεύτερη περίπτωση επέβαλλε πρόστιμο ύψους δέκα χιλιάδων (10.000) Ευρώ για την παραβίαση του άρθρου 10 ν. 2472/1997 και κάλεσε την Τράπεζα να εφαρμόσει πιστά τις διατάξεις της Οδηγίας 1/2005 της Αρχής σχετικά με την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού επεξεργασίας.

1.3.7 Παράνομη παρακράτηση και άρνηση απόδοσης προσκομισθέντων εγγράφων υποψηφίου πελάτη.

Τράπεζα παρακράτησε και αρνήθηκε να αποδώσει σε υποψήφιο πελάτη τα δικαιολογητικά έγγραφα, που αυτός είχε προσκομίσει για την υποστήριξη αίτησής του για χορήγηση πιστωτικής κάρτας, η οποία όμως απορρίφθηκε. Σύμφωνα με την Απόφαση 26/2003 της Αρχής από τη διάταξη του άρθρου 4 παρ.7 του ν.2331/95 προκύπτει υποχρέωση της τράπεζας για τήρηση τουλάχιστον επί πενταετία στοιχείων σχετικών με συναλλαγές και συμβάσεις που συνάπτει στα πλαίσια επιχειρηματικών σχέσεων. Επομένως, εφόσον η τράπεζα δεν προχώρησε στη σύναψη σύμβασης ή συναλλακτικής σχέσης με τον προσφεύγοντα, αλλά η συλλογή των στοιχείων έγινε κατά το προσυμβατικό στάδιο, δεν διαπιστώθηκε νόμιμος λόγος για την τήρηση των στοιχείων του μετά την απόρριψη της αίτησης χορήγησης πιστωτικής κάρτας και επομένως η τήρηση αυτών κρίθηκε παράνομη. Η Αρχή απεύθυνε προειδοποίηση προς την τράπεζα να επιστρέψει τα αιτούμενα στοιχεία στον προσφεύγοντα.

[29] Απόφαση 39/2015 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

1.3.8 Επεξεργασία προσωπικών δεδομένων για την προώθηση ή διαφήμιση προϊόντων ή υπηρεσιών της Τράπεζας.

Με την Απόφαση 50/2000 η Αρχή προσδιορίζει τους όρους για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης, γενικότερα. Η επεξεργασία είναι νόμιμη εφόσον παρέχεται η συγκατάθεση του υποκειμένου. Εάν δεν υπάρχει συγκατάθεση, η επεξεργασία θεωρείται νόμιμη στις παρακάτω περιπτώσεις:

Τα δεδομένα προέρχονται από καταλόγους που απευθύνονται στο ευρύ κοινό και να υπάρχει η βεβαιότητα πως τα υποκείμενα που έχουν συμπεριληφθεί σε αυτόν έχουν δώσει τη συγκατάθεσή τους/ ή από πηγές δημόσια προσβάσιμες που προορίζονται για την παροχή πληροφοριών στο ευρύ κοινό, εφόσον έχουν τηρηθεί οι νόμιμες προϋποθέσεις για την πρόσβαση σε αυτές/ ή το ίδιο το υποκείμενο να έχει δημοσιοποιήσει τα δεδομένα του για συναφείς σκοπούς.

Ο υπεύθυνος επεξεργασίας να έχει συμβουλευθεί το Μητρώο που τηρεί η Αρχή, στο οποίο καταχωρούνται όσοι δεν επιθυμούν την επεξεργασία δεδομένων τους.

Ο υπεύθυνος επεξεργασίας να περιορίζεται στα απολύτως αναγκαία δεδομένα για την επίτευξη του συγκεκριμένου σκοπού (ονοματεπώνυμο, διεύθυνση, επάγγελμα)

Ο σκοπός της επεξεργασίας να περιορίζεται στη διαφήμιση ή στην προώθηση πώλησης αγαθών ή στην παροχή υπηρεσιών εξ' αποστάσεως και να μην αντίκειται στα χρηστά ήθη.[30]

1.3.9 Νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για το σκοπό της διαπίστωσης πιστοληπτικής ικανότητας.

Με την απόφαση 50/2000 της, η Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα ορίζει τις προϋποθέσεις υπό τις οποίες η συλλογή πληροφοριών με σκοπό τη διαπίστωσης πιστοληπτικής ικανότητας είναι νόμιμη χωρίς τη συγκατάθεση του υποκειμένου με βάση την εξαίρεση του άρθρου 5 παρ. 2 εδ. ε του Ν.2472/97. Η νομιμότητα αιτιολογείται γιατί η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του εννόμου συμφέροντος το οποίο επιδιώκει ο υπεύθυνος επεξεργασίας και ο τρίτος αποδέκτης των δεδομένων. Το συγκεκριμένο έννομο συμφέρον συνίσταται στην άσκηση του δικαιώματος οικονομικής ελευθερίας με βάση πληροφορίες που εξασφαλίζουν την εμπορική πίστη, την αξιοπιστία και την ασφάλεια των συναλλαγών. Είναι εύλογο ότι χωρίς τη δυνατότητα πρόσβασης σε ορθές και επίκαιρες πληροφορίες, οι οποίες αφορούν την πιστοληπτική ικανότητα των συναλλασσομένων η ικανοποίηση του εν λόγω εννόμου συμφέροντος δυσχεραίνεται σημαντικά. Επίσης κρίνει πως το συγκεκριμένο έννομο συμφέρον υπερέχει προφανώς των συμφερόντων του υποκειμένων που δεν

[30] Απόφαση 50/2000 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

θίγονται ουσιωδώς και πάντως η ικανοποίησή τους δεν θίγει τις θεμελιώδεις ελευθερίες των υποκειμένων. Για να συμβεί αυτό η συλλογή και επεξεργασία των δεδομένων πρέπει να πραγματοποιείται υπό τους ακόλουθους τουλάχιστον περιορισμούς:

Τα δεδομένα που επιτρέπεται να συλλέξουν οι εταιρείες χωρίς συγκατάθεση του υποκειμένου είναι μόνο:

α) Αιτήσεις πτωχεύσεων

β) Αποφάσεις επί αιτήσεων πτωχεύσεων

γ) Διαταγές πληρωμής

δ) Προγράμματα πλειστηριασμού ακινήτων

ε) Προγράμματα πλειστηριασμού κινητών

στ) Μεταβολές προσωπικών εταιρειών

ζ) Μεταβολές Α.Ε., ΕΠΕ και Κοινοπραξιών

η) Υποθήκες και προσημειώσεις υποθηκών

θ) Κατασχέσεις και επιταγές βάσει Ν.Δ. 1923

ι) Ακάλυπτες επιταγές

ια) Διαμαρτυρημένες συναλλαγματικές και γραμμάτια εις διαταγήν.

Μετά τη συλλογή των δεδομένων και πριν από κάθε διαβίβαση ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώσει ατομικά τα υποκείμενα βάσει του άρθρου 11 του ν. 2472/97, ώστε να ασκήσουν τα δικαιώματα πρόσβασης και αντίρρησης σύμφωνα με τα άρθρα 12 και 13 του ανωτέρω νόμου. Σε περίπτωση που το υποκείμενο ασκώντας το δικαίωμα αντίρρησης ζητήσει τη διαγραφή των δεδομένων του, ο υπεύθυνος επεξεργασίας υποχρεούται να προχωρήσει στη διαγραφή ενημερώνοντας το υποκείμενο για τις τυχόν επιπτώσεις που θα έχει η διαγραφή στην εν γένει συναλλακτική του συμπεριφορά. Στην περίπτωση πού το υποκείμενο αμφισβητήσει την νομιμότητα της εγγραφής και αφού ακολουθηθεί η διαδικασία των άρθρων 12 και 13, το βάσιμο του αιτήματος θα κρίνεται από την Αρχή. Ο υπεύθυνος επεξεργασίας μπορεί να ενημερώσει τον αποδέκτη των δεδομένων για τυχόν άρνηση του υποκειμένου να δώσει συγκατάθεση για την συλλογή ορισμένων δεδομένων του.[31]

1.3.10 Επεξεργασία προσωπικών δεδομένων μέσω πιστωτικών/χρεωστικών καρτών για ανέπαφες («contactless») συναλλαγές

Η Αρχή, με την απόφαση 48/2018, εξέτασε το ζήτημα της επεξεργασίας

[31]Απόφαση 50/2000 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

προσωπικών δεδομένων μέσω ανέπαφων συναλλαγών με χρεωστικές/πιστωτικές κάρτες, κατόπιν σχετικών καταγγελιών που διαβιβάστηκαν από τη Διεύθυνση Προστασίας Καταναλωτή του Υπουργείου Οικονομίας αλλά και από τον Συνήγορο του Καταναλωτή. Η Αρχή, με την ως άνω απόφαση, αφού εξέτασε ζητήματα ασφάλειας της εν λόγω επεξεργασίας, καθώς επίσης και τους σχετικούς κινδύνους, και λαμβάνοντας υπόψη και τις διεθνείς προδιαγραφές που ακολουθούνται αναφορικά με τις ανέπαφες χρεωστικές ή και πιστωτικές κάρτες, απηύθυνε σύσταση στις καταγγελλόμενες τράπεζες προκειμένου είτε να παρέχουν τη δυνατότητα απενεργοποίησης της ανέπαφης λειτουργίας μιας τέτοιας κάρτας είτε να χορηγούν νέα, μη ανέπαφη κάρτα, εφόσον ο πελάτης δηλώσει ότι δεν επιθυμεί να έχει κάρτα με δυνατότητα πραγματοποίησης ανέπαφων συναλλαγών. Περαιτέρω, στο πλαίσιο εξέτασης του εν λόγω ζητήματος, η Αρχή διαπίστωσε ότι σε ορισμένες περιπτώσεις τηρείται στο chip της κάρτας ιστορικό πρόσφατων συναλλαγών που πραγματοποιήθηκαν με χρήση αυτής, το οποίο μπορεί επίσης να αναγνωσθεί ανέπαφα. Ως προς το ζήτημα αυτό, η Αρχή, με την ως άνω Απόφαση, ζήτησε από τις τράπεζες το εξής: εφόσον σε κάρτα που έχει χορηγηθεί σε πελάτη είναι ενεργοποιημένη η δυνατότητα τήρησης ιστορικού συναλλαγών στο chip αυτής χωρίς να έχει δώσει την ειδική προς τούτο συγκατάθεσή του, θα πρέπει ο πελάτης να ενημερωθεί σχετικώς με κάθε πρόσφορο τρόπο (π.χ. μέσω μηνύματος ηλεκτρονικού ταχυδρομείου, μέσω μηνύματος κατά τη σύνδεσή του σε προσωποποιημένες ηλεκτρονικές υπηρεσίες του υπεύθυνου επεξεργασίας, μέσω ταχυδρομικής επιστολής κ.λπ.) ως προς την επεξεργασία αυτή, παρέχοντάς του τη δυνατότητα διακοπής της επεξεργασίας αυτής. Περαιτέρω, σε κάθε νέα έκδοση/χορήγηση κάρτας, το εν λόγω χαρακτηριστικό θα πρέπει να είναι εξ αρχής απενεργοποιημένο και να ενεργοποιείται μόνο αν υπάρχει ειδική προς τούτο συγκατάθεση του πελάτη, εφόσον έχει προηγουμένως σχετικώς ενημερωθεί για την επεξεργασία αυτή.[32]

1.3.11 Τιτλοποίηση απαίτησης τραπεζών (υποχρέωση ενημέρωσης οφειλετών)

Υποβλήθηκε στην Αρχή καταγγελία κατά του Ταμείου Παρακαταθηκών και Δανείων σχετικά με παράνομη επεξεργασία δεδομένων δανειολήπτη που συνίσταται σε τιτλοποίηση απαίτησης, η οποία έγινε το 2006 χωρίς ιδιαίτερη αιτία, κατά τον προσφεύγοντα, καθώς επρόκειτο για «υγιές» δάνειο. Η Αρχή απηύθυνε προειδοποίηση στο Ταμείο Παρακαταθηκών και Δανείων, για μη τήρηση της υποχρέωσης προηγούμενης ενημέρωσης οφειλέτη για την τιτλοποίηση οφειλής του, με αποτέλεσμα ο τελευταίος να υποστεί οικονομική βλάβη και συγκεκριμένα να στερηθεί της δυνατότητάς του να κάνει χρήση ευνοϊκότερων για εκείνον διατάξεων προκειμένου να αντιμετωπίσει τη

[32] Απόφαση 48/2018 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

σχετική οφειλή του προς το Ταμείο Παρακαταθηκών και Δανείων. Σημειωτέο, για την ως άνω τιτλοποίηση ο προσφεύγων δανειολήπτης ενημερώθηκε το 2016 από τυχαίο γεγονός και συγκεκριμένα, όταν αιτήθηκε τη μείωση των επιτοκίων της ως άνω δανειακής σύμβασης βάσει ευνοϊκών ρυθμίσεων. Ο προσφεύγων ενημερώθηκε από το Ταμείο Παρακαταθηκών και δανείων ότι δεν δικαιούταν της ευνοϊκότερης μεταχείρισης λόγω της τιτλοποίησης της δανειακής του σύμβασης. Όταν δε ο προσφεύγων ζήτησε διευκρινίσεις αναφορικά με την εν λόγω τιτλοποίηση και, ιδίως, για τους λόγους αυτής, η απάντηση που έλαβε κατά τους ισχυρισμούς του ήταν ότι «πουλήθηκε ως σίγουρο δάνειο».

Η Αρχή, με τη με αριθ. 71/2018 απόφασή της, δέχθηκε ότι σύμφωνα με το άρθρο 14 παρ. 12 του ν. 2801/2000 είναι επιτρεπτή η μεταβίβαση εσόδων του Ταμείου Παρακαταθηκών και Δανείων, κατά τις ειδικότερες ρυθμίσεις που ορίζονται με το άρθρο 9 του ν. 3453/2006. Ειδικότερα, ο νόμος ορίζει ότι η επεξεργασία προσωπικών δεδομένων οφειλετών κατά το μέτρο που είναι αναγκαία για τους σκοπούς τιτλοποίησης απαιτήσεων κατά τον νόμο αυτόν γίνεται σύμφωνα με τον ν. 2472/1997 (ΦΕΚ 50 Α`) και δεν προϋποθέτει προηγούμενη άδεια της Αρχής ή συναίνεση του οφειλέτη[33].

Αναφορικά δε με το ζήτημα της υποχρεωτικής ή μη προηγούμενης ενημέρωσης των δανειοληπτών, ως υποκειμένων των δεδομένων, σε περίπτωση τιτλοποίησης δανείων, η Αρχή έχει δεχθεί [34] ότι η σύμβαση μεταβίβασης των τιτλοποιούμενων επιχειρηματικών απαιτήσεων καταχωρίζεται στο δημόσιο βιβλίο του άρθρου 3 του ν. 2844/2000 σε περίληψη που περιέχει τα ουσιώδη στοιχεία αυτής.[35] Από την καταχώριση της σχετικής σύμβασης επέρχεται η μεταβίβαση των τιτλοποιούμενων απαιτήσεων, εκτός αν άλλως ορίζεται στους όρους της σύμβασης, η δε μεταβίβαση (εκχώρηση) αναγγέλλεται εγγράφως από τον μεταβιβάζοντα ή την εταιρία ειδικού σκοπού στον οφειλέτη.[36] Συνεπώς, η ως άνω εγγραφή της σύμβασης στο δημόσιο βιβλίο συνιστά κατά το άρθρο 10 παρ. 10 του ν. 3156/2003 αναγγελία της σύμβασης εκχώρησης προς τον οφειλέτη μη απαιτούμενης έγγραφης αναγγελίας της εκχώρησης από την μεταβιβάσασα εταιρία ή την εταιρία ειδικού σκοπού προς τον οφειλέτη. Ως εκ τούτου, δεδομένου ότι οι ειδικότερες διατάξεις για την τιτλοποίηση απαιτήσεων ορίζουν ότι αρκεί και ισχύει ως αναγγελία (ενημέρωση) η καταχώριση της σχετικής σύμβασης στο δημόσιο βιβλίο, πρέπει να γίνει δεκτό ότι δεν απαιτείται στην περίπτωση αυτή σύμφωνα με τις ειδικές διατάξεις και άλλου είδους προηγούμενη ατομική ενημέρωση. Συνιστάται, πάντως, κατά τον χρόνο της συλλογής των δεδομένων ο υπεύθυνος επεξεργασίας που προχωρεί σε

[33] Άρθρο 10 παρ. 1, 9, 10, 21 και 22 του ν. 3156/2003
[34] Ετήσια Έκθεση 2014 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 3.6.2. Τιτλοποίηση απαίτησης τραπεζών
[35] Άρθρο 10 παρ. 8 του ν. 3156/2003
[36] Άρθρο 10 παρ. 9 του ν. 3156/2003

τιτλοποίηση της απαίτησής του, δηλαδή η τράπεζα ή άλλος χρηματοπιστωτικός οργανισμός, να περιλαμβάνει στο περιεχόμενο της ενημέρωσης στην οποία προβαίνει, κατά το άρθρο 11 παρ. 1 του ν. 2472/1997, ως κατηγορία αποδεκτών, τις εταιρίες ειδικού σκοπού για την περίπτωση τιτλοποίησης απαιτήσεων και, πάντως, το αργότερο μετά την τιτλοποίηση της απαίτησης ο ανωτέρω υπεύθυνος επεξεργασίας ή η εταιρία ειδικού σκοπού πρέπει να ενημερώνει σχετικά ατομικώς τον οφειλέτη (π.χ. με την αποστολή του σχετικού λογαριασμού του). Και τούτο διότι από τη συστηματική ερμηνεία των προαναφερόμενων διατάξεων προκύπτει ότι οι ειδικότερες διατάξεις για την τιτλοποίηση απαιτήσεων αίρουν την υποχρέωση ενημέρωσης του άρθρου 11 παρ. 3 ν. 2472/1997 μόνο κατά το αναγκαίο για να εφαρμοστούν περιεχόμενό τους και όχι την ίδια την υποχρέωση ενημέρωσης. Τούτο είναι σύμφωνο και με την υποχρέωση ενημέρωσης, όπως αυτή προβλέπεται στην Οδηγία 95/46/ΕΚ[37], την οποία Οδηγία ενσωμάτωσε στο ελληνικό δίκαιο ο ν. 2472/1997, αλλά και πλέον με τον Γενικό Κανονισμό για την Προστασία Δεδομένων.[38] Στη συγκεκριμένη δε περίπτωση, η Αρχή επέβαλε την κύρωση της προειδοποίησης στο Ταμείο Παρακαταθηκών και Δανείων, σύμφωνα με το άρθρο 21 παρ. 1 εδ. α΄ του ν. 2472/1997, για εφεξής τήρηση της υποχρέωσης[39] προσήκουσας ενημέρωσης οφειλετών σε περίπτωση τιτλοποίησης οφειλής τους.

1.3.12 Νομιμότητα υποχρεωτικής καταγραφής τηλεφωνικών συνομιλιών και δικαίωμα πρόσβασης του υποκειμένου των δικαιωμάτων σε αυτές.

Με την απόφαση 72/2013 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επισημάνθηκε ότι κατά το δίκαιο της Ε.Ε., επιτρέπεται, ιδίως όταν προβλέπεται από νόμο, η καταγραφή συνομιλιών προς το σκοπό της απόδειξης εμπορικής συναλλαγής ή επαγγελματικής επικοινωνίας, και μάλιστα το άλλο μέρος της επικοινωνίας θα πρέπει να ενημερώνεται για την καταγραφή, το σκοπό της καθώς και το χρόνο αποθήκευσης των δεδομένων.[40]Η διάταξη αυτή μεταφέρθηκε και στο ελληνικό δίκαιο, στο άρθρο 4 παρ. 3 του ν. 3471/2006, σύμφωνα με το οποίο η καταγραφή τηλεφωνικών συνομιλιών επιτρέπεται ενόψει του ανωτέρω σκοπού. Διευκρινίστηκε ότι, σύμφωνα με τη συμπληρωματικώς εφαρμοζόμενη γενική αρχή του άρθρου 4 παρ. 1 του ν. 2472/1997, τα δεδομένα θα πρέπει να τηρούνται για όσο χρόνο απαιτείται για την επίτευξη του ως άνω σκοπού.

Με βάση τα προαναφερθέντα, κρίθηκε ότι η διάταξη του άρθρου 18 του ν. 3340/2005 είναι σύμφωνη με το ενωσιακό δίκαιο και τις σχετικές διατάξεις

[37] Άρθρο 11 της Οδηγίας 95/46/ΕΚ
[38] Άρθρα 12, 13 και 14 του Γ.Κ.Π.Δ. (ΕΕ) 2016/679
[39]Απόφαση 33/2018 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για εξατομικευμένη πληροφόρηση
[40] άρθρο 5 παρ. 2 και Αιτιολογική Σκέψη 23 της Οδηγίας 2002/58/ΕΚ σχετικά με την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.

του ν. 2472/1997 και του ν. 3471/2006. Το άρθρο 18 του ν. 3340/2005 ορίζει ότι τα πρόσωπα που διαμεσολαβούν κατ' επάγγελμα στην κατάρτιση συναλλαγών, υποχρεούνται να καταγράφουν και να αρχειοθετούν όλες τις εντολές που δίνουν οι πελάτες τους για κατάρτιση συναλλαγών επί χρηματοπιστωτικών μέσων (ιδίως να ηχογραφούν τις εντολές που δίδονται τηλεφωνικώς), να τηρούν τα σχετικά δεδομένα για τουλάχιστον ένα έτος και, ύστερα από σχετική απόφαση της Επιτροπής Κεφαλαιαγοράς, εφόσον διενεργείται έρευνα για κατάχρηση της αγοράς, για πρόσθετη περίοδο που δεν μπορεί να υπερβαίνει τα δύο έτη, καθώς και να ενημερώνουν τους καλούντες κατά την έναρξη της τηλεφωνικής συνομιλίας ότι η τηλεφωνική συνομιλία καταγράφεται για λόγους προστασίας των συναλλαγών.

Δικαίωμα πρόσβασης σε καταγεγραμμένες συνομιλίες με υπαλλήλους τράπεζας

Υποβλήθηκε στην Αρχή καταγγελία κατά τράπεζας για μη ικανοποίηση δικαιώματος πρόσβασης σε καταγεγραμμένες συνομιλίες. Συγκεκριμένα, ο προσφεύγων δέχθηκε στα γραφεία της επιχείρησής του τηλεφωνική όχληση από τράπεζα σχετικά με οφειλή του από επιχειρηματικό δάνειο. Στο τηλεφώνημα όμως αυτό δεν απάντησε ο προσφεύγων, ο οποίος είναι ο οφειλέτης, αλλά τρίτο πρόσωπο , το οποίο δεν έχει καμία σχέση με την εν λόγω οφειλή και βρισκόταν συμπωματικά στο γραφείο του προσφεύγοντος. Ο προσφεύγων καταγγέλλει ότι, με την ενέργεια αυτή της τράπεζας, έτυχαν παράνομης επεξεργασίας τα προσωπικά του δεδομένα και πλήττεται και η επιχείρηση του, καθώς το τρίτο αυτό πρόσωπο, ο οποίος είναι εμμέσως και ανταγωνιστής του, ενημερώθηκε πλήρως για την οικονομική του κατάσταση δηλώνοντας ψευδώς στον συνομιλητή του (υπάλληλο τράπεζας) ότι είναι ο πατέρας του προσφεύγοντος, ο οποίος τυγχάνει να είναι εγγυητής στο προαναφερθέν επιχειρηματικό του δάνειο. Ακολούθως, ο προσφεύγων απευθύνθηκε εγγράφως στην τράπεζα και ζήτησε να λάβει αντίγραφα δυο συνομιλιών με υπαλλήλους της σχετικά με το συγκεκριμένο περιστατικό. Ωστόσο, η τράπεζα δεν ανταποκρίθηκε στα αιτήματα αυτά. Η Αρχή, εν προκειμένω, δέχθηκε ότι το αίτημα του προσφεύγοντος ασκήθηκε εγγράφως και ήταν ορισμένο και σαφές (αποστολή αντιγράφων δυο συγκεκριμένων συνομιλιών), ενώ η τράπεζα ούτε εκπλήρωσε εμπροθέσμως την αντίστοιχη υποχρέωσή της να απαντήσει εγγράφως με σαφήνεια και πληρότητα (σχετικά με τη μη καταγραφή της πρώτης συνομιλίας και με την αποστολή της δεύτερης καταγεγραμμένης συνομιλίας) ούτε κοινοποίησε την απάντησή της στην Αρχή, ενημερώνοντας τον ενδιαφερόμενο ότι μπορεί να προσφύγει σε αυτήν.[41] Η Αρχή, με τη με αριθ. 47/2018 απόφασή της, επέβαλε στην τράπεζα πρόστιμο ύψους δέκα χιλιάδων (10.000) ευρώ για μη εκπλήρωση της υποχρέωσής της να απαντήσει στον προσφεύγοντα εντός της προβλεπόμενης προθεσμίας της, παραβιάζοντας το κατ' άρθρο 12 του ν. 2472/1997 δικαίωμα

[41] Άρθρο 12 παρ. 2 και 4 του ν. 2472/1997

πρόσβασής του. Επίσης, στην ίδια απόφαση η Αρχή απηύθυνε στην τράπεζα τη σύσταση, κατά την τηλεφωνική επικοινωνία με πελάτες της, να μεριμνά για την ταυτοποίηση του συνομιλητή, προτού προχωρήσει σε συνομιλία σχετικά με δεδομένα συναλλαγών ή οφειλών του ιδίου ή προσώπων που συνδέονται με τις συναλλαγές ή οφειλές αυτού (φυσικών προσώπων που έχουν την ιδιότητα του εγγυητή, ενεχυρούχου ή υποθηκικού οφειλέτη).

1.3.13 Εταιρίες Ενημέρωσης Οφειλετών

Σύμφωνα με το σχετικό νομοθετικό πλαίσιο[42], όταν ο οφειλέτης δεν εκπληρώνει τις οικονομικές του υποχρεώσεις και καθίσταται υπερήμερος, ο δανειστής (πιστωτικό ίδρυμα, έμπορος κ.ά.) έχει το δικαίωμα να επεξεργαστεί προσωπικά δεδομένα που τηρεί στο αρχείο του δυνάμει της μεταξύ τους σύμβασης με σκοπό να προβεί σε εξώδικες ενέργειες τόσο για να τον ενημερώσει για την ύπαρξη ληξιπρόθεσμων οφειλών όσο και για να διαπραγματευτεί μαζί του, για τον τρόπο, χρόνο και λοιπούς όρους αποπληρωμής, τη ρύθμιση ή τον διακανονισμό οφειλής. Επίσης, ο δανειστής δύναται να αναθέσει τις ως άνω ενέργειες σε Εταιρείες Ενημέρωσης Οφειλετών. Με το ν. 3758/2009 «Εταιρίες ενημέρωσης οφειλετών για ληξιπρόθεσμες απαιτήσεις και άλλες διατάξεις», όπως τροποποιήθηκε με το άρθρο 36 του ν. 4038/2012 και ισχύει, ρυθμίστηκε το πλαίσιο λειτουργίας των εταιρειών ενημέρωσης οφειλετών και ειδικότερα, μεταξύ άλλων, οι ειδικότερες υποχρεώσεις τους προς τους δανειστές και οι μεταξύ τους σχέσεις. Στο νόμο προβλέπεται ότι οι δανειστές έχουν δικαίωμα να χορηγούν στις εταιρείες ενημέρωσης οφειλετών στοιχεία σχετικά με ληξιπρόθεσμες απαιτήσεις έναντι των τελευταίων, χωρίς τη συγκατάθεσή τους, για τους προβλεπόμενους νόμιμους σκοπούς της ενημέρωσης των οφειλετών για την ύπαρξη ληξιπρόθεσμων οφειλών τους και τη διαπραγμάτευση του χρόνου, του τρόπου και των λοιπών όρων αποπληρωμής αυτών.[43]

Νομιμότητα επεξεργασίας από εταιρίες ενημέρωσης οφειλετών.

Η Αρχή με το με αρ. πρωτ. Γ/ΕΞ/73-1/28-01-2013 έγγραφό διευκρίνισε σχετικά με τη νομιμότητα τήρησης και χρήσης των στοιχείων επικοινωνίας των οφειλετών από τις εταιρείες ενημέρωσης οφειλετών ότι με τον ν. 3758/2009, πέραν του ότι προβλέπεται ότι οι δανειστές έχουν δικαίωμα υπό συγκεκριμένους όρους να χορηγούν στις εταιρείες ενημέρωσης οφειλετών στοιχεία σχετικά με ληξιπρόθεσμες απαιτήσεις έναντι των τελευταίων, ρυθμίζονται το πλαίσιο λειτουργίας των εταιριών ενημέρωσης οφειλετών και οι ειδικότερες υποχρεώσεις που συνεπάγεται η υπηρεσία αυτή, τόσο για τις ως άνω εταιρείες όσο και για τους δανειστές.

Απουσία συγκατάθεσης οφειλέτη για διαβίβαση δεδομένων του σε εταιρία

[42] ν. 3758/2009 «Εταιρείες ενημέρωσης οφειλετών για ληξιπρόθεσμες απαιτήσεις και άλλες διατάξεις» και άρθρο 36 του ν. 4038/2012
[43] Άρθρα 3 παρ. 3, 4 παρ. 2, 8 παρ. 3 ν. 3758/2009, όπως τροποποιήθηκε και ισχύει

ενημέρωσης οφειλετών.

Επί επιτρεπτής επεξεργασίας, όπως στην περίπτωση επεξεργασίας αναγκαίας για την εκτέλεση σύμβασης,[44] η χορήγηση/ανακοίνωση των στοιχείων οφειλετών από τον δανειστή-υπεύθυνο επεξεργασίας προς την εκάστοτε συνεργαζόμενη με αυτόν εταιρεία ενημέρωσης οφειλετών-εκτελούσα την επεξεργασία επιτρέπεται και χωρίς τη συγκατάθεση του οφειλέτη-υποκειμένου των δεδομένων, με την προϋπόθεση ότι ο δανειστής έχει ενημερώσει με σαφήνεια τον οφειλέτη για την κατηγορία αυτή αποδεκτών των δεδομένων του. Σε κάθε περίπτωση, οι υποχρεώσεις για το απόρρητο και την ασφάλεια της επεξεργασίας πρέπει να τηρούνται απαρεγκλίτως και τα προσωπικά δεδομένα να μην χρησιμοποιούνται για άλλους σκοπούς. [45]

Έλεγχος ορθότητας στοιχείων πριν την χορήγηση τους στην εταιρία ενημέρωσης οφειλετών

Στο με αριθμ. πρωτ. Γ/ΕΞ/4744/12-07-2013 έγγραφό της η Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα επισήμανε ότι ο δανειστής οφείλει να επεξεργάζεται ακριβή στοιχεία για τον οφειλέτη. Συνεπώς, ο δανειστής πρέπει να επιβεβαιώνει τις οφειλές και να έχει προβεί σε ταυτοποίηση του οφειλέτη πριν από οποιαδήποτε ενέργεια ενημέρωσης οφειλετών από τον ίδιο ή πριν από την ανακοίνωση των στοιχείων σε εταιρεία ενημέρωσης οφειλετών. Η επικαιροποίηση του σχετικού αρχείου μπορεί να γίνει με κάθε πρόσφορο τρόπο, όπως για παράδειγμα με διασταύρωση των στοιχείων από δημόσια προσβάσιμες πηγές, με τηλεφωνική επικοινωνία με τον οφειλέτη ή με αποστολή σχετικής επιστολής για την επιβεβαίωση των στοιχείων. Σε περίπτωση δε που διαπιστωθεί ότι τα στοιχεία που είχαν δηλωθεί στον δανειστή είναι λανθασμένα ή ψευδή το βάρος για την εύρεση των αληθών στοιχείων του οφειλέτη φέρει ο δανειστής. Συνεπώς, δεν επιτρέπεται να ζητείται από τους πολίτες να προσκομίζουν έγγραφα για να αποδείξουν ότι πράγματι δεν έχουν καμία σχέση με τον οφειλέτη ή την οφειλή (για παράδειγμα, όταν ο καλούμενος πολίτης δηλώνει στο δανειστή ότι ουδεμία σχέση έχει με τον οφειλέτη ή την οφειλή ή ότι ο οφειλέτης δεν διαμένει πια στη συγκεκριμένη οικία). Ως απόδειξη για την ανακρίβεια των στοιχείων και μέχρι την εύρεση των αληθών μπορεί να τηρείται από τον δανειστή η συνομιλία με το πρόσωπο που δήλωσε π.χ. ότι δεν είναι ο ίδιος οφειλέτης ή ότι ο συγκεκριμένος αριθμός τηλεφώνου δεν ανήκει πια στον οφειλέτη επειδή διαμένει αλλού.[46]

Πρότερη ενημέρωση του οφειλέτη.

[44] Άρθρο 5 παρ. 2 στοιχ. α΄ του Ν. 2472/1997
[45] Υπ' αριθμ. πρωτ. Γ/ΕΞ/73-1/28-01-2013 έγγραφό της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[46] Υπ' αριθμ. πρωτ. Γ/ΕΞ/4744/12-07-2013 έγγραφό της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Σύμφωνα με το με αριθμ. πρωτ. Γ/ΕΞ/4744/12-07-2013 έγγραφό τηςΑρχής Προστασίας Δεδομένων Προσωπικού χαρακτήρα ο δανειστής έχει υποχρέωση ενημέρωσης του οφειλέτη για την ανακοίνωση των δεδομένων του σε εταιρείες ενημέρωσης οφειλετών. Η ενημέρωση αυτή μπορεί να πραγματοποιείται κατά τη σύναψη της σύμβασης με τον πελάτη, δηλαδή η ενημέρωση πρέπει να συμπεριληφθεί στο ίδιο το κείμενο της σύμβασης, στο οποίο πρέπει να καθίσταται σαφές ότι ο δανειστής έχει δικαίωμα με βάση το Ν. 3758/2009, σε περίπτωση που η οφειλή καταστεί ληξιπρόθεσμη, να ανακοινώσει τα δεδομένα του πελάτη σε εταιρεία ενημέρωσης οφειλετών με σκοπό τη σχετική ενημέρωσή του σύμφωνα με τους όρους του ως άνω νόμου. Συνεπώς, οι όροι συμβάσεων που περιέχουν αόριστες ή ανακριβείς διατυπώσεις πρέπει να τροποποιηθούν αναλόγως. Επισημαίνεται δε ότι οι παλαιοί πελάτες, δηλαδή εκείνοι που υπέγραψαν συμβάσεις με τους δανειστές πριν από την έναρξη ισχύος του Ν. 3758/2009, πρέπει να ενημερώνονται για την εν λόγω νέα επεξεργασία με τρόπο πρόσφορο και σαφή, για παράδειγμα με συστημένη επιστολή που θα περιλαμβάνει την ανωτέρω πληροφόρηση ή με ενσωμάτωση της σχετικής πληροφόρησης στα αντίγραφα λογαριασμών.

Η ενημέρωση μπορεί να πραγματοποιείται εναλλακτικά κατά την τελευταία έγγραφη ενημέρωση του οφειλέτη ότι η οφειλή του κατέστη ληξιπρόθεσμη και ότι, σε περίπτωση μη τακτοποίησης αυτής, τα δεδομένα του θα ανακοινωθούν σε εταιρεία ενημέρωσης οφειλετών με σκοπό τη σχετική ενημέρωσή του σύμφωνα με τον Ν. 3758/2009. Στο στάδιο αυτό, προτείνεται να ζητείται από τον οφειλέτη να διατυπώσει τυχόν αντιρρήσεις του σχετικά με την ακρίβεια των στοιχείων του, ιδίως ύψος της οφειλής και στοιχεία επικοινωνίας, εντός ευλόγου προθεσμίας, έτσι ώστε να πραγματοποιείται ταυτόχρονα και η ενημέρωση των δεδομένων στο αρχείο που τηρεί ο δανειστής.

Στην περίπτωση ανάθεσης της δικαστικής επιδίωξης της απαίτησης από δικηγορικά γραφεία, επειδή δεν υπάρχει ειδική εκ του νόμου υποχρέωση για την καταγραφή των συνομιλιών και έτσι δεν μπορεί να αποδειχθεί ευχερώς αν πραγματοποιήθηκε παράνομη όχληση στο πλαίσιο εκτέλεσης της εντολής για δικαστική επιδίωξη της απαίτησης, την ευθύνη τόσο για την ακρίβεια των στοιχείων που ανακοινώνουν στους δικηγόρους τους όσο και για λοιπές παραβάσεις του Ν. 3758/2009 σε συνδυασμό με τη νομοθεσία για την προστασία προσωπικών δεδομένων κατά την επικοινωνία φέρουν οι ίδιοι οι δανειστές ως υπεύθυνοι επεξεργασίας. Συνεπώς, οι δανειστές θα πρέπει να αποδεικνύουν ότι χορήγησαν στους δικηγόρους τους ακριβή στοιχεία, ήτοι ότι τα φερόμενα στην εκάστοτε καταγγελία ως ανακριβή στοιχεία είναι ακριβή, ή ότι διόρθωσαν αμέσως τα ανακριβή και ενημέρωσαν σχετικά και τον δικηγόρο τους, καιότι η εντολή που έδωσαν στον δικηγόρο τους περιορίστηκε στη δικαστική επιδίωξη της απαίτησης και ότι ουδεμία ενέργεια πραγματοποιήθηκε κατά παράβαση της νομοθεσίας για την προστασία

προσωπικών δεδομένων ή/και του Ν. 3758/2009. Μετά την εκ μέρους του δανειστή κοινοποίηση στο δικηγόρο της δήλωσής του ότι η εντολή περιορίζεται στη δικαστική και μόνο επιδίωξη της απαίτησης και εφεξής, ο εντολοδόχος θα υπέχει ιδία ευθύνη για οποιαδήποτε επεξεργασία επιχειρήσει πέραν της εντολής. [47]

Και με την υπ' αριθ. 98/2017 απόφαση[48] της Αρχής Προσωπικών Δεδομένων Προσωπικού χαρακτήρα κρίθηκε υποχρεωτική η ατομική ειδική ενημέρωση οφειλετών για τη διάθεση των δεδομένων τους από τους δανειστές σε εταιρείες ενημέρωσης οφειλετών. Ο δανειστής, ως υπεύθυνος επεξεργασίας φέρει την υποχρέωση να ενημερώνει για τη διάθεση των δεδομένων στην εκάστοτε συγκεκριμένη Εταιρεία Ενημέρωσης Οφειλετών, να παρέχει ένα εύλογο διάστημα (ενδεικτικά, 10-15 ημερών) πριν από τη διάθεση για την άσκηση των δικαιωμάτων πρόσβασης και αντίρρησης και να μεριμνήσει ώστε η ενημέρωση αυτή να γίνεται με κάθε πρόσφορο τρόπο, π.χ. με ενσωμάτωση της σχετικής πληροφόρησης στα αντίγραφα λογαριασμών και σε ευδιάκριτο σημείο αυτών ή μέσω ηλεκτρονικού ταχυδρομείου (e-mail), σε όλες τις περιπτώσεις, στις οποίες τούτο καθίσταται εφικτό, και ιδίως εφόσον τα σχετικά στοιχεία έχουν χορηγηθεί στον υπεύθυνο επεξεργασίας από τα υποκείμενα των δεδομένων. Αυτονόητο είναι ότι ο δανειστής, ως υπεύθυνος επεξεργασίας, οφείλει να ενημερώνει εκ νέου, σύμφωνα με τα παραπάνω, κάθε φορά που τα στοιχεία των οφειλετών του διατίθενται σε διαφορετική Εταιρεία Ενημέρωσης Οφειλετών.

Καταγεγραμμένες τηλεφωνικές συνομιλίες και νομιμότητα επεξεργασίας δεδομένων τρίτων προσώπων-μη οφειλετών στο πλαίσιο ενημέρωσης οφειλετών για ληξιπρόθεσμες απαιτήσεις

Σχετικά με τη νομιμότητα επεξεργασίας δεδομένων τρίτων προσώπων-μη οφειλετών στο πλαίσιο ενημέρωσης οφειλετών για ληξιπρόθεσμες απαιτήσεις η Αρχή, με το με αριθμ. πρωτ. Γ/ΕΞ/1325-1/12-07-2013 έγγραφό της, διασαφήνισε ότι τόσο η υποχρέωση τήρησης ηλεκτρονικού αρχείου με τα εξωτερικά στοιχεία κάθε πραγματοποιηθείσας επικοινωνίας, όσο και η υποχρέωση τήρησης αρχείου με το περιεχόμενο των καταγεγραμμένων συνομιλιών, έχουν θεσμοθετηθεί με σκοπό να καταστεί πρακτικά δυνατός ο έλεγχος της συμμόρφωσης των δανειστών και των εταιριών ενημέρωσης

[47] αριθμ. πρωτ. Γ/ΕΞ/4744/12-07-2013 έγγραφό τηςΑρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

[48] Αναφέρουμε ότι η τράπεζα υπέβαλε αίτηση θεραπείας κατά της με αριθ. 98/2017 Απόφασης της Αρχής, η οποία απορρίφθηκε με την αριθ. 39/2019 Απόφαση της Αρχής.
Επίσης, η Ένωση Ελληνικών Τραπεζών ισχυρίζεται ότι η Απόφαση 98/2017 με το συγκεκριμένο περιεχόμενο που θεσπίζει δεν ισχύει υπό το καθεστώς του ΓΚΠΔ και ότι είναι αναγκαίο να αναθεωρηθεί.
Η αιτιολόγηση είναι πως οι Εταιρείες Ενημέρωσης Οφειλετών δεν είναι «τρίτοι» υπό την έννοια του άρθρου 2 στοιχ. θ΄ του ν. 2472/1997, και συνεπώς δεν τίθεται ζήτημα εφαρμογής της παρ. 3 του άρθρου 11 του ν. 2472/1997, αλλά εφαρμόζεται η παρ. 1 του ίδιου άρθρου, σύμφωνα με την οποία αρκεί η τράπεζα να ενημερώσει τα υποκείμενα των δεδομένων για τον αποδέκτη ή την κατηγορία αποδεκτών. Ομοίως σε αποδέκτες ή κατηγορίες αποδεκτών αναφέρεται και το άρθρο 13 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΕΕ) 2016/679.

οφειλετών με το ισχύον θεσμικό πλαίσιο, καθώς και ότι η καταγραφή των ως άνω δεδομένων είναι νόμιμη σύμφωνα με τις προαναφερθείσες διατάξεις του Ν. 3758/2009, αποτελεί δηλαδή εκ του νόμου υποχρέωση.[49]

Συνεπώς η καταγραφή κάθε επικοινωνίας με τρίτο πρόσωπο-μη οφειλέτη συνιστά επεξεργασία που είναι αναγκαία για την εκπλήρωση της εκ του Ν. 3758/2009 υποχρέωσης του υπευθύνου επεξεργασίας να παρέχει στη ΓΓΚ κάθε στοιχείο που αποδεικνύει τη συμμόρφωσή του με τις επιταγές του νόμου αυτού, ήτοι αν πραγματοποίησε την εν λόγω επικοινωνία σύμφωνα με τους όρους του άρθρου 4 του Ν. 3758/2009, αλλά και αν κατά την επικοινωνία αυτή όχλησε ή όχι οικεία πρόσωπα του οφειλέτη. Ο καλών οφείλει να ενημερώνει τόσο για την ιδιότητά του και τα λοιπά στοιχεία που προβλέπονται στο Ν. 3758/2009 όσο και το γεγονός της καταγραφής πριν από την έναρξη κάθε επικοινωνίας από οποιοδήποτε πρόσωπο και αν απαντηθεί η κλήση, δηλαδή είτε αυτή απαντηθεί από τον ίδιο τον οφειλέτη είτε από τρίτο πρόσωπο. Η καλούσα εταιρεία οφείλει κατ' αρχάς να βεβαιωθεί για την ταυτότητα του καλούμενου, δηλαδή αν πρόκειται για τον ίδιο τον οφειλέτη ή τρίτο πρόσωπο, και μόνο στην πρώτη περίπτωση να προβεί σε ενημέρωση σχετικά με την οφειλή, ενώ στη δεύτερη περίπτωση θα πρέπει να διακόψει τη συνομιλία. Ειδικότερα, στην τελευταία περίπτωση πρέπει να αποκαλύπτονται στο τρίτο πρόσωπο μόνο όσα στοιχεία είναι αναγκαία για τον σκοπό της ενημέρωσής του σχετικά με την καταγραφή και απαγορεύεται να ανακοινώνονται περαιτέρω στοιχεία σχετικά με την ίδια την οφειλή. Το ηλεκτρονικό αρχείο με τα εξωτερικά στοιχεία των τηλεφωνικών επικοινωνιών, αλλά και το αρχείο με τις ηχογραφημένες συνομιλίες περιέχουν απλά προσωπικά δεδομένα τόσο του τρίτου προσώπου όσο και του οφειλέτη, καθώς στην πρώτη περίπτωση (τρίτο πρόσωπο-οικείος του οφειλέτη) πρόκειται για το ίδιο το πρόσωπο που συνομιλεί, ενώ στη δεύτερη περίπτωση (οφειλέτης) το περιεχόμενο της συνομιλίας αφορά κατεξοχήν στον οφειλέτη και δη στην αναζήτησή του. Συνεπώς, το τρίτο πρόσωπο-οικείος του οφειλέτη και ο οφειλέτης, ως υποκείμενα των δεδομένων, έχουν δικαίωμα πρόσβασης στα δεδομένα που τους αφορούν και περιέχονται στο σύνολο των ηχογραφημένων αυτών συνομιλιών.

Δεδομένου ότι ο σκοπός του Ν. 3758/2009 όπως ισχύει είναι, όπως προαναφέρθηκε, η κατά το δυνατόν αποτελεσματικότερη εποπτεία των δανειστών και των εταιριών ενημέρωσης οφειλετών και κατά συνέπεια η μέγιστη δυνατή προστασία του οφειλέτη, η καταγραφή μηνυμάτων στον αυτόματο τηλεφωνητή του οφειλέτη δεν αντίκειται στη νομοθεσία για την προστασία δεδομένων προσωπικού χαρακτήρα.

Όχληση σε λάθος πρόσωπο.

Σχετικά με την υποχρέωση της τράπεζας, ως υπεύθυνου επεξεργασίας, να

[49] άρθρο 5 παρ. 2 στοιχ. β΄ του Ν. 2472/1997

ελέγχει τα στοιχεία/δεδομένα ως προς την ακρίβειά τους και να τα υποβάλλει σε τακτική ενημέρωση και επικαιροποίηση, η Αρχή έχει εκδώσει τις αποφάσεις 55/2018 , 56/2018 και 57/2018, με τις οποίες επέβαλε πρόστιμο σε τρεις τράπεζες για μη εκπλήρωση της υποχρέωσής τους να τηρούν και να επεξεργάζονται περαιτέρω ακριβή στοιχεία για τους οφειλέτες της προς εκπλήρωση των προβλεπόμενων από το ν. 3758/2009 σκοπών. Οι υποθέσεις αφορούσαν όχληση τρίτων με τηλεφωνική κλήση στο πλαίσιο ενημέρωσης οφειλετών για ληξιπρόθεσμες απαιτήσεις, για τους οποίους καταχωρήθηκε λανθασμένος ή μη επικαιροποιημένος αριθμός επικοινωνίας, δηλαδή ο τηλεφωνικός αριθμός ανήκε στο παρελθόν σε οφειλέτη ή δόθηκε από τους ίδιους τους οφειλέτες κατά την κατάρτιση της σύμβασης και δεν επιβεβαιώθηκε.

Οι τράπεζες κατά κανόνα μεριμνούν[50] για την ενημέρωση των πελατών τους σχετικά με την ανάγκη επικαιροποίησης των στοιχείων τους σε τακτά χρονικά διαστήματα μέσω διάθεσης ειδικού εντύπου «Συστηθήκατε» της Ελληνικής Ένωσης Τραπεζών στους χώρους υποδοχής των καταστημάτων της, μέσω ηχογραφημένου μηνύματος σε συναλλαγές με Phone Banking, μέσω ηλεκτρονικών μηνυμάτων σε συναλλαγές με E-Banking και με εξατομικευμένη ενημέρωση στα καταστήματα όταν διαπιστώνεται επ' ευκαιρία της διενεργούμενης συναλλαγής ότι τα στοιχεία τους είναι ελλιπή. Σημειώνεται ότι στις συμβάσεις δανειακών προϊόντων ή/και υπηρεσιών περιλαμβάνεται κατά κανόνα όρος, σύμφωνα με τον οποίο ο αντισυμβαλλόμενος, καταθέτης ή οφειλέτης, υποχρεούται να γνωστοποιήσει στην τράπεζα άμεσα κάθε αλλαγή των στοιχείων επικοινωνίας του (συμβατική υποχρέωση). Θεσμική δε υποχρέωση προκύπτει τόσο από τον ορισμό του συνεργάσιμου δανειολήπτη, όσο και από τον Κώδικα Δεοντολογίας της Τράπεζας της Ελλάδος. Σε περίπτωση δε που διαπιστωθεί ότι τα στοιχεία που είχαν δηλωθεί στον δανειστή είναι λανθασμένα ή ψευδή (για παράδειγμα, όταν ο καλούμενος πολίτης δηλώνει στον δανειστή ότι ουδεμία σχέση έχει με τον οφειλέτη ή την οφειλή ή ότι ο οφειλέτης δεν διαμένει πια στη συγκεκριμένη οικία), πρέπει να καταχωρείται το αίτημα αντίρρησης ή διόρθωσης από τις Εισπρακτικές Εταιρίες, να διαβιβάζεται άμεσα στον δανειστή για λογαριασμό του οποίου γίνεται η επικοινωνία και να γίνονται άμεσα όλες οι απαραίτητες διορθωτικές ενέργειες. Πρέπει να γίνεται άμεσα σηματοδότηση του συγκεκριμένου τηλεφωνικού αριθμού, ώστε να μην χρησιμοποιηθεί στο μέλλον για σκοπό ενημέρωσης ή όχλησης για οφειλές τρίτου προσώπου (ως απόδειξη για την ανακρίβεια των στοιχείων και μέχρι την εύρεση των αληθών μπορεί να τηρείται από τον δανειστή η συνομιλία με το πρόσωπο που δήλωσε π.χ. ότι δεν είναι ο ίδιος οφειλέτης ή ότι ο συγκεκριμένος αριθμός τηλεφώνου δεν ανήκει πια στον οφειλέτη επειδή διαμένει αλλού). Εάν διαπιστώνεται από δημόσια προσβάσιμες πηγές ή από στοιχεία που προσκομίζει στον δανειστή ο

[50] Απόφαση 55/2018 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

καλούμενος τρίτος μη οφειλέτης (π.χ. αντίγραφο λογαριασμού ή έγγραφο παρόχου για τον τηλεφωνικό του αριθμό), τότε πρέπει να διαγράφεται άμεσα και οριστικά ο συγκεκριμένος τηλεφωνικός αριθμός που δόθηκε από τον οφειλέτη και να ενημερώνεται με κάθε πρόσφορο τρόπο, ει δυνατόν εγγράφως, ο ως άνω καλούμενος τρίτος μη οφειλέτης που ζητεί να διορθωθούν τα τηρούμενα στοιχεία και να σταματήσουν οι οχλήσεις στον δικό του αριθμό. Η Αρχή, με τις με αριθ. 55/2018, 56/2018 και 57/2018 αποφάσεις της, επέβαλε σε τρεις τράπεζες τράπεζα πρόστιμα για μη εκπλήρωση της υποχρέωσής τους να τηρούν και να επεξεργάζονται περαιτέρω ακριβή στοιχεία για τους οφειλέτες τους προς εκπλήρωση των προβλεπόμενων από τον ν. 3758/2009 σκοπών στις ως άνω τρεις περιπτώσεις.

Υποχρέωση καταγραφής τηλεφωνικών κλήσεων

Με την απόφαση 53/2016 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα αποφάνθηκε ότι οι Εταιρείες Ενημέρωσης Οφειλετών, για τον σκοπό ελέγχου της δραστηριότητάς τους από τη Γενική Γραμματεία Εμπορίου & Προστασίας Καταναλωτή, πρέπει[51] να καταγράφουν τις τηλεφωνικές κλήσεις, ήτοι το περιεχόμενο και τα εξωτερικά στοιχεία της επικοινωνίας, προς τους καλούμενους οφειλέτες, ανεξάρτητα από το ποιος απαντά την κλήση, δηλαδή ο οφειλέτης ή τρίτο πρόσωπο-μη οφειλέτης. Συγκεκριμένα, η Αρχή διαπίστωσε ότι ο σκοπός στην επικοινωνία με τον τρίτο δεν είναι η ενημέρωση του οφειλέτη για ληξιπρόθεσμες απαιτήσεις, αλλά απλώς η τηλεφωνική ανεύρεση του οφειλέτη. Ως εκ τούτου, η Αρχή χορήγησε άδεια για ενημέρωση των τρίτων-μη οφειλετών δια του Τύπου, καθώς έκρινε ότι η αρχή της αναλογικότητας και η αρχή του σκοπού επιτάσσουν η ενημέρωση των τρίτων-μη οφειλετών για την καταγραφή των τηλεφωνικών συνδιαλέξεων της εταιρείας με αυτούς, στο πλαίσιο αναζήτησης των οφειλετών, να γίνεται, όχι κατά την έναρξη της τηλεφωνικής συνομιλίας –όπως είχε κριθεί με την προσβαλλόμενη πράξη της– αλλά δια του Τύπου. Εξάλλου, στο αυτό συνηγορούν τα ακόλουθα: α) Η επίμαχη επικοινωνία που αφορά μόνο στην αναζήτηση του οφειλέτη διαρκεί ελάχιστα δευτερόλεπτα, και εάν ο οφειλέτης δεν είναι παρών και διαθέσιμος η επικοινωνία διακόπτεται αμέσως, έχει δε μικρή σημασία για τον καλούμενο (τρίτο-μη οφειλέτη) από απόψεως προστασίας προσωπικών δεδομένων (πολύ μεγαλύτερη για τον ίδιο τον οφειλέτη), και β) είναι μεγάλος ο αριθμός των προσώπων (πολλές χιλιάδες) που δέχονται παρόμοιες ανεπιτυχείς κλήσεις. Το ίδιο ισχύει και για τους δανειστές, όταν προβαίνουν σε επαναλαμβανόμενη ενημέρωση οφειλετών για τις ληξιπρόθεσμες απαιτήσεις τους.

1.3.14 Αιτήματα τραπεζών για χορήγηση αδειών ενημέρωσης δια

[51] Άρθρο 8 , παρ.2. ν. 3758/2009: « Οι εταιρίες καταγράφουν υποχρεωτικώς το περιεχόμενο κάθε τηλεφωνικής επικοινωνίας με τον οφειλέτη. Το περιεχόμενο της καταγραφής δεν επιτρέπεται να χρησιμοποιηθεί σε βάρος του οφειλέτη, δικαστικώς ή εξωδικαστικώς, και διατηρείται από Εταιρίες υποχρεωτικώς για ένα έτος από την πραγματοποίηση της επικοινωνίας.»

του Τύπου

Δια του τύπου ενημέρωση πελατών σχετικά με τη διαβίβαση των δεδομένων τους λόγω συγχώνευσης Τραπεζών.

Με τις αποφάσεις 38/2013 και 127/2013 της Αρχής Προστασίας προσωπικών δεδομένων επισημάνθηκαν τα ακόλουθα :

Τα στοιχεία των πελατών των υπό συγχώνευση τραπεζών, ήτοι στοιχεία ταυτοποίησης, καταναλωτικής πίστης, στεγαστικής πίστης και επαγγελματικής-επιχειρηματικής πίστης, εμπίπτουν στην έννοια των απλών προσωπικών δεδομένων. Περαιτέρω, οι υπό συγχώνευση τράπεζες τελούν, μέχρι την απορρόφησή τους από την αποκτώσα τράπεζα, σε σχέση θυγατρικών-μητρικής, ενώ σύμφωνα με το θεσμικό πλαίσιο εποπτείας σε ενοποιημένη βάση της Τράπεζας της Ελλάδος, η μητρική τράπεζα, ως εποπτευόμενο πιστωτικό ίδρυμα από την Τράπεζα της Ελλάδος, υποχρεούται να υποβάλλει οικονομικές καταστάσεις και για τις θυγατρικές της. Σε κάθε περίπτωση, όπως μπορεί να συναχθεί από το ίδιο θεσμικό πλαίσιο, η μητρική τράπεζα μπορεί και εντός του ιδίου ομίλου να ζητήσει από τη θυγατρική της τα σχετικά στοιχεία, προκειμένου να διαπιστώσει τη σωστή τήρηση των κανόνων χρηματοδότησης για τους σκοπούς εσωτερικού ελέγχου. Ως εκ τούτου, διαβιβάσεις των εν λόγω στοιχείων από τον έναν υπεύθυνο επεξεργασίας στον άλλον για τους ως άνω συμβατούς σκοπούς είναι επιτρεπτές και χωρίς τη συγκατάθεση των υποκειμένων των αντίστοιχων δεδομένων, καθώς πρόκειται για συμμόρφωση των τραπεζών αυτών με τις υποχρεώσεις εποπτείας τους. Επίσης, εφόσον α) η γνωστοποιούμενη διαβίβαση των υπό κρίση δεδομένων πρόκειται να γίνει για σκοπούς ενοποίησης των αρχείων των τριών τραπεζών ενόψει της επικείμενης απορρόφησης και τελικά της περιέλευσης των δεδομένων σε έναν υπεύθυνο επεξεργασίας, β) για την περιέλευση των σχετικών δεδομένων από τις υπό απορρόφηση τράπεζες μέχρι την ικανοποιητική επεξεργασία αυτών από την αποκτώσα τράπεζα για την ομαλή εξυπηρέτηση των υποκειμένων-πελατών θα απαιτηθεί χρονικό διάστημα τουλάχιστον 3-4 μηνών, και γ) τα δικαιώματα των υποκειμένων και οι θεμελιώδεις ελευθερίες τους δεν θίγονται από την εν λόγω επεξεργασία, συντρέχει νόμιμη περίπτωση για τη χορήγηση άδειας για τη δια του Τύπου ενημέρωση αναφορικά με τη διαβίβαση των υπό κρίση προσωπικών δεδομένων των πελατών των υπό συγχώνευση τραπεζών στην αποκτώσα τράπεζα πριν από το στάδιο της απορρόφησης.

Η ενημέρωση των πελατών των υπό συγχώνευση τραπεζών αφορά σε μεγάλο αριθμό υποκειμένων και, ως εκ τούτου, η ατομική και έγκαιρη ενημέρωσή τους καθίσταται δυσχερής, ενώ παράλληλα το κόστος σε χρόνο και τέλη των ατομικών ταχυδρομικών επιστολών είναι υψηλό. Συνεπώς, πληρούνται οι όροι σύμφωνα με τους οποίους επιτρέπεται η ενημέρωση των υποκειμένων

δια του Τύπου[52], με την επισήμανση ότι η εν λόγω ενημέρωση θα πρέπει να δημοσιευθεί σε δύο πανελλαδικής κυκλοφορίας εφημερίδες.

Για τους παραπάνω λόγους, η Αρχή χορήγησε[53] τις σχετικές άδειες στις αιτούσες και έκρινε ότι η ως άνω ενημέρωση πρέπει να αναρτηθεί και στους διαδικτυακούς τόπους όλων των εμπλεκόμενων τραπεζών.

Ενημέρωση οφειλετών στις περιπτώσεις τιτλοποίησης απαίτησης τραπεζών

Υποχρέωση ενημέρωσης οφειλετών

Όπως έχει προαναφερθεί στην ενότητα 1.3.11 «Τιτλοποίηση απαιτήσεων Τραπεζών», η Αρχή, έχει κρίνει[54] ότι η διαβίβαση των στοιχείων οφειλών από την τράπεζα στην εταιρεία ειδικού σκοπού μπορεί να θεωρηθεί αναγκαία για την εκπλήρωση υποχρέωσής της που επιβάλλεται από νόμο[55], τηρούνται δε και οι όροι και προϋποθέσεις του νόμου[56], ήτοι διαβίβαση απολύτως αναγκαία για την επιδίωξη και είσπραξη των σχετικών απαιτήσεων, η οποία υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των οφειλετών, χωρίς να θίγονται οι θεμελιώδεις ελευθερίες τους, εφόσον η επεξεργασία γίνεται στο πλαίσιο του νόμου 3156/2003 από περιορισμένο κύκλο αποδεκτών.

Ακολούθως, επισημαίνεται ότι η σύμβαση μεταβίβασης των τιτλοποιούμενων επιχειρηματικών απαιτήσεων καταχωρίζεται στο δημόσιο βιβλίο του άρθρου 3 του ν. 2844/2000 σε περίληψη που περιέχει τα ουσιώδη στοιχεία αυτής[57]. Από την καταχώριση της σχετικής σύμβασης επέρχεται η μεταβίβαση των τιτλοποιούμενων απαιτήσεων, εκτός αν άλλως ορίζεται στους όρους της σύμβασης, η δε μεταβίβαση (εκχώρηση) αναγγέλλεται εγγράφως από τον μεταβιβάζοντα ή την εταιρία ειδικού σκοπού στον οφειλέτη[58]. Συνεπώς, η ως άνω εγγραφή της σύμβασης στο δημόσιο βιβλίο συνιστά, κατά το άρθρο 10 παρ. 10 του ν. 3156/2003, αναγγελία της σύμβασης εκχώρησης προς τον οφειλέτη μη απαιτούμενης έγγραφης αναγγελίας της εκχώρησης από τη μεταβιβάσασα εταιρία ή την εταιρία ειδικού σκοπού προς τον οφειλέτη[59]. Ως εκ τούτου, δεδομένου ότι οι ειδικότερες διατάξεις για την τιτλοποίηση απαιτήσεων ορίζουν ότι αρκεί και ισχύει ως αναγγελία (ενημέρωση) η καταχώριση της σχετικής σύμβασης στο δημόσιο βιβλίο, πρέπει να γίνει δεκτό ότι δεν απαιτείται στην περίπτωση αυτή σύμφωνα με τις ειδικές διατάξεις και άλλου είδους προηγούμενη ατομική ενημέρωση.

Συνιστάται, πάντως, κατά τον χρόνο της συλλογής των δεδομένων ο υπεύθυνος επεξεργασίας –η τράπεζα που μετέπειτα προχωρεί σε

[52] Άρθρα 11 και 24 παρ. 3 εδ. β΄ και γ΄ του Ν. 2472/1997 σε συνδυασμό με τις Κανονιστικές Πράξεις 1/1999 και 408/1998 της Αρχής
[53] Αποφάσεις 38/2013 και 127/2013 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[54] Ετήσια Έκθεση της Αρχής Προστασίας Δεδομένων Προσωπικού χαρακτήρα 2012, 3.6.6. Τιτλοποίηση απαίτησης τραπεζών
[55] Άρθρο 5 παρ. 2 στοιχ. β΄ του ν. 2472/1997
[56] Άρθρο 5 παρ. 2 στοιχ. 2 στοιχ. ε΄ του ν. 2472/1997,
[57] Άρθρο 10 παρ. 8 του ν. 3156/2003
[58] Άρθρο 10 παρ. 9 του ν. 3156/2003
[59] Απόφαση 2391/2011 ΜΠΡ ΑΘ

τιτλοποίηση της απαίτησής της– να περιλαμβάνει στο περιεχόμενο της ενημέρωσης στην οποία προβαίνει, κατά το άρθρο 11 παρ. 1 του ν. 2472/1997, ως κατηγορία αποδεκτών, τις εταιρίες ειδικού σκοπού για την περίπτωση τιτλοποίησης απαιτήσεων και, πάντως, το αργότερο μετά την τιτλοποίηση της απαίτησης η εκχωρήτρια τράπεζα ή η εταιρία ειδικού σκοπού πρέπει να ενημερώνει σχετικά ατομικώς τον οφειλέτη (π.χ. με την αποστολή του σχετικού λογαριασμού του). Και τούτο διότι από τη συστηματική ερμηνεία των προαναφερόμενων διατάξεων προκύπτει ότι οι ειδικότερες διατάξεις για την τιτλοποίηση απαιτήσεων αίρουν την υποχρέωση ενημέρωσης του άρθρου 11 παρ. 3 ν. 2472/1997 μόνο κατά το αναγκαίο για να εφαρμοστούν περιεχόμενό τους και όχι την ίδια την υποχρέωση ενημέρωσης[60].

Τέλος, η Αρχή επισημαίνει στα υποκείμενα των δεδομένων ότι έχουν τα προβλεπόμενα από τα άρθρα 12 και 13 του ν. 2472/1997 δικαιώματα πρόσβασης και αντίρρησης. Τα δικαιώματά τους αυτά πρέπει να τα ασκήσουν διαδοχικώς απευθυνόμενοι κατά πρώτο λόγο στον υπεύθυνο επεξεργασίας και όχι στην Αρχή. Αν, όμως, ο υπεύθυνος επεξεργασίας δεν απαντήσει εμπροθέσμως ή εάν η απάντησή του δεν είναι ικανοποιητική, έχουν τότε δικαίωμα να προσφύγουν στην Αρχή σύμφωνα με τις πιο πάνω διατάξεις, προσκομίζοντας όλα τα σχετικά στοιχεία.

Χορήγηση αδειών ενημέρωσης δια του τύπου για τιτλοποίηση και μεταβίβαση απαιτήσεων Τραπεζών.

Η Αρχή, υπό το καθεστώς της Οδηγίας 95/46/ΕΚ και του ν. 2472/1997 (βλ. και κανονιστικές πράξεις 408/1998 και 1/1999), εξέτασε[61] σχετικά αιτήματα τραπεζών και χορήγησε άδειες ενημέρωσης δια του Τύπου.

Ειδικότερα, τράπεζα γνωστοποίησε στην Αρχή ότι προέβη σε τιτλοποίηση και μεταβίβαση χαρτοφυλακίου δανείων και πιστώσεων σε οριστική καθυστέρηση σε εταιρεία ειδικού σκοπού, η οποία με σύμβαση ανέθεσε τη διαχείριση του εν λόγω χαρτοφυλακίου σε άλλη εταιρία, που έχει ιδρυθεί σύμφωνα με τις διατάξεις του ν. 4354/2015. Όπως δηλώθηκε, η υπό κρίση χορήγηση δεδομένων αφορούσε σε μεγάλο αριθμό υποκειμένων (πάνω από 20.000 φυσικά πρόσωπα), το δε 80% των τιτλοποιημένων αυτών απαιτήσεων αφορούσε σε συμβάσεις δανείων που είχαν ήδη καταγγελθεί, ενώ το υπόλοιπο 20% αφορούσε σε ληξιπρόθεσμες απαιτήσεις από είκοσι (20) δανειακές συμβάσεις που δεν είχαν καταγγελθεί. Συγκεκριμένα, η Τράπεζα ζήτησε να ενημερώσει δια του Τύπου τα φυσικά πρόσωπα που συνδέονται με τις ανωτέρω απαιτήσεις με οποιαδήποτε ιδιότητα (όπως, ενδεικτικά, οφειλέτες / συνοφειλέτες, εγγυητές, εμπράγματοι οφειλέτες, ειδικοί ή καθολικοί διάδοχοι των ανωτέρω, αντίκλητοι ή πληρεξούσιοι των ανωτέρω

[60] Τούτο είναι σύμφωνο και με την υποχρέωση ενημέρωσης, όπως αυτή προβλέπεται στην Οδηγία 95/46/ΕΚ (βλ. άρθρο 11), την οποία Οδηγία ενσωμάτωσε στο ελληνικό δίκαιο ο ν. 2472/1997 (ενδεικτικά, Γ/ΕΞ/5079-1/14-10-2014).
[61] 134/2017 απόφασή της Αρχής Προστασίας Δεδομένων Προσωπικού χαρακτήρα

κ.ά.) ότι τα προσωπικά τους δεδομένα που αφορούν στις ως άνω απαιτήσεις θα διαβιβαστούν από την τράπεζα στην εταιρία ειδικού σκοπού στο πλαίσιο τιτλοποίησης/μεταβίβασης των απαιτήσεων και, κατ' εντολή και για λογαριασμό της τελευταίας, στην τρίτη εταιρεία του ν.4354/2015 για τον σκοπό της διαχείρισής τους.

Η Αρχή, με τη με αριθ. 134/2017 απόφασή της, για όσες απαιτήσεις είχαν τιτλοποιηθεί μέχρι και την ημερομηνία έκδοσης της εν λόγω απόφασης, χορήγησε άδεια για ενημέρωση των υποκειμένων των δεδομένων δια του Τύπου με τους ακόλουθους όρους: i) το κείμενο του υποβληθέντος σχεδίου ενημέρωσης να τροποποιηθεί, ώστε α) να αναφέρονται με σαφήνεια οι κατηγορίες των απαιτήσεων που έχουν τιτλοποιηθεί (π.χ. όλες οι καταγγελθείσες συμβάσεις μέχρι μια συγκεκριμένη ημερομηνία και οι ληξιπρόθεσμες απαιτήσεις από τις είκοσι δανειακές συμβάσεις που θα αναφέρονται μόνο με τον αριθμό τους), προκειμένου τα υποκείμενα των δεδομένων να είναι σε θέση να αναγνωρίσουν ευχερώς ότι τους αφορά, και β) να αποσαφηνίζεται σε ποιον υπεύθυνο επεξεργασίας μπορούν να απευθύνονται τα υποκείμενα των δεδομένων προκειμένου να ασκήσουν τα δικαιώματα πρόσβασης και αντίρρησης αναφορικά με την τιτλοποίηση και αναφορικά με τη διαχείριση των απαιτήσεων, ii) η εν λόγω ενημέρωση να δημοσιευθεί στις πέντε πανελλαδικής κυκλοφορίας εφημερίδες με τη μεγαλύτερη κυκλοφορία, τόσο στις έντυπες όσο και στις αντίστοιχες ηλεκτρονικές εκδόσεις αυτών, iii) η εν λόγω ενημέρωση να πραγματοποιηθεί και μέσω των πέντε διαδικτυακών τόπων ειδησεογραφικού χαρακτήρα με την υψηλότερη επισκεψιμότητα στην Ελλάδα, iv) η εν λόγω ενημέρωση να επαναλαμβάνεται ανά μήνα μέχρι να ολοκληρωθεί η διάθεση των σχετικών δεδομένων στην αποδέκτρια Εταιρεία Διαχείρισης Απαιτήσεων και να επαναληφθεί δύο φορές, ανά τρίμηνο, μετά την ολοκλήρωση της διάθεσης, v) η εν λόγω ενημέρωση να αναρτηθεί, επίσης, στον διαδικτυακό τόπο της Τράπεζας και να αναπαραχθεί στον διαδικτυακό τόπο της Ελληνικής Ένωσης Τραπεζών, και iv) να πραγματοποιηθεί, επίσης, εξατομικευμένη ηλεκτρονική ενημέρωση, μέσω ηλεκτρονικού ταχυδρομείου (e-mail), σε όλες τις περιπτώσεις στις οποίες τούτο καθίσταται εφικτό και, ιδίως, εφόσον τα σχετικά στοιχεία έχουν χορηγηθεί στην Τράπεζα από τα υποκείμενα των δεδομένων.

Στη συνέχεια, όμως, με την 33/2018 απόφασή της, η Αρχή απεύθυνε σύσταση στην Τράπεζα, διότι από τα συμπληρωματικά στοιχεία που εστάλησαν μετά την έκδοση της προαναφερθείσας με αριθ. 134/2017 απόφασης, προέκυψε ότι δεν τηρήθηκε πλήρως ο όρος 2.1. της απόφασης. Το κείμενο της ενημέρωσης τροποποιήθηκε και δημοσιεύθηκε χωρίς να αναφέρονται οι μοναδικοί αριθμοί ή άλλα προσδιοριστικά στοιχεία των σχετικών συμβάσεων, ώστε τα υποκείμενα των δεδομένων να μπορούν να αναγνωρίσουν ευχερώς ό,τι τα αφορά. Από τη σχετική διατύπωση της ως άνω απόφασης η Αρχή έθεσε ως όρο να αναφέρονται με σαφήνεια οι κατηγορίες των απαιτήσεων που έχουν

τιτλοποιηθεί και, ειδικότερα, ως προς τις είκοσι μη καταγγελθείσες συμβάσεις να «αναφέρονται μόνο με τον αριθμό τους», προκειμένου τα υποκείμενα των δεδομένων να είναι σε θέση να αναγνωρίσουν ευχερώς ότι τους αφορά. Εξάλλου, εφόσον η Τράπεζα διαπίστωσε ότι δεν υφίσταται μοναδικός αριθμός συμβάσεων δανείων/πιστώσεων προσδιοριστικός και αναγνωριστικός του είδους, της φύσης του χρόνου σύναψης κλπ των κάθε φύσεως συμβάσεων σε επίπεδο Τράπεζας (δεδομένου ότι κάθε κατάστημά της τηρεί ξεχωριστό μητρώο συμβάσεων από το οποίο αντλεί τον αριθμό των συμβάσεων, συνεπώς, για έναν αριθμό σύμβασης μπορεί να αντιστοιχούν συμβάσεις τουλάχιστον όσα είναι και τα καταστήματα της Τράπεζας), όφειλε να εκπληρώσει τον σχετικό όρο της Απόφασης με κάθε πρόσφορο τρόπο (π.χ. με αναφορά σε αριθμό σύμβασης και κωδικό καταστήματος ή άλλα στοιχεία προσδιοριστικά κάθε σύμβασης). Κατά την εξέταση της υπόθεσης, η τράπεζα δήλωσε ότι για όλες τις περιπτώσεις της κατηγορίας αυτής προέβη αμέσως μετά την έκδοση της απόφασης 134/2017 σε ειδική και εξατομικευμένη ενημέρωση με την αποστολή στους πιστούχους (αλλά και στους εγγυητές) εγγράφων επιστολών ενημέρωσης. Σε όσες δε εκ των ανωτέρω περιπτώσεων (κυρίως εγγυητών), παρά τις επανειλημμένες αποστολές για επίδοση στις υφιστάμενες στα αρχεία ή στους φακέλους της τράπεζας διευθύνσεις επεστράφησαν ως ανεπίδοτες, συνεχίζεται η προσπάθεια ανεύρεσης νέων διευθύνσεων προς επίδοσή τους. Κατόπιν τούτου, λαμβάνοντας ιδίως υπόψη το γεγονός ότι η τράπεζα προκάλεσε αναίτια την έκδοση μιας απόφασης δηλώνοντας ότι υπήρχε αντικειμενική αδυναμία να ενημερώσει εξατομικευμένα τα υποκείμενα των δεδομένων στις συγκεκριμένες περιπτώσεις και ζητώντας την κατά προτεραιότητα εξέταση της υπόθεσης λόγω του επείγοντος χαρακτήρα της, η Αρχή, με τη με αριθ. 33/2018 απόφασή της, απηύθυνε σύσταση στην τράπεζα να επιδεικνύει τη δέουσα επιμέλεια προς εκπλήρωση της θεμελιώδους υποχρέωσής της για ενημέρωση των υποκειμένων των δεδομένων σύμφωνα με το άρθρο 11 του ν. 2472/1997 σε συνδυασμό με τη με αριθ. 1/1999 κανονιστική πράξη της Αρχής, ιδίως να υποβάλλει αίτημα για την κατ’ εξαίρεση ενημέρωση των υποκειμένων δια του Τύπου μόνο εφόσον είναι απολύτως απαραίτητο.

Εν τω μεταξύ, η ίδια τράπεζα γνωστοποίησε στην Αρχή ότι προτίθεται, για δεύτερη φορά, να προβεί σε τιτλοποίηση και μεταβίβαση χαρτοφυλακίου περίπου 13.000 ληξιπρόθεσμων μη εξυπηρετούμενων ή και καταγγελμένων δανείων της και πιστώσεων σε έτερη εταιρεία ειδικού σκοπού (SPV). Συγκεκριμένα, η τράπεζα ζήτησε να της επιτραπεί να ενημερώσει δια του Τύπου τα φυσικά πρόσωπα που συνδέονται με τις ανωτέρω απαιτήσεις με οποιαδήποτε ιδιότητα (όπως, ενδεικτικά, οφειλέτες/συνοφειλέτες, εγγυητές, εμπράγματοι οφειλέτες, ειδικοί ή καθολικοί διάδοχοι των ανωτέρω, αντίκλητοι ή πληρεξούσιοι των ανωτέρω κ.ά.) ότι τα προσωπικά τους δεδομένα που αφορούν στις ως άνω απαιτήσεις θα διαβιβαστούν στην ανωτέρω αλλοδαπή εταιρεία στο πλαίσιο τιτλοποίησης/μεταβίβασης των

απαιτήσεων και, κατ' εντολή και για λογαριασμό της τελευταίας, σε ημεδαπή Εταιρεία Διαχείρισης Απαιτήσεων του ν. 4354/2015. Η Αρχή, με τη με αριθ. 23/2018 απόφασή της, δέχθηκε εν μέρει το υποβληθέν αίτημα ενημέρωσης δια του Τύπου, υπό συγκεκριμένους όρους, μεταξύ των οποίων, να αναφέρονται στο κείμενο ενημέρωσης με σαφήνεια οι κατηγορίες των απαιτήσεων που έχουν τιτλοποιηθεί. Απέρριψε δε το αίτημα για τη δια του Τύπου ενημέρωση των ίδιων φυσικών προσώπων σχετικά με τη διάθεση των στοιχείων τους από την τράπεζα, ενεργούσα κατ' εντολή και για λογαριασμό της εταιρίας ειδικού σκοπού, σε ημεδαπή εταιρεία με σκοπό την εξωτερική ανάθεση της διαχείρισης των απαιτήσεων αυτών, καθώς ο δεύτερος αυτός αποδέκτης δεν ορίζεται συγκεκριμένα.

Επίσης, με την απόφαση 87/2017, χορηγήθηκε σε δύο τράπεζες άδεια ενημέρωσης των υποκειμένων των δεδομένων δια του Τύπου για τη διάθεση / χορήγηση δεδομένων σχετικά με ληξιπρόθεσμες απαιτήσειςαπό δάνεια και πιστώσεις, που παρέμεναν σε καθυστέρηση, στις αντίστοιχες συνεργαζόμενες με αυτές Εταιρείες Διαχείρισης Απαιτήσεων, στην οποία δεν υπάρχει αντίστοιχος όρος συγκεκριμένης αναφοράς των εν λόγω συμβάσεων / απαιτήσεων.

Η Αρχή λαμβάνοντας υπόψη ότι: α) «ασκήθηκε παρέμβαση» της Ένωσης Ελληνικών Τραπεζών υπέρ των αιτουσών και εκκρεμούσε η υποβολή τρίτης αίτησης τράπεζας με το ίδιο αίτημα, από όπου προέκυπτε ότι το ζήτημα είναι μείζονος σημασίας συνολικά για τις τράπεζες μέλη της ΕΕΤ, και β) ενώπιον της Ολομέλειας της Αρχής εκκρεμούσε εξέταση ατομικών προσφυγών κατά τραπεζών για πλημμελή εκπλήρωση της υποχρέωσης ενημέρωσης σχετικά με τη διαβίβαση δεδομένων σε εταιρείες ενημέρωσης οφειλετών, ζήτημα συναφές με το υπό εξέταση θέμα, αποφάσισε να παραπέμψει την υπόθεση στην Ολομέλεια, προκειμένου να ερευνηθούν ενιαίως οι εν λόγω συναφείς υποθέσεις.[62] Οι εν λόγω υποθέσεις εξετάστηκαν από την Ολομέλεια της Αρχής, η οποία με την απόφαση 87/2017 δέχτηκε εν μέρει το υποβληθέν αίτημα για την δια του Τύπου ενημέρωση των προσώπων που σχετίζονται με ληξιπρόθεσμες απαιτήσεις προς τις δύο ως άνω τράπεζες. Ειδικότερα, για όσες απαιτήσεις είχαν καταστεί ληξιπρόθεσμες και παρέμεναν σε καθυστέρηση μέχρι και την ημερομηνία έκδοσης της παρούσας απόφασης, χορήγησε[63] στις αιτούσες τράπεζες άδεια για ενημέρωση των υποκειμένων των δεδομένων δια του Τύπου σχετικά με τη διάθεση των σχετικών δεδομένων στις αντίστοιχες Εταιρείες Διαχείρισης Απαιτήσεων, με τους ακόλουθους όρους: α) η εν λόγω ενημέρωση να δημοσιευθεί στις πέντε πανελλαδικής κυκλοφορίας εφημερίδες με τη μεγαλύτερη κυκλοφορία, τόσο στις έντυπες όσο και στις αντίστοιχες ηλεκτρονικές εκδόσεις αυτών, β) η εν λόγω ενημέρωση να πραγματοποιηθεί και μέσω πέντε διαδικτυακών τόπων

[62] απόφαση 62/2017 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[63] σύμφωνα με την υπ' αριθ. 1/1999 Κανονιστική Πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ειδησεογραφικού χαρακτήρα με την υψηλότερη επισκεψιμότητα στην Ελλάδα, γ) η εν λόγω ενημέρωση να επαναλαμβάνεται ανά μήνα μέχρι να ολοκληρωθεί η διάθεση των σχετικών δεδομένων στην αποδέκτρια Εταιρεία Διαχείρισης Απαιτήσεων και να επαναληφθεί δύο φορές, ανά τρίμηνο, μετά την ολοκλήρωση της διάθεσης, δ) η εν λόγω ενημέρωση να αναρτηθεί, επίσης, στον διαδικτυακό τόπο της Τράπεζας και να αναπαραχθεί στον διαδικτυακό τόπο της Ελληνικής Ένωσης Τραπεζών, και ε) να πραγματοποιηθεί, επίσης, εξατομικευμένη ηλεκτρονική ενημέρωση, μέσω ηλεκτρονικού ταχυδρομείου (e-mail), σε όλες τις περιπτώσεις στις οποίες τούτο καθίσταται εφικτό και, ιδίως, εφόσον τα σχετικά στοιχεία έχουν χορηγηθεί στην Τράπεζα από τα υποκείμενα των δεδομένων. Για όσες απαιτήσεις καταστούν ληξιπρόθεσμες ή είναι ακόμα ενήμερες μετά την ημερομηνία έκδοσης της παρούσας απόφασης, επισήμανε στις αιτούσες τράπεζες την υποχρέωσή τους να ενημερώνουν εφεξής, καταρχήν, εξατομικευμένα, με κάθε πρόσφορο τρόπο όλα τα υποκείμενα των δεδομένων που σχετίζονται με τις απαιτήσεις αυτές σχετικά με τη διάθεση των σχετικών δεδομένων τους στις αντίστοιχες Εταιρείες Διαχείρισης Απαιτήσεων. Η δια του Τύπου ενημέρωση στις περιπτώσεις αυτές επιτρέπεται μόνον αν η εξατομικευμένη ενημέρωση δεν καθίσταται αποδεδειγμένα εφικτή (π.χ. ελλείψει στοιχείων επικοινωνίας, αγνώστου διαμονής).

1.3.15 Μη ικανοποίηση του δικαιώματος πρόσβασης υποκειμένου των δεδομένων

Με την απόφαση 143/2017, η Αρχή επέβαλε κυρώσεις σε Τράπεζα για μη ικανοποίηση δικαιώματος πρόσβασης σχετικά με έλεγχο τραπεζικού λογαριασμού του υποκειμένου των δεδομένων. Σύμφωνα με τα πραγματικά περιστατικά, ο προσφεύγων στην Αρχή δήλωσε ότι η Τράπεζα παρανόμως επεξεργάστηκε τα στοιχεία του τραπεζικού του λογαριασμού όψεως καθώς είχε αποδείξεις ότι τρίτοι απέκτησαν παρανόμως πρόσβαση σ’ αυτόν με τη συνδρομή κάποιου υπαλλήλου της εν λόγω Τράπεζας και αιτήθηκε από αυτήν να του γνωστοποιήσει τα συγκεκριμένα τρίτα πρόσωπα. Η Τράπεζα αρνήθηκε την παροχή οποιασδήποτε πληροφορίας, αναφέροντας αυτολεξεί «Πρόσβαση στους λογαριασμούς των πελατών της Τράπεζας έχουν αποκλειστικά και μόνο τα νομίμως εξουσιοδοτημένα αρμόδια όργανα αυτής.». Κατόπιν τούτου, ο προσφεύγων ακολούθησε τη δικαστική οδό στέλνοντας στην Τράπεζα εξώδικη δήλωση διαμαρτυρίας – πρόσκληση με την Τράπεζα να ανταπαντά ότι δεν διαπιστώθηκε παραβίαση του τραπεζικού απορρήτου. Συγκεκριμένα, η Τράπεζα υποστήριξε ότι προέβη σε έλεγχο του λογαριασμού, ενέργεια που εμπίπτει στην αρμοδιότητα των εξουσιοδοτημένων προς τούτο τραπεζικών υπαλλήλων, με σκοπό να διαπιστώσει τη βασιμότητα ή μη της προσβληθείσης από τον εμπλεκόμενο πελάτη – τρίτο της αμφισβήτησης της τραπεζικής συναλλαγής χωρίς να προβεί σε κάποια περαιτέρω επεξεργασία γι’ αυτό και έκρινε ότι το αίτημα του προσφεύγοντος δεν πληρούσε τις τυπικές και

ουσιαστικές προϋποθέσεις άσκησης του δικαιώματος πρόσβασης.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, αφού αξιολόγησε τα ανωτέρω, έκρινε: α) ότι για την ικανοποίηση του δικαιώματος πρόσβασης δεν απαιτείται η επίκληση έννομου συμφέροντος, το υποκείμενο δικαιούται να λάβει γνώση των πληροφοριών που το αφορούν και που τηρεί σε αρχείο ο υπεύθυνος επεξεργασίας, σύμφωνα με την αρχή της διαφάνειας της επεξεργασίας ως προϋπόθεση της νομιμότητά της, ενώ το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων θα πρέπει να ικανοποιηθεί μέσα σε εύλογο χρονικό διάστημα, κάτι που δεν έπραξε η Τράπεζα απαντώντας αρνητικά με αδικαιολόγητη χρονική καθυστέρηση, β) η απόφαση της Τράπεζας να χορηγήσει πλήρη στοιχεία του προσφεύγοντος σχετικά με τη συγκεκριμένη συναλλαγή σε άλλο πελάτη - τρίτο χωρίς να επικαλεστεί το τραπεζικό απόρρητο, ενώ έναντι του προσφεύγοντος προέβαλε το τραπεζικό απόρρητο για την ίδια ακριβώς συναλλαγή, ενέχει αξιολογική αντινομία και καθιστά την αιτιολόγηση της άρνησης αποκάλυψης των στοιχείων του άλλου πελάτη – τρίτου προσχηματική, και ουδόλως ικανοποιητική, γ) η Τράπεζα επεξεργάστηκε τα στοιχεία λογαριασμού του προσφεύγοντος χωρίς νόμιμο λόγο, καθώς δεν απέδειξε ότι ανέκυψε πράγματι «υπηρεσιακή ανάγκη» για την εν λόγω αναζήτηση και περαιτέρω διάθεση προσωπικών δεδομένων, όπως ισχυρίστηκε, καθώς και ότι πρέπει να απευθύνει σύσταση στη Τράπεζα για βελτίωση των τεχνικών και οργανωτικών μέτρων ασφαλείας που τηρεί, λαμβανομένου υπόψη ότι τα γεγονότα, που συνιστούν τις κατ' ιδίαν συνθήκες του συγκεκριμένου περιστατικού ελέγχου του λογαριασμού του προσφεύγοντος δεν βεβαιώθηκαν απολύτως, ούτε αποκαλύφθηκαν στην Αρχή τα στοιχεία του προσώπου που φέρεται να αμφισβήτησε τη συγκεκριμένη συναλλαγή (νέος αποδέκτης των δεδομένων). Για τους ανωτέρω λόγους και λαμβάνοντας υπόψη τη βαρύτητα των παραβάσεων η Αρχή επέβαλε χρηματικό πρόστιμο στη Τράπεζα για μη ικανοποίηση του υπό κρίση δικαιώματος πρόσβασης του προσφεύγοντος σε τραπεζικό του λογαριασμό.

1.3.16 Παράνομη επεξεργασία προσωπικών δεδομένων.

Σχετικά με νομιμότητα επεξεργασίας δεδομένων από ιδρύματα πληρωμών, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα κλήθηκε να συνδράμει το Υπουργείο Οικονομικών-Νομικό Συμβούλιο του Κράτους στην ερμηνεία της Οδηγίας 95/46/ΕΚ στο πλαίσιο προδικαστικού ερωτήματος που υπέβαλε ισπανικό δικαστήριο στο Δικαστήριο της Ευρωπαϊκής Ένωσης[64]. Ειδικότερα, το αιτούν ισπανικό δικαστήριο έθετε τρία ερωτήματα, εκ των οποίων, τα δυο πρώτα αφορούσαν στην ερμηνεία της Οδηγίας 2005/60/ΕΚ σχετικά με την

[64]C235/2014 Υπόθεση C-235/14: Αίτηση προδικαστικής αποφάσεως την οποία υπέβαλε το Audiencia Provincial de Barcelona (Ισπανία) στις 13 Μαΐου 2014 — Safe Interenvios, S.A. κατά Liberbank, S.A., κ.λπ., δημοσίευση του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 21.7.2014
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62014CN0235

πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας, ενώ το τρίτο ερώτημα στην εφαρμογή της Οδηγίας 95/46/ΕΚ, και, ειδικότερα, σε περίπτωση που κριθεί ότι τα πιστωτικά ιδρύματα διαθέτουν εξουσία λήψεως μέτρων αυξημένης δέουσας επιμέλειας ως προς τα ιδρύματα πληρωμών, α) αν πρέπει να γίνει δεκτό ότι μεταξύ των μέτρων αυτών μπορεί να περιλαμβάνεται η απαίτηση διαβιβάσεως των στοιχείων ταυτότητας όλων των πελατών τους, από τους οποίους προέρχονται τα κεφάλαια που εμβάζονται, καθώς επίσης και της ταυτότητας των ληπτών και β) αν είναι σύμφωνη με την Οδηγία 95/46/ΕΚ η επιβολή στα ιδρύματα πληρωμών της υποχρεώσεως να παρέχουν τα στοιχεία των πελατών τους στα πιστωτικά ιδρύματα με τα οποία υποχρεούνται να συνεργάζονται και με τα οποία τελούν ταυτόχρονα σε σχέση ανταγωνισμού.

Κατά την άποψη της Αρχής όπως αυτή αποτυπώθηκε στο Γ/ΕΞ/4417-1/31-7-2014 έγγραφό της, εφόσον γίνει δεκτό ότι η Οδηγία 2005/60/ΕΚ παρέχει στα πιστωτικά ιδρύματα τη δυνατότητα λήψεως μέτρων αυξημένης δέουσας επιμέλειας ως προς τα ιδρύματα πληρωμών, τα μέτρα αυτά δεν μπορούν, να εκτείνονται στην υποχρεωτική διαβίβαση ονομαστικών δεδομένων των πελατών (αποστολέα και λήπτη), αν τούτο δεν επιτάσσεται ρητά από τον αντίστοιχο εθνικό νόμο ή έστω από τις πράξεις της αρμόδιας εποπτικής αρχής που τον εξειδικεύουν. Σημειώνεται δε ότι ούτε το ίδιο το ίδρυμα πληρωμών που υπόκειται σε εποπτεία δεν επιτρέπεται να διενεργήσει πλήρη έλεγχο για τους δικούς του, υποψήφιους και υφιστάμενους, πελάτες αν τούτο δεν προβλέπεται ρητά από το νόμο ή/και τις ειδικά για τα ιδρύματα πληρωμών εκδοθείσες πράξεις κανονιστικού περιεχομένου της Τράπεζας της Ελλάδος.[65]

Επίσης, η Αρχή, με τη με αριθμ. 70/2015 απόφασή της, επέβαλε σε τράπεζα, ως υπεύθυνο επεξεργασίας, πρόστιμο για παράνομη επεξεργασία δεδομένων της προσφεύγουσας και για μη τήρηση κατάλληλων οργανωτικών και τεχνικών μέτρων ασφάλειας, η οποία οδήγησε σε μη εξουσιοδοτημένες προσβάσεις υπαλλήλων της στα προσωπικά δεδομένα της προσφεύγουσας. Απηύθυνε δε σύσταση στην Τράπεζα να λάβει κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από παράνομη ή αθέμιτη επεξεργασία, ώστε να τεκμηριώνονται επαρκώς οι προσβάσεις που πραγματοποιούν οι εξουσιοδοτημένοι προς τούτο υπάλληλοί της στους λογαριασμούς των πελατών της (π.χ. ενεργοποίηση μηχανισμών που να μην επιτρέπουν προσβάσεις σε λογαριασμούς πελατών από μη εξουσιοδοτημένους χρήστες, διενέργεια σε τακτά χρονικά διαστήματα δειγματοληπτικών ελέγχων προς διαπίστωση συμμόρφωσης των υπαλλήλων της με τις σχετικές οδηγίες της τράπεζας).

Στην ειδική περίπτωση, όπου υπάρχει καταγγελία για αθέμιτη πρόσβαση σε

[65] Γ/ΕΞ/2179-1/22-07-2013, Ετήσια έκθεση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

λογαριασμό πελάτη, έγινε σύσταση στη Τράπεζα να ακολουθεί ορθές διαδικασίες, οργανωτικά άλλα και τεχνικά, προκειμένου να διασφαλίσει ότι η διερεύνηση της καταγγελίας διεξάγεται κατά τρόπο που να συνάδει με τις αρχές της ψηφιακής εγκληματολογίας, στο βαθμό που ακολουθούνται διεθνώς αποδεκτές πρακτικές συλλογής και ανάλυσης ψηφιακών πειστηρίων. Με βάση τις αρχές της ψηφιακής εγκληματολογίας καμία ενέργεια, η οποία πραγματοποιείται από το άτομο που ερευνά υπόθεση, όπου εμπλέκονται ψηφιακά πειστήρια, δεν θα πρέπει να αλλοιώνει δεδομένα (ψηφιακά πειστήρια), τα οποία αργότερα μπορεί να χρησιμοποιηθούν σε δικαστήριο, στην περίπτωση που παραστεί ανάγκη πρόσβασης σε δεδομένα στην «αυθεντική» τους μορφή θα πρέπει η όποια πρόσβαση να πραγματοποιείται από άτομο καταρτισμένο για αυτό και ικανό να εξηγήσει τόσο τη συνάφεια όσο και τις συνέπειες της πρόσβασης αυτής. Θα πρέπει να τηρείται ένα αρχείο καταγραφής (audit trail) όλων των ενεργειών που αφορούν τα ψηφιακά πειστήρια. Ένας ανεξάρτητος τρίτος θα πρέπει να μπορεί να εξετάσει αυτές τις ενέργειες καταλήγοντας στο ίδιο συμπέρασμα. Το άτομο που είναι υπεύθυνο για την έρευνα είναι υπεύθυνο τόσο για την τήρηση του νόμου όσο και για την τήρηση των προαναφερθέντων αρχών.

Με την ίδια απόφαση κρίθηκε πως η Τράπεζα προέβη σε επεξεργασία προσωπικών δεδομένων της προσφεύγουσας, ήτοι σε έλεγχο των λογαριασμών που η καταγγέλλουσα τηρούσε στην Τράπεζα, επεξεργασία που είναι νόμιμη βάσει του άρθρου 5 παρ. 2 στοιχ. β’ του ν. 2472/1997 και δεν απαιτείται προηγούμενη συγκατάθεση του υποκειμένου των δεδομένων, όταν είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από τον νόμο.[66]

Αντίστοιχα η Αρχή εξέδωσε την απόφαση 116/2014, με την οποία έκρινε πως ο έλεγχος λογαριασμών με αφορμή κατηγορία για συμμετοχή του πελάτη / υποκειμένου των δικαιωμάτων σε εγκληματικές ενέργειες αποτελεί νόμιμη επεξεργασία.

Επίσης, με την απόφαση 91/2014 έκρινε πως ο έλεγχος των λογαριασμών βάσει των ειδικών υποχρεώσεων της τράπεζας που απορρέουν από τη νομοθεσία για την πρόληψη και καταστολή εσόδων από εγκληματικές ενέργειες[67] συνιστά νόμιμη επεξεργασία.

Στον αντίποδα, αναφέρεται η απόφαση 109/2013 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Σύμφωνα με την καταγγελία η Τράπεζα εμφανίστηκε να έχει αγοράσει λίστες με παρανόμως συλλεχθέντα δεδομένα

[66] Ειδικότερες διατάξεις των ν. 3691/2008 (Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας και άλλες διατάξεις) και ν. 3601/2007 (Ανάληψη και άσκηση δραστηριοτήτων από τα πιστωτικά ιδρύματα, επάρκεια ιδίων κεφαλαίων των πιστωτικών ιδρυμάτων και των επιχειρήσεων παροχής επενδυτικών υπηρεσιών), οι οποίες εξειδικεύονται με σχετικές πράξεις και αποφάσεις της Τράπεζας της Ελλάδος.

[67] ν. 3691/2008 (Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας και άλλες διατάξεις)

προσωπικού χαρακτήρα, για το σκοπό της στοχευμένης προώθησης προϊόντων και υπηρεσιών. Η Αρχή επέβαλε χρηματικό πρόστιμο και την καταστροφή κάθε σχετικής λίστας δεδομένων προσωπικού χαρακτήρα, που είχε αποκτηθεί με παράνομο τρόπο.

1.3.17 Ευαίσθητα προσωπικά δεδομένα

Η συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων επιτρέπεται κατ' εξαίρεση[68] όταν παρέχεται η γραπτή συγκατάθεση του υποκειμένου, αφού προηγουμένως ενημερωθεί κατ' ελάχιστον για τον σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες των δεδομένων, καθώς και τον υπεύθυνο επεξεργασίας.

Με την υπ' αριθμ. 55/2010Απόφαση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, απευθύνθηκε προειδοποίηση προς τράπεζα να καταστρέψει από το φάκελο που τηρούσε για πελάτη της τα φωτοαντίγραφα των αποτελεσμάτων των ιατρικών εξετάσεών του. Σύμφωνα με τα πραγματικά περιστατικά, ο προσφεύγων αιτήθηκε να του χορηγηθεί από την Τράπεζα συμπληρωματικό στεγαστικό δάνειο και για το λόγο αυτό του ζητήθηκε από την Τράπεζα να συνάψει ασφαλιστήριο συμβόλαιο ζωής με συνεργαζόμενη ασφαλιστική εταιρία. Προς τούτο, ο προσφεύγων υπέγραψε αίτηση ασφάλισης συμπληρώνοντας ερωτηματολόγιο σχετικά με την κατάσταση της υγείας του και συγκατατέθηκε να υποβληθεί σε σειρά ιατρικών εξετάσεων. Μεταξύ των εξετάσεων στις οποίες υποβλήθηκε περιλαμβανόταν και εξέταση για αντισώματα HIV.Τα δε αποτελέσματα των εξετάσεων διαβιβάστηκαν από το διαγνωστικό κέντρο στην Τράπεζα σε πλήρη και αναλυτική μορφή και στη συνέχεια περιλήφθησαν στο αρχείο που τηρεί η Τράπεζα. Ο προσφεύγων κατήγγειλε ότι η Τράπεζα παρανόμως τηρούσε αρχείο με ευαίσθητα δεδομένα υγείας του καθώς και ότι δεν ενημερώθηκε προσηκόντως από την ασφαλιστική εταιρία για τις ιατρικές εξετάσεις στις οποίες κλήθηκε να υποβληθεί.

Οι τράπεζες ενεργούν, βάσει συμβάσεων με ασφαλιστικές εταιρίες, ως συνδεδεμένοι ασφαλιστικοί διαμεσολαβητές[69]. Στο πλαίσιο αυτό οι τράπεζες διαβιβάζουν προς την εκάστοτε ασφαλιστική εταιρία έγγραφα που σχετίζονται με την εν γένει εκτέλεση της ασφαλιστικής σύμβασης και τα οποία υποβάλλουν οι ίδιοι οι ασφαλισμένοι ή υπό ασφάλιση πελάτες στα υποκαταστήματα των τραπεζών. Σύμφωνα με τα παραπάνω, κατά την επεξεργασία προσωπικών δεδομένων πελατών που είναι απαραίτητα για τη λειτουργία της ασφαλιστικής σύμβασης η τράπεζα ενεργεί ως εκτελούσα την

[68] άρθρο 7 παρ. 2 περ. α' ν. 2472/1997 και άρθρο 9 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός Προστασίας Δεδομένων)
[69] π.δ.190/2006, υπ. Αριθμ. Κ3-8010/2007 απόφαση του Υπουργού Ανάπτυξης.

επεξεργασία[70]

Η Αρχή έκρινε ότι η πρώτη διαβίβαση των αποτελεσμάτων των ιατρικών αποτελεσμάτων στην τράπεζα έγινε μετά από σχετικό αίτημα του προσφεύγοντος, ο οποίος ζήτησε από την τράπεζα να του αποστείλει τα αποτελέσματα των εξετάσεών του σε αριθμό φαξ, που υπέδειξε. Επομένως, είχε δώσει τη συγκατάθεσή του για την εν λόγω επεξεργασία. Ακόμα και στη περίπτωση που τα εν λόγω στοιχεία διαβιβάστηκαν στην τράπεζα όχι από την ασφαλιστική εταιρία αλλά από το διαγνωστικό κέντρο, η επεξεργασία αυτή δεν είναι παράνομη, αφού τα στοιχεία απεστάλησαν στην τράπεζα αποκλειστικά προκειμένου να παραδοθούν στον προσφεύγοντα, ως υποκείμενο των δεδομένων και όχι μετά από αίτημα της τράπεζας για ίδια χρήση. Συνεπώς, η Τράπεζα, κατά την πρώτη αναζήτηση δεν τηρούσε τα σχετικά στοιχεία στο αρχείο της. Η μεταγενέστερη τήρηση αυτών στο αρχείο της έγινε επ' ευκαιρία της κατοχής του εγγράφου μετά τη πρώτη αναζήτησή του από τον προσφεύγοντα, προκειμένου να διευκολυνθεί νέα τυχόν αναζήτηση από τον ίδιο. Επισημαίνεται ότι τα αποτελέσματα των ιατρικών εξετάσεων των ασφαλισμένων δεν τηρούνται στα αρχεία των Τραπεζών. Εξάλλου για να είναι νόμιμη η επεξεργασία αυτή, θα πρέπει η κάθε τράπεζα να λάβει από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα άδεια τήρησης αρχείου με ευαίσθητα δεδομένα υγείας των δανειοληπτών της. Συμπερασματικώς, δεν υπάρχει νόμιμος λόγος διατήρησης των δεδομένων υγείας από την Τράπεζα και, ως εκ τούτου, τα αποτελέσματα των ιατρικών εξετάσεων του καταγγέλλοντα επιβάλλεται να διαγραφούν από το αρχείο της Τράπεζας.

Χορήγηση αδειών τήρησης ευαίσθητων δεδομένων στις τράπεζες

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα χορήγησε[71] μια δέσμη αδειών τήρησης ευαίσθητων δεδομένων σε τράπεζες για την εκπλήρωση του σκοπού της υπαγωγής των υποκειμένων των δεδομένων στις εξαιρέσεις από τις απαγορεύσεις και περιορισμούς που τέθηκαν στην ανάληψη μετρητών και τη μεταφορά κεφαλαίων (Capital Controls)[72]. Ειδικότερα, τηρούνται από τις τράπεζες ευαίσθητα προσωπικά δεδομένα υγείας (φυσική και πνευματική κατάσταση, ανικανότητες και αναπηρίες, ιατρικό ιστορικό ασθενούς, λοιπά στοιχεία υγείας) και ποινικών καταδικών

[70] Υπό την έννοια του άρθρου 2 στοιχ.η' Ν.2472/97

[71] αρ. πρωτ. ΓΝ/ΕΞ/1656/9.6.17, 1657/9.6.17, 1658/9.6.17, 1659/9.6.17, 1660/9.6.17 και 1661/9.6.17 έγγραφα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

[72] δυνάμει της από 18-07-2015 Πράξης Νομοθετικού Περιεχομένου (ΦΕΚ Α' 84), όπως κυρώθηκε με τον ν. 4350/2015 (ΦΕΚ Α' 161/30-11-2015). Σημειώνεται ότι με το Ν.4624/2019 καταργήθηκε το άρθρο πρώτο της ανωτέρω από 18-7-2015 Πράξης Νομοθετικού Περιεχομένου και αποφασίστηκε «ότι το ηλεκτρονικό αρχείο της Επιτροπής Έγκρισης Τραπεζικών Συναλλαγών σφραγίζεται και διατηρείται αναλλοίωτο σε αδρανή κατάσταση, στα οικεία συστήματα της Τράπεζας της Ελλάδος. Το αρχείο θα είναι προσβάσιμο από τις εποπτικές αρχές και από κάθε ελεγκτική, δικαστική ή εισαγγελική αρχή για τη διερεύνηση πράξεων ή παραλείψεων που σχετίζονται με παραβάσεις των καταργούμενων διατάξεων , κατά το χρόνο ισχύος τους.»

(δικαστικές αποφάσεις) των αιτούντων την υπαγωγή τους στις διατάξεις της από 18-07-2015 Πράξης Νομοθετικού Περιεχομένου «Επείγουσες Ρυθμίσεις για τη θέσπιση περιορισμών στην ανάληψη μετρητών και τη μεταφορά κεφαλάιων», σύμφωνα με τις οποίες κατοχυρώνονται συγκεκριμένες εξαιρέσεις από τους περιορισμούς στην ανάληψη μετρητών και τη μεταφορά κεφαλαίων για σοβαρούς λόγους υγείας ή εξαιρετικούς κοινωνικούς λόγους.

Η Αρχή χορήγησε[73] επίσης άδειες τήρησης ευαίσθητων προσωπικών δεδομένων σε τράπεζες για την εκπλήρωση του σκοπού της υπαγωγής των δανειοληπτών στη Διαδικασία Επίλυσης Καθυστερήσεων, η οποία κατοχυρώνεται στον Κώδικα Δεοντολογίας πιστωτικών ιδρυμάτων, που θεσπίστηκε από την Τράπεζα της Ελλάδος, κατ' εφαρμογή του ν. 4224/2013. Ειδικότερα, τηρούνται από τις τράπεζες ευαίσθητα προσωπικά δεδομένα υγείας (φυσική και πνευματική κατάσταση, ανικανότητες και αναπηρίες, ιατρικό ιστορικό ασθενούς, λοιπά στοιχεία υγείας) των δανειοληπτών οι οποίοι έχουν υπαχθεί στη Διαδικασία Επίλυσης Καθυστερήσεων, τα οποία προσκομίζουν οι ίδιοι στις τράπεζες με τη συγκατάθεσή τους, προκειμένου να αποδείξουν πραγματοποιηθείσες ιατρικές δαπάνες οι οποίες έχουν διαμορφώσει την τρέχουσα οικονομική τους κατάσταση.

Όσον αφορά και τις δύο περιπτώσεις αδειών (λόγω των Capital Controls και λόγω υπαγωγής στη Διαδικασία Επίλυσης Καθυστερήσεων), αποφασίστηκε ότι, ενόψει του ιδιαίτερου χαρακτήρα της επεξεργασίας, οι τράπεζες οφείλουν να διαχωρίζουν τα τηρούμενα δεδομένα από τα δεδομένα που τηρούνται για άλλους σκοπούς. Επίσης, τα δεδομένα που τηρούνται σε ηλεκτρονική μορφή πρέπει να τηρούνται κρυπτογραφημένα και να φυλάσσονται διαχωρισμένα με κατάλληλες μεθόδους, ώστε να αποκλείεται η πιθανότητα να καταστούν προσβάσιμα σε πρόσωπα που δεν διαθέτουν κατάλληλη εξουσιοδότηση. Η πρόσβαση στα ευαίσθητα προσωπικά δεδομένα επιτρέπεται μόνο στους ειδικά εξουσιοδοτημένους υπαλλήλους. Σε κάθε περίπτωση το γεγονός και οι λεπτομέρειες της πρόσβασης θα πρέπει να καταγράφονται ώστε να μπορούν να ελεγχθούν εκ των υστέρων[74].

1.3.18 Καθυστερημένη υποβολή γνωστοποίησης περιστατικών παραβίασης προσωπικών δεδομένων.

Ενδεικτικά αναφέρονται οι αποφάσεις 68/2018 και 69/2018, με τις οποίες η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα απηύθυνε επιπλήξεις σε δυο Τράπεζες, με βάση το άρθρο 58 παρ. 2 στοιχ. β' του Γενικού Κανονισμού Προστασίας Δεδομένων, λόγω του ότι η κάθε μία υπέβαλε στην Αρχή γνωστοποίηση περιστατικού παραβίασης προσωπικών δεδομένων

[73] αρ. πρωτ. ΓΝ/ΕΞ/1862/29.6.17, 1856/29.6.17, 1864/29.6.17, 1860/29.6.17, 1858/29.6.17, 1854/29.6.17 και 2915/5.10.17 έγγραφα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

[74] αρ. πρωτ. ΓΝ/ΕΞ/2915/5.10.17 ,1656/9.6.17, 1657/9.6.17, 1658/9.6.17, 1659/9.6.17, 1660/9.6.17 και 1661/9.6.17, 1862/29.6.17, 1856/29.6.17, 1864/29.6.17, 1860/29.6.17, 1858/29.6.17 και 1854/29.6.17 έγγραφα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

καθυστερημένα[75], ήτοι μετά την πάροδο 72 ωρών από τη στιγμή που η εκάστοτε τράπεζα έλαβε γνώση του περιστατικού, χωρίς να τεκμηριώνονται επαρκώς λόγοι για τους οποίους αυτή η καθυστέρηση θα μπορούσε να είναι δικαιολογημένη.

Οι Τράπεζες υπέβαλαν στην Αρχή γνωστοποίηση περιστατικού παραβίασης προσωπικών δεδομένων, που αφορούσε λίγες μεμονωμένες περιπτώσεις κοινοποίησης παραστατικών πελατών σε διαφορετικό πελάτη τους. Επρόκειτο για μεμονωμένες περιπτώσεις κοινοποίησης με μήνυμα ηλεκτρονικού ταχυδρομείου (email) αποδείξεων και παραστατικών σε διαφορετικό συναλλασσόμενο. Η τράπεζες προχώρησαν σε διερεύνηση και εντοπισμό των λαθών, καθώς και στη θέσπιση ελεγκτικών μηχανισμών και δικλείδων ασφαλείας για την αποφυγή τους στο μέλλον, ενώ επίσης ενημέρωσαν τα επηρεαζόμενα από το περιστατικό πρόσωπα. Επισημαίνεται ότι και στις δύο περιπτώσεις το περιστατικό είχε περιορισμένη έκταση και, κατά τα λοιπά, αντιμετωπίστηκε σωστά από τη στιγμή που κατέστη γνωστό στον υπεύθυνο επεξεργασίας, γι ‘αυτό και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα απηύθυνε μόνο επιπλήξεις.

1.3.19 Επεξεργασία δεδομένων οικονομικής συμπεριφοράς.

Με τη σταδιακή ανάπτυξη της ελληνικής οικονομίας και του τραπεζικού συστήματος, οι Τράπεζες της χώρας αναγνώρισαν την ανάγκη για πρόσβαση σε ακριβή δεδομένα οικονομικής συμπεριφοράς, αφού κατέστη σαφές ότι τέτοιες πληροφορίες συμβάλλουν στην προστασία της πίστης και στη μείωση των επισφαλειών προς όφελος του τραπεζικού συστήματος και των ίδιων των συναλλασσομένων αλλά και εν τέλει της εθνικής οικονομίας. Για το σκοπό αυτό το σύνολο, σχεδόν, των ελληνικών Τραπεζών ίδρυσε την εταιρεία Τειρεσίας στην οποία και ανετέθη η ανάπτυξη και διαχείριση ενός αξιόπιστου Αρχείου Δεδομένων Οικονομικής Συμπεριφοράς.[76] Το Σύστημα Πληροφοριών της ΤΕΙΡΕΣΙΑΣ ΑΕ δημιουργήθηκε ως μια κεντρική βάση δεδομένων με σκοπό τη συγκέντρωση και διάθεση στα χρηματοπιστωτικά ιδρύματα οικονομικών πληροφοριών με σκοπό επεξεργασίας την ελαχιστοποίηση των κινδύνων από τη σύναψη πιστωτικών συμβάσεων με αφερέγγυους πελάτες και, εν γένει, από τη δημιουργία επισφαλών απαιτήσεων.

Τα σημαντικότερα αρχεία της ΤΕΙΡΕΣΙΑΣ είναι τα εξής:

Σύστημα Αθέτησης Υποχρεώσεων ΣΑΥ

Στο σύστημα τηρούνται δεδομένα, τα λεγόμενα δεδομένα της «μαύρης λίστας», δηλαδή δεδομένα που αφορούν ακάλυπτες επιταγές, απλήρωτες συναλλαγματικές, καταγγελίες συμβάσεων χορηγήσεων, διαταγές πληρωμής, προγράμματα πλειστηριασμών, κατασχέσεις και επιταγές του Ν.Δ.1923,

[75] άρ. 33 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός Προστασίας Δεδομένων)
[76] http://www.tiresias.gr/company.html

πτωχεύσεις, κ.ά. Τα δεδομένα τηρούνται χωρίς τη συγκατάθεση των υποκειμένων, μετά από ενημέρωση δια του Τύπου[77]. Με την κανονιστική απόφαση 25/2004 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ορίστηκε το επιτρεπτό χρονικό διάστημα τήρησης των δεδομένων στο σύστημα. για χρονικό διάστημα ανάλογα με το είδος τους[78]. Η Αρχή όρισε[79] τις προϋποθέσεις τήρησης αρχείου από την ΤΕΙΡΕΣΙΑ Α.Ε. σκοπός τήρησης και λειτουργίας του εν λόγω αρχείου είναι « η ελαχιστοποίηση των κινδύνων από τη σύναψη πιστωτικών συβάσεων με αφερέγγυους πελάτες και εν γένει από τη δημιουργία επισφαλών απαιτήσεων και τελικά προστασία της εμπορικής πίστης και εξυγίανση των οικονομικών συναλλαγών», ενώ η σχετική επεξεργασία επιτρέπεται ως επεξεργασία απολύτως αναγκαία για την ικανοποίηση του υπέρτερου έννομου συμφέροντος του υπεύθυνου επεξεργασίας και των νομίμων αποδεκτών των δεδομένων, δηλαδή, κατά κύριο λόγο, των μοναδικών μετόχων του τραπεζικών ιδρυμάτων, σύμφωνα με το άρθρο 5 παρ. 2 στοιχ. ε΄ του ν. 2472/1997 (βλ. παρ. 1 της απόφασης 24/2004). Επισημαίνεται δε ότι, σύμφωνα με την παρ. 4 της απόφασης 24/2004, «Αποδέκτες των δεδομένων, σύμφωνα με τον σκοπό της επεξεργασίας, δικαιολογείται να είναι μόνο οι τράπεζες, τα χρηματοπιστωτικά ιδρύματα και οι εταιρείες διαχείρισης πιστωτικών καρτών, καθώς και φορείς του δημόσιου τομέα, όχι τρίτοι μετέχοντες στις οικονομικές συναλλαγές και ακόμη λιγότερο μη μετέχοντες.[80]

Με αίτησή της, η Ανώνυμη Εταιρεία ΤΕΙΡΕΣΙΑΣ Α.Ε., ζήτησε την έγκριση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για την ένταξη των Εταιρειών Διαχείρισης Απαιτήσεων (ν. 4354/2015) στους νομιμοποιούμενους αποδέκτες των δεδομένων των αρχείων « Σύστημα Αθέτησης Υποχρεώσεων» (εφεξής ΣΑΥ ή «μαύρη λίστα») και « Σύστημα Συγκέντρωσης Χορηγήσεων» (εφεξής ΣΣΧ ή «λευκή λίστα»), τα οποία τηρεί, με τους ίδιους όρους και προϋποθέσεις που ισχύουν για τις Τράπεζες. Οι Εταιρείες Διαχείρισης Απαιτήσεων θεωρούνται σε κάθε περίπτωση δανειστές και προμηθεύτριες, κατά την έννοια του νόμου περί Προστασίας Καταναλωτή, και πρέπει να τηρούν τον Κώδικα Δεοντολογίας των Τραπεζών, τους κανόνες που διέπουν τη χορήγηση δανείων και πιστώσεων που ισχύουν για τα πιστωτικά ιδρύματα, καθώς και όλες τις σχετικές με χορηγούμενα από πιστωτικά και χρηματοδοτικά ιδρύματα δάνεια και πιστώσεις αποφάσεις της ΤτΕ και να λαμβάνουν ειδική μέριμνα για κοινωνικά ευπαθείς ομάδες (άρθρο 1 παρ. 22 του ως άνω νόμου). Οι Εταιρείες Διαχείρισης Απαιτήσεων λογίζονται ως χρηματοπιστωτικοί οργανισμοί, κατά την έννοια του άρθρου 4 παρ. 3 ν. 3691/2008 και ως υπόχρεα πρόσωπα κατά την έννοια του άρθρου 5 παρ. 1 του ιδίου νόμου, εποπτεύονται δε από την Τράπεζα της Ελλάδος (άρθρο 1 παρ. 25

[77] Απόφαση 24/2004 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ΦΕΚ Β΄ 684/11-05-2004
[78] Όπως τροποποιήθηκε με το άρθρο 40 του ν. 3259/2004, άρθρο 70 του ν. 3746/2009 και το άρθρο 4 του ν. 3816/2010
[79] Αποφάσεις 24/2004 και 25/2004 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[80] Απόφαση 185 / 2014 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ν. 4354/2015). Σύμφωνα με τον ήδη σε ισχύ Γενικό Κανονισμό (ΕΕ) 2016/679 (άρθρα 57-58), η Αρχή δεν είναι πλέον αρμόδια να αδειοδοτήσει ή να εγκρίνει επεξεργασίες προσωπικών δεδομένων (βλ. και την με αριθ. 52/2018 Απόφαση της Αρχής). Συνακόλουθα, ο υπεύθυνος επεξεργασίας καθορίζει τους σκοπούς και τους αποδέκτες της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στην οποία προβαίνει, λαμβάνοντας υπόψη και την αρχή της λογοδοσίας (άρθρο 5 παρ. 2 ΓΚΠΔ). Επισημαίνεται η υποχρέωση του υπευθύνου επεξεργασίας για διενέργεια εκτίμησης αντικτύπου, όπου απαιτείται κατά τις διατάξεις του άρθρου 35 ΓΚΠΔ. Με την υπ' αριθμ.18/2019 Απόφασή της η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έκρινε ότι πρέπει η ΤΕΙΡΕΣΙΑΣ Α.Ε. και η αιτούσα την αυτόνομη, ως υπεύθυνη επεξεργασίας, πρόσβαση στα εν λόγω αρχεία της ΤΕΙΡΕΣΙΑΣ ΑΕ Εταιρεία Διαχείρισης Απαιτήσεων, να διενεργήσουν, σύμφωνα με τα προαναφερόμενα, εκτίμηση αντικτύπου των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.

Σύστημα Συγκέντρωσης Χορηγήσεων ΣΣΧ

Στο σύστημα αυτό εμπεριέχονται προσωπικά δεδομένα της «λευκής λίστας» σχετικά με προσωπικά, καταναλωτικά, ανοικτά και στεγαστικά δάνεια, retail factoring, υπεραναλήψεις και κάρτες. Τα δεδομένα του αρχείου διαβιβάζονται στην ΤΕΙΡΕΣΙΑΣ από τα πιστωτικά ιδρύματα στο σύνολό τους χωρίς τη συγκατάθεση των υποκειμένων[81], και η πρόσβαση των τραπεζών στο σύστημα γίνεται μετά από συγκατάθεση του πελάτη/υποψήφιου δανειολήπτη. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από το έτος 2002 έχει εκδώσει απόφαση για τις προϋποθέσεις τήρησης αρχείου «συγκέντρωσης κινδύνων ή λευκής λίστας» από την ΤΕΙΡΕΣΙΑΣ Α.Ε. Συγκεκριμένα, η Αρχή με την Απόφαση 86/2002 έκρινε ότι, σε αντίθεση με το αρχείο δυσμενών οικονομικών δεδομένων («μαύρης λίστας»), η δημιουργία του εν λόγω αρχείου («λευκής λίστας») από την ΤΕΙΡΕΣΙΑΣ Α.Ε., χωρίς τη συγκατάθεση του υποκειμένου αντίκειται στο νόμο και υπερβαίνει το σκοπό της επεξεργασίας. Έγινε δηλαδή δεκτό ότι το εν λόγω αρχείο («λευκή λίστα»), το οποίο περιέχει τις ενήμερες οφειλές και τις οφειλές σε καθυστέρηση, χωρίς αυτές όμως να είναι οφειλές βεβαιωμένες και απαιτητές (όπως στην περίπτωση της «μαύρης λίστας»), μπορεί να δημιουργηθεί και να λειτουργήσει μόνο στη βάση της συγκατάθεσης του υποκειμένου των δεδομένων.

Παραθέτουμε τη σχετική απόφαση με αριθμ. 71/2015, με την οποία η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επέβαλε χρηματικό πρόστιμο σε Τράπεζα για παράνομη επεξεργασία δεδομένων και απηύθυνε προς την τράπεζα την κύρωση της προειδοποίησης να μεριμνήσει ώστε στα έντυπα της αίτησης/σύμβασης να υπάρχει ειδική ενημέρωση για το Σύστημα ΣΣΧ και το Σύστημα Βαθμολογικής Συμπεριφοράς.

[81] άρθρο 70 παρ. 2 του ν. 3746/2009

Σύστημα Βαθμολόγησης Οικονομικής Συμπεριφοράς

Είναι ένα σύστημα που αναπτύσσει η ΤΕΙΡΕΣΙΑΣ ΑΕ και αξιολογείται από κοινού με τα λοιπά κριτήρια που η τράπεζα χρησιμοποιεί στο εσωτερικό σύστημα αξιολόγησης και πιστοληπτικής διαβάθμισης (credit scoring). Σκοπός της επεξεργασίας είναι η μέτρηση της πιθανότητας αθέτησης της υποχρέωσης προς τις τράπεζες, η οποία αποτελεί βασικό στοιχείο για τον υπολογισμό του πιστωτικού κινδύνου. Στοιχεία βαθμολόγησης διαβιβάζονται μόνο στην τράπεζα που έχει την αίτηση του ενδιαφερόμενου και τη σχετική συγκατάθεση και δεν τηρούνται στο σύστημα μετά τη λειτουργία της δανειοδότησης ούτε ανακοινώνονται σε άλλους συμμετέχοντες στο σύστημα χωρίς ξεχωριστή συγκατάθεση.[82]

Σύστημα Ταυτοτήτων/Διαβατηρίων ΣΤΔ

Λειτουργεί από το 2000 με σκοπό επεξεργασίας την προστασία των υποκειμένων από πιθανή απάτη λόγω απώλειας της ταυτότητας ή του διαβατηρίου τους. Με την απόφαση 11/2006 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εγκρίθηκε η διαβίβαση στην ΤΕΙΡΕΣΙΑΣ ΑΕ των αντίστοιχων στοιχείων από το αρχείο της Ελληνικής Αστυνομίας με on-line σύνδεση, με συγκεκριμένους αποδέκτες.

Σύστημα Ελέγχου Κινδύνου (ΤΣΕΚ)

Σκοπός του ΤΣΕΚ[83], είναι η παροχή ορθών και επίκαιρων πληροφοριών οικονομικής συμπεριφοράς των υποκειμένων για την εξασφάλιση γενικά της εμπορικής πίστης, της αξιοπιστίας και ασφάλειας των συναλλαγών και τελικά της άσκησης του δικαιώματος οικονομικής ελευθερίας των επιχειρηματιών, έχει δηλαδή σκοπό ανάλογο των εταιρειών διαπίστωσης πιστοληπτικής ικανότητας της απόφασης 26/2004 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Με την υπ' αριθμ. 185/2014 απόφαση της, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαπίστωσε ότι με τη λειτουργία του συστήματος ΤΣΕΚ η ΤΕΙΡΕΣΙΑΣ ΑΕ διεύρυνε παρανόμως τον σκοπό επεξεργασίας των δεδομένων του αρχείου της ως διατραπεζική εταιρεία που λειτουργεί χάριν των πιστωτικών και χρηματοδοτικών ιδρυμάτων, σκοπός που είναι σαφής, περιορισμένος και προσδιορισμένος από τη νομοθεσία, από τις αποφάσεις της Αρχής, αλλά και από τις δημόσιες ανακοινώσεις της εταιρείας. Επίσης ότι υπέβαλε τη σχετική γνωστοποίηση στην Αρχή με σημαντική χρονική καθυστέρηση, ήτοι, όσον αφορά επεξεργασία δεδομένων φυσικών προσώπων, έξι μήνες μετά την έναρξη της επεξεργασίας, και δεν ενημέρωσε προσηκόντως τα υποκείμενα των δεδομένων για τη μεταβολή αυτή. Για τις ως άνω διαπιστωθείσες παραβάσεις, η Αρχή επέβαλε στην ΤΕΙΡΕΣΙΑΣ ΑΕ

[82] απόφαση 51/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[83] απόφαση185 / 2014 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και υπ' αριθμ. πρωτ. ΓΝ/ΕΙ /6547/30-10-2014 υπόμνημα

πρόστιμο ύψους εβδομήντα πέντε χιλιάδων ευρώ.

Στη συνέχεια, με την υπ' αριθμ. 186/2014 απόφασή της η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έθεσε τους όρους και τις προϋποθέσεις για την εφεξής νόμιμη λειτουργία του εν λόγω συστήματος ΤΣΕΚ. Συγκεκριμένα, η Αρχή επέβαλε τον πλήρη διαχωρισμό των δεδομένων που τηρούνται για καθέναν από τους διακριτούς σκοπούς που επιδιώκει η ΤΕΙΡΕΣΙΑΣ ΑΕ, έθεσε προϋποθέσεις για τη νόμιμη συλλογή των δεδομένων και εξειδίκευσε πώς θα πρέπει να γίνεται η ατομική ενημέρωση των υποκειμένων, καθώς και πώς θα πρέπει να ασκούνται και να ικανοποιούνται τα δικαιώματα πρόσβασης και αντίρρησης αυτών.

Η απευθείας πρόσβαση των Τραπεζών στη βάση δεδομένων της ΤΕΙΡΕΣΙΑΣ ΑΕ επιτρέπεται μόνο για τον προληπτικό έλεγχο της πιστοληπτικής ικανότητας. Χρησιμοποίηση των δεδομένων αυτών για άλλο σκοπό, όπως για την υποστήριξη εννόμου συμφέροντος της Τράπεζας σε δίκη της ενώπιον Δικαστηρίου υπερβαίνει το θεμιτό σκοπό της επεξεργασίας[84] Στην απόφαση της 61/2001 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έκρινε ότι η πρόσβαση τράπεζας στο αρχείο της ΤΕΙΡΕΣΙΑΣ ΑΕ με σκοπό την ανεύρεση και προσκόμισή τους στο δικαστήριο δυσμενών στοιχείων πελάτη της και αντιδίκου της σε δίκη είναι παράνομη.

Με την 62/2003 απόφασή της η Αρχή προστασίας Δεδομένων Προσωπικού Χαρακτήρα έκρινε ότι η επέκταση των αποδεκτών του αρχείου της ΤΕΙΡΕΣΙΑΣ ΑΕ και στις εταιρίες Ασφάλισης Πιστώσεων και Εγγυήσεων δεν δικαιολογείται από το σκοπό επεξεργασίας του συγκεκριμένου αρχείου και επομένως δεν είναι νόμιμη. Στο αιτιολογικό της απόφασης αναφέρθηκε πως Σύμφωνα με την υπ΄ αριθ. 109/1999 Απόφαση της Αρχής, αποδέκτες των δεδομένων που τηρούνται στο αρχείο της εταιρίας ΤΕΙΡΕΣΙΑΣ ΑΕ μπορεί να είναι μόνο οι τράπεζες, άλλα χρηματοπιστωτικά ιδρύματα, εταιρίες που διαχειρίζονται πιστωτικές κάρτες, καθώς και φορείς του δημόσιου τομέα. Με την υπ΄ αριθ. 523/1999 Απόφαση της Αρχής επιτρέπεται ακόμη να είναι αποδέκτες οι εταιρίες πρακτορείας επιχειρηματικών απαιτήσεων (factoring) και οι εταιρίες χρηματοδοτικής μίσθωσης (leasing). Ο σκοπός επεξεργασίας του αρχείου ΤΕΙΡΕΣΙΑΣ ΑΕ έγκειται στην ελαχιστοποίηση των κινδύνων από τη σύναψη πιστωτικών συμβάσεων με αφερέγγυους πελάτες και εν γένει από τη δημιουργία επισφαλών απαιτήσεων και τελικά στην προστασία της εμπορικής πίστης και στην εξυγίανση των οικονομικών συναλλαγών. Η ασφάλιση, ως εμπορική πράξη, ενέχει εξ ορισμού την έννοια του κινδύνου. Κατά συνέπεια, η ασφάλιση των πιστώσεων και εγγυήσεων από ασφαλιστική εταιρία εμπεριέχει τον κίνδυνο αφερεγγυότητας του οφειλέτη. Το γεγονός ότι μετά την τροποποίηση της αρχικής απόφασης της Αρχής , στους αποδέκτες του αρχείου της 'ΤΕΙΡΕΣΙΑΣ ΑΕ» προσετέθησαν και οι εταιρίες πρακτορείας επιχειρηματικών απαιτήσεων (factoring),δεν αποτελεί επαρκή

[84] Απόφαση 61/2001 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

λόγο γιατί η διεύρυνση του κύκλου των αποδεκτών, ώστε σε αυτούς να συμπεριλαμβάνονται και οι ασφαλιστικές εταιρίες που ασφαλίζουν πιστώσεις.Και τούτο, γιατί ακόμη και αν η πρακτορεία επιχειρηματικής απαίτησης έχει και εξασφαλιστικό σκοπό (εκτός, δηλαδή, από τον χρηματοδοτικό και διαχειριστικό), αυτή εξακολουθεί να διαφέρει από την ασφάλιση πιστώσεων και επομένως δικαιολογείται διαφορετική μεταχείριση, αφού το προέχον στοιχείο στην τελευταία έγκειται στην ανάληψη του ασφαλιστικού κινδύνου (της αφερεγγυότητας του οφειλέτη).[85]

Η Αρχή με την απόφαση 57/2013 επέβαλε σε Τράπεζα χρηματικό πρόστιμο για παράβαση του άρθρου 5 παρ. 1 και 2 και του άρθρου 12 του Ν. 2472/97 διότι έκρινε ότι υπήρξε αθέμιτη πρόσβαση στα στοιχεία που αφορούσαν τον προσφεύγοντα και τηρούνται από την ΤΕΙΡΕΣΙΑΣ ΑΕ και απηύθυνε προειδοποίηση στην τράπεζα να εξετάσει και να λάβει μέτρα για την πρόληψη παρόμοιων περιστατικών. Η Αρχή έκρινε ότι κάθε πρόσβαση θα πρέπει, για να είναι νόμιμη, να συνάδει με τους σκοπούς επεξεργασίας του διατραπεζικού αρχείου της ΤΕΙΡΕΣΙΑΣ ΑΕ στο πλαίσιο αξιολόγησης των αντλούμενων πληροφοριών για τη διασφάλιση της ομαλής εξέλιξης των χρηματοπιστωτικών συμβάσεων που συνάπτουν οι τράπεζες με πελάτες τους. Η καθ' ου Τράπεζα, ως υπεύθυνος επεξεργασίας, δεν ήταν σε θέση να ελέγξει εάν αναζητήσεις στο σύστημα της ΤΕΙΡΕΣΙΑΣ ΑΕ από τους υπαλλήλους της έχουν γίνει νόμιμα ή όχι, αφού δεν είχε θεσπίσει συγκεκριμένη διαδικασία που να της παρέχει δυνατότητα ελέγχου και απόδειξης των νόμιμων λόγων αναζήτησης προκειμένου να είναι ευχερής ο προσδιορισμός της οικείας εντολής αναζήτησης πληροφορίας και, ως εκ τούτου, ο εκάστοτε σκοπός της κάθε πρόσβασης.[86]

Η Αρχή με την απόφαση 154/2013 επέβαλε πρόστιμο σε Τράπεζα και ιδιωτική εταιρία για παράνομη συλλογή και χρήση δεδομένων πιστοληπτικής ικανότητας. Η Αρχή έκρινε ότι οι εν λόγω επεξεργασίες πραγματοποιήθηκαν για παράνομο σκοπό, καθώς δεν είχε προσκομιστεί σχετικό αποδεικτικό έγγραφο (αντίγραφο επιταγής εκδόσεως της προσφεύγουσας), ώστε να νομιμοποιείται η τράπεζα να ελέγξει την πιστοληπτική της ικανότητα από το αρχείο της ΤΕΙΡΕΣΙΑΣ ΑΕ και να ανακοινώσει, έστω και εμμέσως, το δεδομένο της αφερεγγυότητας της προσφεύγουσας στην ιδιωτική εταιρεία πελάτη της τράπεζας. Αν και διαπίστωσε ότι η Τράπεζα είχε λάβει κατ' αρχάς κατάλληλα οργανωτικά μέτρα σύμφωνα με το άρθρο 10 του Ν. 2472/1997 τόσο προς τεκμηρίωση των αναζητήσεων στα αρχεία της ΤΕΙΡΕΣΙΑΣ ΑΕ όσο και προς έλεγχο και απόδειξη των νόμιμων λόγων αναζήτησης, η Αρχή απηύθυνε σύσταση στην τράπεζα να λάβει αυστηρότερα οργανωτικά μέτρα ώστε να αποφευχθούν στο μέλλον παρόμοια περιστατικά αναφορικά με πρόσβαση στα εν λόγω αρχεία χωρίς νόμιμο λόγο, δεδομένου ότι σε καμία περίπτωση η

[85] Απόφαση 62/2003 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[86] Απόφαση 57/2013 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

τράπεζα δεν νομιμοποιείται να ενεργεί ως «εταιρεία επιχειρηματικής πληροφόρησης/πιστοληπτικής ικανότητας» παρέχοντας στους πελάτες της, ανταποκρινόμενη μάλιστα σε απλά τηλεφωνικά ερωτήματα, οποιαδήποτε πληροφορία σχετικά με τη φερεγγυότητα ενός άλλου φυσικού προσώπου. Με την ίδια απόφαση η Αρχή εξέτασε τη προσφυγή του νόμιμου εκπροσώπου ιδιωτικής εταιρείας, που κατήγγειλε, ως φυσικό πρόσωπο, παράνομη ανακοίνωση δεδομένων τραπεζικού του λογαριασμού μέσω προσωπικής επιστολής σε τρίτα πρόσωπα, καθώς και παράνομη συλλογή και χρήση ευαίσθητων δεδομένων του σχετικών με ποινική δίωξη. Η Αρχή έκρινε ότι η καθ' ου Τράπεζα συνέλεξε νομίμως τα υπό κρίση δεδομένα, αφού αυτά είχαν κατατεθεί από τον ίδιο σε φάκελο εκδοθείσας σε βάρος της διαταγής πληρωμής, ωστόσο, η πραγματοποιηθείσα ανακοίνωση δεδομένων σχετικά με περιοδικές καταθέσεις χρημάτων σε τραπεζικό του λογαριασμό πραγματοποιήθηκε χωρίς νόμιμο σκοπό και για τον λόγο αυτό επέβαλε την κύρωση της προειδοποίησης[87].

Η Αρχή, στην απόφαση 66/2013 έκρινε ότι η περαιτέρω επεξεργασία των δεδομένων, πέραν του σκοπού για τον οποίο αρχικά νομίμως συλλέχθηκαν, για τον σκοπό του πειθαρχικού ελέγχου του υπαλλήλου της διενεργούσης την επεξεργασία τράπεζας συνιστά θεμιτή μεταβολή του σκοπού της αρχικής συλλογής και επεξεργασίας των προσωπικών δεδομένων του προσφεύγοντος. Στην προκειμένη υπόθεση, ο προσφεύγων κατήγγειλε ότι ασκήθηκε εις βάρος του έλεγχος από επιθεωρητή τράπεζας σχετικά με τακτοποίηση οφειλών του σχετικά με συμβάσεις που είχε ο προσφεύγων στην εν λόγω τράπεζα, αλλά και σε άλλες τράπεζες σε διάφορα καταναλωτικά προϊόντα με σημαντικότατες καθυστερήσεις. Τα στοιχεία αυτά βρήκε ο ανωτέρω επιθεωρητής μετά από αναζήτηση στα αρχεία της ΤΕΙΡΕΣΙΑΣ ΑΕ με την εν λόγω ιδιότητά του και στο πλαίσιο ελέγχου για αντικανονική συμμετοχή υπαλλήλου σε πιστοδότηση πελάτη. Η Αρχή έκρινε ότι ο προσφεύγων πελάτης της τράπεζας που έχει παράλληλα και την ιδιότητα του υπαλλήλου του υποκαταστήματος που δανειοδοτεί δεν μπορεί να έχει εύλογη προσδοκία προστασίας της ιδιωτικότητάς του με την έννοια ότι προσωπικά του δεδομένα που συλλέγονται λόγω της ιδιότητάς του ως πελάτη της τράπεζας δεν θα χρησιμοποιηθούν περαιτέρω ευθύς ως διαπιστωθεί ότι φέρει και την ιδιότητα του υπαλλήλου της τράπεζας, εφόσον ενήργησε κατά τρόπο αντίθετο προς τις υποχρεώσεις του ως υπαλλήλου της τράπεζας, όπως αυτές απορρέουν από τον οργανισμό προσωπικού της Τράπεζας. Η φύση των δεδομένων του προσφεύγοντος που συλλέχθηκαν είναι άρρηκτα συνδεδεμένη με τον αρχικό σκοπό αναζήτησης και συλλογής τους ενόψει της ιδιότητάς του ως πιστολήπτη, η δε περαιτέρω χρήση των δεδομένων, κατά τον έλεγχο της επιδράσεως της συμπεριφοράς του ως υπαλλήλου της τράπεζας, τυγχάνει ευλόγως αναμενόμενη από το υποκείμενο των δεδομένων στο πρόσωπο του

[87]Απόφαση 154/2013 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

οποίου συμπίπτουν οι δύο αυτές ιδιότητες, όπως αναμενόμενη είναι και η οποιαδήποτε τυχόν επιβλαβής επίδραση της περαιτέρω αυτής επεξεργασίας των δεδομένων.[88]

Η Αρχή εξέδωσε τη με αριθμ. 65/2015 απόφαση, με την οποία επέβαλε ως κύρωση χρηματικό πρόστιμο σε Τράπεζα για παράνομη διάθεση/χορήγηση δεδομένων των αρχείων ΣΑΥ/ΣΥΠ και ΣΣΧ της ΤΕΙΡΕΣΙΑΣ ΑΕ σε συνεργαζόμενη εταιρία και για παράλειψη γνωστοποίησης στην Αρχή βασικών χαρακτηριστικών της επεξεργασίας, όπως, ιδίως, τα στοιχεία του εκτελούντος, τη διεύθυνση του αρχείου και του εξοπλισμού που υποστηρίζει την εν λόγω επεξεργασία. Όπως αποδείχθηκε, δυνάμει της τότε υφιστάμενης σύμβασης με την καθ' ού Τράπεζα, η ιδιωτική εταιρία απέκτησε πρόσβαση στα στοιχεία της ΤΕΙΡΕΣΙΑΣ ΑΕ ως εκτελούσα την επεξεργασία για λογαριασμό της Τράπεζας. Παρά τις συμβατικές δεσμεύσεις της ότι θα ελέγχει συστηματικά τις προσβάσεις της ιδιωτικής εταιρίας/ συνεργάτη της στην ΤΕΙΡΕΣΙΑΣ ΑΕ μέσω σύγκρισής τους με τις αιτήσεις για χορήγηση καρτών, η τράπεζα δεν έδωσε οδηγίες για «κατάλληλη πρόσβαση» της εταιρίας στα αρχεία της ΤΕΙΡΕΣΙΑΣ ΑΕ, ενώ προέκυψε ότι ο αριθμός των προσβάσεων των χρηστών της ιδιωτικής εταιρίας στο σύστημα της ΤΕΙΡΕΣΙΑΣ ΑΕ το διάστημα εκείνο ήταν ιδιαίτερα μεγαλύτερος και εξαιρετικά δυσανάλογος σε σχέση με τον αριθμό των πελατών της Τράπεζας, για τους οποίους η Τράπεζα ζήτησε υπηρεσίες από την εταιρία[89].

Με την απόφαση 172/2014 της η Αρχή επέβαλε σε Τράπεζα χρηματικό πρόστιμο συνολικού ύψους τριάντα χιλιάδων ευρώ για μη ικανοποίηση δικαιώματος πρόσβασης και για επεξεργασία ανακριβών δεδομένων, της απηύθυνε δε επιπλέον τη σύσταση να ελέγχει εφεξής ανά τακτά χρονικά διαστήματα την ακρίβεια των δεδομένων που τηρεί και, σε κάθε περίπτωση, να μεριμνά, εντός ευλόγου χρόνου από κάθε σχετική μεταβολή, για τη διόρθωση/διαγραφή των αντίστοιχων στοιχείων που έχει διαβιβάσει στην ΤΕΙΡΕΣΙΑΣ ΑΕ. Ειδικότερα η Αρχή διαπίστωσε ότι η τράπεζα, ως υπεύθυνος επεξεργασίας δεν εκπλήρωσε προσηκόντως την υποχρέωση ελέγχου της ακρίβειας των δεδομένων του προσφεύγοντος, καθώς τηρούσε και επεξεργαζόταν λανθασμένα στοιχεία σχετικά με το πρόσωπό του για τρεισήμισι και πλέον έτη από τότε που έλαβε χώρα η μεταβολή των στοιχείων αυτών (απαλλαγή από εγγύηση δανείου), τα οποία μάλιστα είχε διαβιβάσει και στην ΤΕΙΡΕΣΙΑΣ ΑΕ, η δε επακολουθήσασα διόρθωση των σχετικών δεδομένων δεν οφειλόταν σε πρωτοβουλία της τράπεζας, αλλά στο γεγονός ότι ο ίδιος ο προσφεύγων άσκησε το δικαίωμα αντίρρησης στην ΤΕΙΡΕΣΙΑΣ ΑΕ.

[88]Απόφαση 66/2013 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[89] Απόφαση 65/2015 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

2.Εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων στο πλαίσιο εκτέλεσης τραπεζικών εργασιών.

2.1.Εναρμόνιση με τις βασικές αρχές επεξεργασίας δεδομένων.

Για να είναι σύννομη η επεξεργασία των δεδομένων θα πρέπει να εφαρμόζονται οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 5 του Γ.Κ.Π.Δ., το άρθρο 4 της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και το άρθρο 45 του ν.4624/2019.
Τα πιστωτικά ιδρύματα οφείλουν να τηρούν και να είναι σε θέση να αποδείξουν τη συμμόρφωσή τους με τις θεμελιώδεις αρχές που διέπουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ήτοι νομιμότητα, αντικειμενικότητα, διαφάνεια, προσδιορισμό του σκοπού της επεξεργασίας, ελαχιστοποίηση των δεδομένων, ακρίβεια και επικαιροποίηση αυτών, όπου είναι εφικτό, προσδιορισμό του χρόνου τήρησης, ακεραιότητα, εμπιστευτικότητα και λογοδοσία, όπως αυτές αναφέρονται στο άρθρο 5 του Γενικού Κανονισμού Προστασίας Δεδομένων. Οι αρχές αυτές είναι απολύτως δεσμευτικές για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα πιστωτικά ιδρύματα ως υπεύθυνων επεξεργασίας. Βάσει αυτών των θεμελιωδών αρχών θα πρέπει επίσης να λειτουργούν όλες οι οργανωτικές δομές των Πιστωτικών Ιδρυμάτων, που εμπλέκονται στη διαδικασία επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.[90]

Η Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας των επεξεργασιών δεδομένων προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.[91]
Επιπροσθέτως της νομιμότητας της επεξεργασίας, σύμφωνα με το δίκαιο της Ε.Ε. και το δίκαιο του Συμβουλίου της Ευρώπης για την προστασία δεδομένων, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται με αντικειμενικό τρόπο. Η αρχή της αντικειμενικής επεξεργασίας διέπει πρωτίστως τη σχέση μεταξύ του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων.
Οι υπεύθυνοι επεξεργασίας θα πρέπει να ενημερώνουν τα υποκείμενα των δεδομένων και το ευρύ κοινό ότι θα επεξεργάζονται τα δεδομένα με σύννομο και διαφανή τρόπο και πρέπει να είναι σε θέση να αποδείξουν τη συμμόρφωση των πράξεων επεξεργασίας με τον Γενικό Κανονισμό Προστασίας Δεδομένων. Οι πράξεις επεξεργασίας δεν πρέπει να διενεργούνται μυστικά, και τα υποκείμενα των δεδομένων θα πρέπει να έχουν επίγνωση των δυνητικών κινδύνων. Επιπλέον, στο μέτρο που είναι εφικτό, οι υπεύθυνοι επεξεργασίας πρέπει να ενεργούν κατά τρόπο που συμμορφώνεται άμεσα με τις επιθυμίες

[90] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 3
[91] Άρθρο 5 αριθμ. 1[α]του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

του υποκειμένου των δεδομένων, ιδίως όταν η συγκατάθεση αυτού αποτελεί τη νομική βάση για την επεξεργασία τους. Όσον αφορά τις υπηρεσίες διαδικτύου, τα χαρακτηριστικά των συστημάτων επεξεργασίας δεδομένων πρέπει να παρέχουν τη δυνατότητα στα υποκείμενα των δεδομένων να κατανοούν πραγματικά τι συμβαίνει με τα δεδομένα τους. Σε κάθε περίπτωση, η αρχή της αντικειμενικότητας βαίνει πέραν των υποχρεώσεων διαφάνειας και θα μπορούσε επίσης να συνδέεται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα με δεοντολογικό τρόπο.[92]

Σύμφωνα με την Αρχή της διαφάνειας η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων[93].

Η αρχή αυτή θεσπίζει την υποχρέωση του υπευθύνου επεξεργασίας να λαμβάνει κατάλληλα μέτρα ώστε να τηρεί ενήμερα τα υποκείμενα των δεδομένων –που μπορεί να είναι χρήστες ή πελάτες– σχετικά με τον τρόπο χρήσης των δεδομένων τους. Η διαφάνεια μπορεί να αφορά τις πληροφορίες που παρέχονται στο φυσικό πρόσωπο προτού ξεκινήσει η επεξεργασία, τις πληροφορίες στις οποίες τα υποκείμενα των δεδομένων πρέπει να έχουν άμεση πρόσβαση κατά τη διάρκεια της επεξεργασίας, αλλά και τις πληροφορίες που παρέχονται στα υποκείμενα των δεδομένων κατόπιν αιτήματός τους για πρόσβαση στα δεδομένα που τα αφορούν.[94] Οι πράξεις επεξεργασίας πρέπει να εξηγούνται στα υποκείμενα των δεδομένων με εύκολα προσβάσιμο μέσο ώστε να διασφαλίζεται ότι κατανοούν τι θα συμβεί στα δεδομένα τους. Αυτό σημαίνει ότι το υποκείμενο των δεδομένων πρέπει να γνωρίζει τον συγκεκριμένο σκοπό της επεξεργασίας των δεδομένων προσωπι¬κού χαρακτήρα κατά τον χρόνο συλλογής τους. Η διαφάνεια της επεξεργα¬σίας επιβάλλει να χρησιμοποιείται σαφής και απλή γλώσσα. Οι ενδιαφερό¬μενοι πρέπει να έχουν επίγνωση των κινδύνων, των κανόνων, των εγγυήσεων και των δικαιωμάτων που αφορούν την επεξεργασία των δεδομένων που τους αφορούν.[95] Ορισμένες βασικές πληροφορίες πρέπει να παρέχονται υποχρεωτικά και με προδραστικό τρόπο από τον υπεύθυνο επεξεργασίας στα υποκείμενα των δεδομένων. Πληροφορίες σχετικά με το ονοματεπώνυμο και τη διεύθυνση του υπευθύνου επεξεργασίας (ή των από κοινού υπευθύνων επεξεργασίας), τη νομική βάση και τους σκοπούς της επεξεργασίας δεδομένων, τις κατηγορίες δεδομένων που υποβάλλονται σε επεξεργασία και τους αποδέκτες τους, καθώς και για τον τρόπο άσκησης των δικαιωμάτων, μπορούν να παρέχονται με κάθε κατάλληλο μέσο (μέσω ισοτόπου, τεχνολογικών εργαλείων σε προσωπικές συσκευές κ.λπ.) υπό τον όρο οι πληροφορίες παρουσιάζονται αντικειμενικά και αποτελεσματικά στο

[92] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018, σελ.152
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
[93] Άρθρο 5 αριθμ. 1[α] του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[94] Άρθρα 12, 13, 14 και 15 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[95]Αιτιολογική σκέψη 39 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

υποκείμενο των δεδομένων. Οι πληροφορίες που παρουσιάζονται θα πρέπει να είναι εύκολα προσβάσιμες, ευανάγνωστες, κατανοητές και προσαρμοσμένες στα αντίστοιχα υποκείμενα των δεδομένων.[96]

Η Αρχή του περιορισμού του σκοπού[97] προβλέπει ότι τα δεδομένα συλλέγονται για καθορισμένους ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περεταίρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς. Η αρχή του περιορισμού του σκοπού συγκαταλέγεται στις θεμελιώδεις αρχές του ευρωπαϊκού δικαίου για την προστασία δεδομένων. Συνδέεται στενά με τη διαφάνεια, την προβλεψιμότητα και τον έλεγχο του χρήστη: εάν ο σκοπός της επεξεργασίας είναι επαρκώς συγκεκριμένος και σαφής, τα άτομα γνωρίζουν τι να περιμένουν και αυξάνονται η διαφάνεια και η ασφάλεια δικαίου. Ταυτόχρονα, η σαφής οριοθέτηση του σκοπού είναι σημαντική προϋπόθεση ώστε τα υποκείμενα των δεδομένων να μπορούν να ασκούν αποτελεσματικά τα δικαιώματά τους, όπως το δικαίωμα εναντίωσης στην επεξεργασία.[98]
Τα πιστωτικά ιδρύματα διασφαλίζουν ότι τα προσωπικά δεδομένα των υποκειμένων συλλέγονται μόνο για νόμιμους και θεμιτούς κάθε φορά σκοπούς και υπόκεινται σε επεξεργασία μόνο κατά τρόπο και στην έκταση που εξυπηρετείται η επίτευξη των σκοπών αυτών. Τα πιστωτικά ιδρύματα καθορίζουν τους σκοπούς της επεξεργασίας των προσωπικών δεδομένων των συμβαλλομένων με αυτά υποκειμένων εντός του πλαισίου της επιχειρηματικής τους δραστηριότητας, όπως αυτή προσδιορίζεται στον καταστατικό σκοπό τους, το θεσμικό πλαίσιο και τις συμβατικές τους υποχρεώσεις, αρκεί να μην θίγονται υπέρμετρα τα έννομα συμφέροντα και οι ελευθερίες των υποκειμένων. Οφείλουν να τεκμηριώνουν κατάλληλα τη νομική βάση για κάθε σκοπό επεξεργασίας, ιδίως στην περίπτωση ειδικών κατηγοριών δεδομένων, όπως δεδομένων υγείας ή ποινικών καταδικών ή αδικημάτων, όπου αυτά είναι απολύτως απαραίτητα.[99]
Η κύρια κατά νόμο δραστηριότητα των πιστωτικών ιδρυμάτων είναι η αποδοχή καταθέσεων και η χορήγηση δανείων, που μπορεί να συμπληρώνονται και από άλλες δραστηριότητες, μεταξύ των οποίων η παροχή επενδυτικών υπηρεσιών (Ν. 4514/2018).
Στο πλαίσιο αυτό τα πιστωτικά ιδρύματα διαθέτουν στους πελάτες τους προϊόντα όπως καταθετικά, χορηγητικά, δάνεια και πιστώσεις κάθε μορφής, επενδυτικά, αλλά και προϊόντα μεικτών χαρακτηριστικών (πχ. κατάθεση μέρος της οποίας επενδύεται σε αξίες) κλπ. Για τη χορήγηση αυτών των προϊόντων και την παροχή των σχετικών υπηρεσιών τα πιστωτικά ιδρύματα

[96]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018, σελ.155
[97]Άρθρο 5, παρ.1 στοιχ. β' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[98]Ομάδα εργασίας του άρθρου 29 (2013), Opinion 3/13 on purpose limitation, WP 203,2 Απριλίου 2013.
[99]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019., Άρθρο 4.

επεξεργάζονται προσωπικά δεδομένα, τόσο σε προσυμβατικό στάδιο, όσο και κατά τη διάρκεια ισχύος των σχετικών συμβάσεων, για τη λειτουργία αυτών, και μετά από τη λήξη της ισχύος τους, για την προάσπιση των εννόμων συμφερόντων των ιδίων, ή των αντισυμβαλλομένων τους.
Συμπερασματικά, ο σκοπός της επεξεργασίας δεδομένων πρέπει να καθορίζεται προτού ξεκινήσει η επεξεργασία. Δεν επιτρέπεται περαιτέρω επεξεργασία των δεδομένων κατά τρόπο ασύμβατο προς τον αρχικό σκοπό, παρότι ο Γενικός Κανονισμός για την Προστασία Δεδομένων προβλέπει εξαιρέσεις από τον κανόνα αυτό για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς. Κατ' ουσίαν, η αρχή του περιορισμού του σκοπού σημαίνει ότι κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται για συγκεκριμένο, καλά καθορισμένο σκοπό και μόνο για πρόσθετους, συγκεκριμένους σκοπούς ,οι οποίοι είναι συμβατοί προς τον αρχικό.[100]

Σύμφωνα με την Αρχή της ελαχιστοποίησης των δεδομένων[101], τα δεδομένα πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά (να περιορίζονται στο αναγκαίο) σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται προς επεξεργασία. Η επεξεργασία δεδομένων πρέπει να περιορίζεται στο αναγκαίο μέτρο για την εκπλήρωση νόμιμου σκοπού. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να πραγματοποιείται μόνο όταν ο σκοπός της επεξεργασίας δεν μπορεί να επιτευχθεί με άλλα μέσα. Η επεξεργασία δεδομένων δεν πρέπει να επεμβαίνει δυσανάλογα στα συμφέροντα, στα δικαιώματα και στις ελευθερίες που διακυβεύονται.
Οι κατηγορίες δεδομένων που επιλέγονται για επεξεργασία πρέπει να είναι αναγκαίες για την επίτευξη του δεδηλωμένου συνολικού σκοπού των πράξεων επεξεργασίας, και ο υπεύθυνος επεξεργασίας θα πρέπει να περιορίζει αυστηρά τη συλλογή δεδομένων σε τέτοιες πληροφορίες οι οποίες είναι άμεσα συναφείς με τον συγκεκριμένο σκοπό που επιδιώκεται με την επεξεργασία.

Η Αρχή της ακρίβειας των δεδομένων προβλέπει ότι τα δεδομένα πρέπει να είναι ακριβή και όταν απαιτείται να ελέγχονται ως προς την ακρίβειά τους και να υποβάλλονται σε τακτική ενημέρωση και επικαιροποίηση σύμφωνα με τις υφιστάμενες για το σκοπό αυτό θεσπισμένες διαδικασίες. Πρέπει να λαμβάνονται όλα τα εύλογα μέτρα που προβλέπονται για την άμεση, χωρίς καθυστέρηση, διαγραφή ή διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα, λαμβανομένων υπόψη των σκοπών της επεξεργασίας. Ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει την αρχή της ακρίβειας των

[100]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018, σελ.156
[101] Άρθρο 5, παρ.1 στοιχ. γ' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

δεδομένων σε όλες τις πράξεις επεξεργασίας.
Υπεύθυνος επεξεργασίας ο οποίος κατέχει προσωπικές πληροφορίες δεν χρησιμοποιεί τις πληροφορίες αυτές αν δεν λάβει μέτρα που να διασφαλίζουν με εύλογη βεβαιότητα ότι τα δεδομένα είναι ακριβή και επικαιροποιημένα.[102]
Ο Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και το Συμβούλιο της Ευρώπης παραθέτουν[103] το παρακάτω παράδειγμα: Όταν ένα πρόσωπο επιθυμεί να συνάψει σύμβαση δανείου με τραπεζικό ίδρυμα, η τράπεζα ελέγχει συνήθως την πιστοληπτική ικανότητα του δυνητικού πελάτη. Για τον σκοπό αυτό, υπάρχουν ειδικές βάσεις δεδομένων οι οποίες περιέχουν στοιχεία για το πιστωτικό ιστορικό φυσικών προσώπων. Εάν μια τέτοια βάση δεδομένων παρέχει ανακριβή ή παρωχημένα στοιχεία για ένα φυσικό πρόσωπο, το γεγονός αυτό μπορεί να έχει αρνητικές συνέπειες για το εν λόγω πρόσωπο. Επομένως, οι υπεύθυνοι επεξεργασίας τέτοιων βάσεων δεδομένων πρέπει να καταβάλλουν ιδιαίτερες προσπάθειες ώστε να τηρούν την αρχή της ακρίβειας των δεδομένων.

Σύμφωνα με την Αρχή του περιορισμού της περιόδου αποθήκευσης[104]τα δεδομένα θα πρέπει να διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων των δεδομένων για χρονικό διάστημα όχι μεγαλύτερο από αυτό που είναι αναγκαίο για την επίτευξη των σκοπών για τους οποίους υποβάλλονται σε επεξεργασία. Επομένως, τα δεδομένα πρέπει να διαγράφονται ή να ανωνυμοποιούνται όταν οι σκοποί αυτοί έχουν εκπληρωθεί. Για τον σκοπό αυτό, ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για τη διαγραφή τους ή για την περιοδική επανεξέτασή τους, ώστε να διασφαλίζεται ότι τα δεδομένα δεν διατηρούνται περισσότερο από όσο είναι αναγκαίο.[105]Χρονικός περιορισμός της αποθήκευσης δεδομένων προσωπικού χαρακτήρα εφαρμόζεται μόνο σε δεδομένα που διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων τους. Επομένως, νόμιμη αποθήκευση δεδομένων τα οποία δεν είναι πλέον αναγκαία θα μπορούσε να επιτευχθεί μέσω της ανωνυμοποίησής τους.
Η αρχειοθέτηση δεδομένων για λόγους δημόσιου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς μπορεί να επιτρέπεται για μεγαλύτερα διαστήματα, εφόσον τα εν λόγω δεδομένα χρησιμοποιηθούν μόνο για τους ανωτέρω σκοπούς. Για τη συνεχή αποθήκευση και χρήση δεδομένων προσωπικού χαρακτήρα πρέπει να εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα, ώστε να διασφαλίζονται τα δικαιώματα και οι ελευθερίες του υποκειμένου των

[102]Άρθρο 5, παρ.1 στοιχ. δ' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[103] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018, σελ.166
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
[104] Άρθρο 5, παρ.1 στοιχ. ε' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[105] Αιτιολογική σκέψη 39 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016.

δεδομένων.[106]

Η Αρχή της ακεραιότητας και εμπιστευτικότητας προβλέπει ότι τα δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εγκεκριμένη ή παράνομη επεξεργασία, τυχαία απώλεια, καταστροφή ή φθορά, με χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων. Να τηρούνται επαρκή μέτρα ασφαλείας για την προστασία των δεδομένων και την πρόληψη κινδύνων όπως απώλεια, μη εξουσιοδοτημένη πρόσβαση, καταστροφή, παράνομη χρήση ή αποκάλυψη.
Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία θα πρέπει να λαμβάνουν υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκο¬πούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, όταν εφαρμόζουν τέτοια μέτρα. Ανάλογα με τις ειδικές συνθήκες κάθε περίπτωσης, τα κατάλληλα τεχνικά και οργανωτικά μέτρα θα μπορούσαν να περιλαμβάνουν, για παράδειγμα, ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα και/ή τακτική δοκιμή και αξιολόγηση της αποτελεσματικότητας των μέτρων ώστε να διασφαλίζεται η ασφάλεια της επε¬ξεργασίας δεδομένων.[107]
Στο άρθρο 25 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016, στο οποίο εξετάζεται η προστασία των δεδομένων ήδη από τον σχεδιασμό, αναφέρεται ρητά η ψευδωνυμοποίηση ως παράδειγμα κατάλληλου τεχνικού και οργανωτικού μέτρου το οποίο θα πρέπει να εφαρμό¬ζουν οι υπεύθυνοι επεξεργασίας για την τήρηση των αρχών της προστασίας δεδομένων και την ενσωμάτωση των απαραίτητων εγγυήσεων. Με τον τρόπο αυτό, οι υπεύθυνοι επεξεργασίας θα ανταποκρίνονται στις απαιτήσεις του κανο¬νισμού και θα προστατεύουν τα δικαιώματα των υποκειμένων των δεδομένων όταν προβαίνουν σε επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Ψευδωνυμοποίηση δεδομένων σημαίνει αντικατάσταση των χαρακτηριστικών στα δεδομένα προσωπικού χαρακτήρα – τα οποία καθιστούν εφικτή την ταυτοποίηση του υποκειμένου των δεδομένων– με ψευδώνυμο και τη διατήρηση των εν λόγω χαρακτηριστικών χωριστά, με τη χρήση τεχνικών ή οργανωτικών μέτρων. Η διαδικασία της ψευδωνυμοποίησης δεν πρέπει να συγχέεται με τη διαδικασία της ανωνυμοποίησης, στην οποία όλοι οι σύνδεσμοι που καθιστούν εφικτή την ταυτοποίηση του προσώπου έχουν διαρρηχθεί.
Η ψευδωνυμοποίηση είναι μέτρο ώστε τα δεδομένα προσωπικού χαρακτήρα

[106]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.165
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
[107] Άρθρο 32 παράγραφος 1. του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

να μην μπορούν να αποδοθούν στο υποκείμενο των δεδομένων χωρίς πρόσθετες πλη¬ροφορίες, οι οποίες διατηρούνται χωριστά. Το «κλειδί» που καθιστά εφικτή την εκ νέου εξακρίβωση της ταυτότητας των υποκειμένων των δεδομένων πρέπει να δια¬τηρείται χωριστά και υπό ασφαλείς συνθήκες. Τα δεδομένα τα οποία αποτέλεσαν αντικείμενο ψευδωνυμοποίησης παραμένουν δεδομένα προσωπικού χαρακτήρα. Δεδομένα προσωπικού χαρακτήρα με κρυπτογραφημένα χαρακτηριστικά ή χαρακτηριστικά που τηρούνται χωριστά χρησιμοποιούνται σε πολλά πλαίσια ως τρόπος διαφύλαξης του απορρήτου της προσωπικής ταυτότητας. Η μέθοδος αυτή είναι ιδιαιτέρως χρήσιμη όταν οι υπεύθυνοι επεξεργασίας πρέπει να δια¬σφαλίσουν ότι πρόκειται για το ίδιο υποκείμενο δεδομένων, αλλά δεν χρειάζο¬νται ή απαγορεύεται να γνωρίζουν την πραγματική ταυτότητα του υποκειμένου των δεδομένων.[108]
Το Συμβούλιο της Ευρώπης παραθέτει ως παραδείγματα κατάλληλων μέτρων ασφάλειας για την προστασία των δεδο¬μένων προσωπικού χαρακτήρα επίσης την τήρηση των δεδομένων σε ασφαλές φυσικό περιβάλλον, το περιορισμό της πρόσβασης με αλλεπάλληλες συνδέσεις και την προστασία της κοινοποίησης δεδομένων με ισχυρή κρυπτογράφηση.[109]
Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας οφείλει να γνωστοποιεί αμελλητί στην αρμόδια εποπτική αρχή την παρα¬βίαση και τους σχετικούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.[110] Παρόμοια υποχρέωση ανακοίνωσης και προς το υποκείμενο των δεδομένων υφίσταται όταν η παραβίαση των δεδομένων προσωπικού χαρα¬κτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες του.[111]

Σύμφωνα με την Αρχή της λογοδοσίας ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και οφείλει να είναι σε θέση να αποδείξει τη συμμόρφωση και την τήρηση των προβλεπόμενων υποχρεώσεών του, σύμφωνα με τις βασικές Αρχές προστασίας δεδομένων.
Η λογοδοσία επιβάλλει σε υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία να εφαρμόζουν, ενεργώς και αδιάλειπτα, μέτρα για την προώ¬θηση και τη διασφάλιση της προστασίας των δεδομένων στις δραστηριότητες επεξεργασίας.
Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία είναι υπεύθυνοι για τη συμμόρφωση των πράξεων επεξεργασίας προς το δίκαιο για την προστασία των δεδομένων και τις αντίστοιχες υποχρεώσεις τους. Οι

[108] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.167
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
[109] Συμβούλιο της Ευρώπης, Επιτροπή της Σύμβασης 108, Γνώμη για τις επιπτώσεις της επεξεργασίας των ονομαστικών καταστάσεων επιβατών στην προστασία δεδομένων (Opinion on the Data protection implications of the processing of Passenger Name Records), T-PD(2016)18rev, 19 Αυγούστου 2016, σ. 9.
[110] Άρθρο 33 παράγραφος 1 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[111] Άρθρο 34, παρ1 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

υπεύθυνοι επεξεργασίας πρέπει να είναι σε θέση να αποδεικνύουν ανά πάσα στιγμή τη συμμόρφωση προς τις διατάξεις περί προστασίας των δεδομένων στα υποκείμενα των δεδομένων, στο ευρύ κοινό και στις εποπτικές αρχές. Οι εκτελού¬ντες την επεξεργασία οφείλουν επίσης να συμμορφώνονται προς ορισμένες υπο¬χρεώσεις οι οποίες συνδέονται αυστηρά με τη λογοδοσία ,όπως τήρηση αρχείου πράξεων επεξεργασίας και διορισμός υπευθύνου προστασίας δεδομένων.[112]

Ο ορισμός υπευθύνου προστασίας δεδομένων, ο οποίος θα εμπλέκεται σε όλα τα θέματα που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα διευκολύνει τη συμμόρφωση προς την παραπάνω υποχρέωση. Επίσης, η συμμόρφωση διευκολύνεται εάν πραγματοποιηθεί εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων για τύπους επεξεργασίας οι οποίοι είναι πιθανό να συνεπάγονται υψηλό κίν¬δυνο για τα δικαιώματα και τις υποχρεώσεις φυσικών προσώπων, εάν προβλεφθεί διασφάλιση της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, με την εφαρμογή ρυθμίσεων και διαδικασιών για την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, καθώς και με την τήρηση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης.

Αναφέρουμε ότι για τα ελληνικά τραπεζικά ιδρύματα, η Ένωση Ελληνικών Τραπεζών, ως φορέας εκπροσώπησης των ελληνικών και ξένων πιστωτικών ιδρυμάτων που λειτουργούν στην Ελλάδα, έχει καταρτίσει σχέδιο Κώδικα Δεοντολογίας για την επεξεργασία των προσωπικών δεδομένων στο χρηματοπιστωτικό σύστημα, το οποίο και έχει υποβάλλει προς έγκριση στην Αρχή Προστασίας Δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 40 παρ. 5 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ)2016/679.

2.1.1 Στοιχεία προς επεξεργασία

Σημειώνεται ότι η Τράπεζα επεξεργάζεται κάθε φορά μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Ειδικότερα, η Τράπεζα ενδέχεται να επεξεργάζεται τα κάτωθι προσωπικά δεδομένα:

Α. Προσωπικά δεδομένα, τα οποία της παρέχει κυρίως το υποκείμενο των δεδομένων:

- στοιχεία ταυτοποίησης & νομιμοποίησης (ονοματεπώνυμο, ημερομηνία/ τόπος γέννησης, στοιχεία δελτίου ταυτότητας/ διαβατηρίου, ΑΜΚΑ)
- δημογραφικά στοιχεία (φύλο, εθνικότητα, οικογενειακή κατάσταση). Τα δεδομένα αυτά συλλέγονται απευθείας από τα υποκείμενα ή/και από δημόσια προσβάσιμες πηγές ή/και από δημόσια προσβάσιμα κοινωνικά δίκτυα (π.χ.

[112] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.171
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

faceboook, twitter).

- στοιχεία επικοινωνίας (ταχυδρομική διεύθυνση, αριθμός σταθερής ή κινητής τηλεφωνίας, διεύθυνση ηλεκτρονικού ταχυδρομείου). Τα δεδομένα συλλέγονται απευθείας από τα υποκείμενα ή/και από δημόσια προσβάσιμες πηγές ή/και κοινωνικά δίκτυα και από συνεργαζόμενες με το πιστωτικό ίδρυμα εταιρείες, όπως εταιρείες ενημέρωσης οφειλετών (Ν. 3758/2009), εταιρείες διαχείρισης απαιτήσεων (Ν. 4354/2015) ή εντολοδόχους δικηγόρους, δικηγορικές εταιρείες ή δικαστικούς επιμελητές.
- οικονομικά στοιχεία (πληροφορίες που αφορούν μισθολογική και περιουσιακή κατάσταση, φορολογική κατοικία). Τα εν λόγω δεδομένα συλλέγονται είτε απευθείας από τα υποκείμενα, είτε από δημόσια προσβάσιμες πηγές, όπως υποθηκοφυλακεία, κτηματολογικά γραφεία κλπ.
- στοιχεία σύνδεσης σε ηλεκτρονικές εφαρμογές και στοιχεία ηλεκτρονικής ταυτοποίησης (π.χ. ηλεκτρονική υπογραφή).
- σε ειδικές περιπτώσεις δεδομένα που σχετίζονται με στοιχεία υγείας και με συνθήκες διαβίωσης (λ.χ. σε συμμόρφωση με τις υποχρεώσεις της Τράπεζας για υπεύθυνο δανεισμό), που συλλέγονται αποκλειστικά από το υποκείμενο των δικαιωμάτων και μόνο, με δική του πρωτοβουλία .

Β. Δεδομένα προσωπικού χαρακτήρα που συλλέγει η εκάστοτε Τράπεζα για τους πελάτες της:

- στο πλαίσιο ελέγχου δέουσας επιμέλειας, ελέγχου κυρώσεων και καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.
- στο πλαίσιο ελέγχου και αξιολόγησης της πιστοληπτικής ικανότητας, διαχείρισης κινδύνων της Τράπεζας και εν γένει εξυπηρέτησης της εκάστοτε συμβατικής ή συναλλακτικής σχέσης με την Τράπεζα. Τα εν λόγω δεδομένα συλλέγονται από το πιστωτικό ίδρυμα στο πλαίσιο των συναλλακτικών σχέσεων των πελατών του με αυτό, από αρχεία δεδομένων οικονομικής συμπεριφοράς και κυρίως την εταιρεία με την επωνυμία “ΤΡΑΠΕΖΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΑΕ” και διακριτικό τίτλο ΤΕΙΡΕΣΙΑΣ Α.Ε. ή οποιαδήποτε εταιρεία επεξεργασίας δεδομένων οικονομικής συμπεριφοράς στην Ελλάδα ή σε άλλο κράτος μέλος της Ευρωπαϊκής Ένωσης ή από δημόσια προσβάσιμες πηγές όπως Δικαστήρια κλπ.[113]
- Δεδομένα στο πλαίσιο συμμόρφωσης με το ισχύον νομοθετικό και κανονιστικό πλαίσιο υποβολής εποπτικών στοιχείων και πληροφοριών
- Οικονομικά στοιχεία αποτίμησης της επενδυτικής και οικονομικής κατάστασης και συμπεριφοράς, των πελατών (και υποψηφίων πελατών). Δεδομένα για τις γνώσεις και την εμπειρία στον επενδυτικό τομέα ή στον τομέα των ασφαλίσεων, την χρηματοοικονομική κατάσταση, το επίπεδο ανοχής στον κίνδυνο και στους επενδυτικούς σας στόχους, τα οποία συλλέγονται απευθείας από τον πελάτη.

[113] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

- Δεδομένα αναγνωριστικά της ηλεκτρονικής ταυτότητας του Πελάτη, όπως η διεύθυνση διαδικτυακού πρωτοκόλλου (IP Address). Δεδομένα περιήγησης στο διαδίκτυο (πχ. cookies) μετά από σχετική ενημέρωση των πελατών και παροχής σχετικής συγκατάθεσης, εκτός των περιπτώσεων που η συλλογή των δεδομένων αυτών είναι απαραίτητη για την λειτουργία των συστημάτων του πιστωτικού ιδρύματος (πχ. βασικά cookies) και συναφείς τεχνολογίες που παρέχουν διευκόλυνση πρόσβασης και χρήσης συγκεκριμένων υπηρεσιών ή /και σελίδων του δικτυακού ιστοτόπου και για στατιστικούς λόγους.
- Δεδομένα στο πλαίσιο αλληλογραφίας και εν γένει επικοινωνίας της Τράπεζας με τους πελάτες της, όπως τηλεφωνικών ή και διαδικτυακών επικοινωνιών του Πελάτη με το πιστωτικό ίδρυμα που καταγράφονται σύμφωνα με το κατά περίπτωση θεσμικό πλαίσιο.
- Δεδομένα διενέργειας πράξεων πληρωμών και παροχής υπηρεσιών πληρωμών, τα οποία συλλέγονται από τον πελάτη ή τον πάροχο υπηρεσιών πληρωμών που έχει αυτός επιλέξει.
- Στοιχεία που διαβιβάζονται από εποπτικές, δικαστικές, και λοιπές Δημόσιες και Ανεξάρτητες Αρχές και αφορούν ποινικές καταδίκες, αδικήματα, επιβολή μέτρων διασφάλισης των συμφερόντων του Δημοσίου, κατασχέσεων, δημεύσεων, δεσμεύσεων. Δεδομένα που χρησιμοποιούνται για την αξιολόγηση του κινδύνου νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή/και χρηματοδότησης της τρομοκρατίας, τα οποία συλλέγονται από το ίδιο το υποκείμενο, από τις συναλλαγές που πραγματοποιεί, από την εταιρία με την επωνυμία, "ΤΡΑΠΕΖΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΑΕ (ΤΕΙΡΕΙΣΙΑΣ ΑΕ), από αστυνομικές αρχές, όπως και από αρμόδιους φορείς του εξωτερικού που είναι επιφορτισμένοι με την πρόληψη και καταστολή των προαναφερθέντων εγκλημάτων.
- στοιχεία τα οποία είναι δημοσίως προσβάσιμα είτε ηλεκτρονικά, είτε με άλλο τρόπο.

  Η Τράπεζα προβαίνει στη συλλογή, τήρηση και επεξεργασία των προσωπικών δεδομένων, που γνωστοποιούνται σε αυτή από υποψήφιους ή/και υφισταμένους πελάτες και από εν γένει συναλλασσομένους με οποιαδήποτε ιδιότητα με αυτήν σε όλα τα στάδια της συναλλακτικής σας σχέσης στο πλαίσιο παροχής προϊόντων / υπηρεσιών από την Τράπεζα ή μέσω αυτής.

  Επίσης, προβαίνει στη συλλογή, τήρηση και επεξεργασία των στοιχείων που προκύπτουν από την κίνηση των τραπεζικών λογαριασμών ή/και από προηγούμενες χορηγήσεις από το τραπεζικό σύστημα.

2.1.2 Υπεύθυνος επεξεργασίας

Η σημαντικότερη συνέπεια που απορρέει από την ιδιότητα του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία είναι η νομική ευθύνη συμμόρ¬φωσης προς τις αντίστοιχες υποχρεώσεις βάσει του δικαίου για την προστασία δεδομένων. Στον ιδιωτικό τομέα, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επε¬ξεργασία είναι συνήθως φυσικό ή νομικό πρόσωπο. Μεταξύ

υπευθύνου επεξεργασίας δεδομένων και εκτελούντος την επεξεργασία υπάρχει σημαντική διαφορά: ο πρώτος είναι το φυσικό ή νομικό πρόσωπο που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας, ενώ ο δεύτερος είναι το φυσικό ή νομικό πρόσωπο που επεξεργάζεται τα δεδομένα για λογαριασμό του υπευθύνου, ακολουθώντας αυστηρές εντολές.

Όποιος καθορίζει τον τρόπο και τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα άλλων προσώπων είναι «υπεύθυνος επεξεργασίας» βάσει του δικαίου προστασίας δεδομένων· εάν λαμβάνουν την απόφαση αυτή περισσό¬τερα πρόσωπα από κοινού, μπορεί να είναι «από κοινού υπεύθυνοι επεξεργασίας».
Ο «εκτελών την επεξεργασία» είναι φυσικό ή νομικό πρόσωπο το οποίο επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπευθύνου επεξεργασίας. Ο εκτελών την επεξεργασία καθίσταται υπεύθυνος επεξεργασίας εάν καθορίζει ο ίδιος τον τρόπο και τους σκοπούς της.[114]
Καταρχήν, ο υπεύθυνος επεξεργασίας δεδομένων είναι αυτός που πρέπει να ασκεί έλεγχο στην επεξεργασία και έχει την ευθύνη αυτής, συμπεριλαμβανομένης της νομικής ευθύνης. Ωστόσο, με τη μεταρρύθμιση των κανόνων περί προστασίας δεδομέ¬νων, οι εκτελούντες την επεξεργασία υποχρεούνται πλέον να συμμορφώνονται με πολλές από τις απαιτήσεις που ισχύουν για τους υπευθύνους επεξεργασίας.[115]
Το κατά πόσον ένα πρόσωπο έχει την αρμοδιότητα να αποφασίζει και να καθορίζει τον σκοπό και τα μέσα της επεξεργασίας θα εξαρτάται από τα πραγ¬ματικά στοιχεία ή τις περιστάσεις της υπόθεσης. Σύμφωνα με τον ορισμό του υπευθύνου επεξεργασίας στον Γενικό Κανονισμό Προστασίας Δεδομένων, μπορεί να είναι φυσικά πρόσωπα, νομικά πρόσωπα ή άλλοι φορείς. Ωστόσο, η Ομάδα εργασίας του άρθρου 29 τόνισε[116] ότι, για να παρασχεθεί στα φυσικά πρόσωπα μια πιο σταθερή οντότητα για την άσκηση των δικαιωμάτων τους, «είναι προτιμότερο να θεωρείται υπεύθυνος της επεξεργασίας η εταιρεία ή ο φορέας παρά ένα συγκεκριμένο πρόσωπο εντός της εταιρείας ή του φορέα».
Ο ρόλος του υπευθύνου της επεξεργασίας είναι κρίσιμος και έχει ιδιαίτερη σημασία όταν πρόκειται να καθορισθεί η ευθύνη και να επιβληθούν κυρώσεις.[117] Η ιδιότητα του υπευθύνου της επεξεργασίας είναι πρωτίστως συνέπεια της πραγματολογικής περίστασης ότι μια οντότητα επέλεξε να

[114] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.129
[115] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.130
[116] Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», (00264/10/EL WP 169), 16 Φεβρουαρίου 2010 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf
[117] Σωτηρόπουλος Β., Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα, εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019, σελ. 94

επεξεργασθεί δεδομένα προσωπικού χαρακτήρα για τους δικούς της στόχους. Πράγματι, ένα απλώς τυπικό κριτήριο δεν θα ήταν αρκετό, για δύο τουλάχιστον λόγους: σε ορισμένες περιπτώσεις, ο τυπικός διορισμός ενός υπευθύνου της επεξεργασίας –ο οποίος προβλέπεται, για παράδειγμα, σε έναν νόμο, μια σύμβαση ή μια κοινοποίηση στην αρχή προστασίας δεδομένων– απλώς θα ελλείπει. Σε άλλες περιπτώσεις ενδέχεται ο τυπικός διορισμός να μην ανταποκρίνεται στην πραγματικότητα, αναθέτοντας τυπικά τον ρόλο του υπευθύνου της επεξεργασίας σε έναν φορέα ο οποίος δεν είναι στην πραγματικότητα σε θέση να «καθορίζει». Η σημασία της πραγματολογικής επιρροής αναδεικνύεται επίσης στην υπόθεση SWIFT.[118]

Στην υπόθεση SWIFT[119], τα ευρωπαϊκά τραπεζικά ιδρύματα ανέθεσαν στην βελγική εταιρία SWIFT, που δραστηριοποιείται στον τομέα της επεξεργασίας μηνυμάτων χρηματοοικονομικού περιεχομένου, αρχικώς ως εκτελούντα την επεξεργασία, να διενεργεί τη διαβίβαση δεδομένων στο πλαίσιο των τραπεζικών συναλλαγών. Η SWIFT διαβίβαζε τέτοια δεδομένα τραπεζικών συναλλαγών αποθηκευμένα σε ένα κέντρο υπολογιστικής υπηρεσίας στις Η.Π.Α. στο Office of Foreign Assets Control (Υπηρεσία ελέγχου περιουσιακών στοιχείων αλλοδαπών) (OFAC) του Υπουργείου Οικονομικών των Ηνωμένων Πολιτειών από τα τέλη του 2001 βάσει κλήσεων που εκδίδονταν σύμφωνα με την νομοθεσία των Η.Π.Α. για τους σκοπούς της καταπολέμησης της τρομοκρατίας, χωρίς να έχει διαταχθεί ρητώς να το πράττει από τα ευρωπαϊκά τραπεζικά ιδρύματα που την είχαν εργοδοτήσει. Η Ομάδα Εργασίας του άρθρου 29, κατά την αξιολόγηση της νομιμότητας της επεξεργασίας κατέληξε [120]ότι τα ευρωπαϊκά τραπεζικά ιδρύματα προσλαμβάνοντας τη SWIFT, αλλά και η SWIFT από μόνη της έπρεπε να θεωρηθούν από κοινού υπεύθυνοι επεξεργασίας, φέροντες την ευθύνη ενώπιον των ευρωπαίων πελατών τους για τη διαβίβαση των δεδομένων τους στις Αρχές των Η.Π.Α.[121]

Ενώ η SWIFT θεωρήθηκε τυπικά εκτελών την επεξεργασία, ενεργούσε στην πραγματικότητα, τουλάχιστον σε κάποιο βαθμό, ως υπεύθυνος της επεξεργασίας των δεδομένων. Στην περίπτωση εκείνη κατέστη σαφές ότι, μολονότι ο ορισμός ενός μέρους ως υπευθύνου της επεξεργασίας ή εκτελούντος την επεξεργασία των δεδομένων σε μια σύμβαση μπορεί να παρέχει συναφείς πληροφορίες σχετικά με το νομικό καθεστώς του εν λόγω μέρους, ο συγκεκριμένος συμβατικός ορισμός δεν είναι αποφασιστικής

[118] Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», (00264/10/EL WP 169), 16 Φεβρουαρίου 2010 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

[119] Παγκόσμια Εταιρεία Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών

[120] Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων, Γνώμη 10/2006 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από την Παγκόσμια Εταιρεία Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (SWIFT), (01935/06/EL WP128), 22 Νοεμβρίου 2006. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_el.pdf

[121] Σωτηρόπουλος Β., «Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019, σελ. 112

σημασίας για τον καθορισμό του πραγματικού καθεστώτος του, το οποίο πρέπει να βασίζεται σε συγκεκριμένες περιστάσεις.[122]

2.1.3 Σκοποί επεξεργασίας

Οι τράπεζες επεξεργάζονται δεδομένα στο πλαίσιο εκτέλεσης της σύμβασης ή πριν από τη σύναψη αυτής, ιδίως για τους παρακάτω καθορισμένους, ρητούς και νόμιμους σκοπούς:
i. Για την ταυτοποίηση και επαλήθευση των στοιχείων
ii. Για την επικοινωνία είτε σε προσυμβατικό στάδιο, είτε σχετικά με ζητήματα που αφορούν τη συναλλακτική σχέση του πελάτη με την Τράπεζα,
iii. Για την εξυπηρέτηση, διαχείριση, παρακολούθηση, διεκπεραίωση των συναλλαγών και την εν γένει παροχή του αιτηθέντος προϊόντος ή/και υπηρεσίας της Τράπεζας
iv. Για την εξυπηρέτηση όλων των μορφών συναλλαγών μέσω ηλεκτρονικών υπηρεσιών (συναλλαγές μέσω εναλλακτικών δικτύων),
v. Για την συγκέντρωση της απαραίτητης πληροφόρησης προκειμένου να αξιολογηθεί η δυνατότητα διάθεσης προϊόντος ή υπηρεσίας.
Οι τράπεζες προβαίνουν σε επεξεργασία δεδομένων, επίσης, στο πλαίσιο της νόμιμης λειτουργίας της Τράπεζας, της προάσπισης των συμφερόντων της καθώς και της εν γένει εύρυθμης λειτουργίας και προστασίας των συναλλαγών, ιδίως αναφορικά με τη συγκέντρωση ή/και ανάλυση δεδομένων που σχετίζονται μεταξύ άλλων με τα ενδιαφέροντα, τις προτιμήσεις και την εν γένει συναλλακτική δραστηριότητα της πελατείας στο πλαίσιο ανάπτυξης ή/και βελτίωσης των προϊόντων και υπηρεσιών της Τράπεζας. Επίσης, αναφορικά με την επίλυση τυχόν αιτημάτων/ παραπόνων της πελατείας. την εκτίμηση και διαχείριση κινδύνων στο πλαίσιο λειτουργίας της Τράπεζας, την πρόληψη και αντιμετώπιση περιπτώσεων εξαπάτησης και άλλων παράνομων δραστηριοτήτων με σκοπό την προστασία του κοινού και την ασφάλεια του προσωπικού, συμπεριλαμβανομένου του συστήματος βιντεοεπιτήρησης.
Επιπροσθέτως, κατά την περίπτωση μεταβίβασης, εκχώρησης (είτε απευθείας είτε ως εξασφάλιση απαιτήσεων) ή/και τιτλοποίησης οιουδήποτε ή του συνόλου των βαρών, απαιτήσεων, εγγυήσεων, προνομίων, τίτλων στο πλαίσιο οιασδήποτε συμφωνίας του πελάτη με την τράπεζα, σε οποιονδήποτε τρίτο/ους.
Είναι επίσης πιθανό να προβεί σε επεξεργασία στο πλαίσιο ενημέρωσής του πελάτη από την Τράπεζα για νέα προϊόντα ή/και υπηρεσίες της Τράπεζας και των Εταιρειών του Ομίλου της καθώς και τρίτων Εταιρειών, τα οποία διαθέτει η Τράπεζα, και ταιριάζουν με τα ενδιαφέροντα και τις προτιμήσεις του, εφόσον ο πελάτης έχει παράσχει τη ρητή του συγκατάθεση, για τον σκοπό αυτό.
Η Ένωση Ελληνικών Τραπεζών, στο κείμενο του «Κώδικα Δεοντολογίας για

[122] Σωτηρόπουλος Β., «Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019, σελ.80

την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», που κατέθεσε προς έγκριση από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,[123] αναφέρει ότι ανά κατηγορία προϊόντων και υπηρεσιών, τα πιστωτικά ιδρύματα επεξεργάζονται προσωπικά δεδομένα πελατών τους για τους ακόλουθους σκοπούς:

Εξυπηρέτηση καταθετικών προϊόντων και πράξεων πληρωμής.

Για τα καταθετικά προϊόντα η επεξεργασία αποσκοπεί κυρίως στην εκπλήρωση των εκ του νόμου υποχρεώσεων ταυτοποίησης του πελάτη, των επαγγελματικών του δραστηριοτήτων και της προέλευσης των πιστούμενων ή προς πίστωση χρημάτων στον καταθετικό λογαριασμό και στηρίζεται στην εκτέλεση σύμβασης, αλλά και στη νομική υποχρέωση των πιστωτικών ιδρυμάτων, να εφαρμόζουν τη νομοθεσία για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες (Ν. 4557/2018, ΕΤΠΘ 281/2009, όπως εκάστοτε ισχύουν).

Τα ανωτέρω ισχύουν και για κάθε μεμονωμένη πράξη πληρωμής ή αλληλουχία τέτοιων πράξεων, συμπεριλαμβανομένης της καταγραφής και αρχειοθέτησης όλων των εντολών που δίνουν πελάτες για κατάρτιση συναλλαγών επί χρηματοπιστωτικών μέσων, που εξειδικεύεται και ως υποχρέωση ηχογράφησης των εντολών που δίδονται τηλεφωνικώς.

Εξυπηρέτηση χορηγητικών προϊόντων και επεξεργασία δεδομένων οικονομικής συμπεριφοράς.

Για τα χορηγητικά προϊόντα, η επεξεργασία αποσκοπεί στην εκπλήρωση των νόμιμων και συμβατικών υποχρεώσεων του πιστωτικού ιδρύματος έναντι των καταθετών, των μετόχων και των εργαζομένων του, με σκοπό την πλήρη και κατά το δυνατόν ακριβέστερη εκτίμηση της φερεγγυότητας και πιστοληπτικής ικανότητας των πιστούχων πελατών του και του αναλαμβανόμενου πιστωτικού κινδύνου, κατά την κατάρτιση αλλά και για όλο το χρόνο ισχύος της συμβατικής σχέσεως. Προς τούτο τα πιστωτικά ιδρύματα συλλέγουν δεδομένα περιουσιακής και οικονομικής κατάστασης και οικονομικής συμπεριφοράς των πελατών τους, τόσο από τους ίδιους, όσο και από αρχεία τέτοιων δεδομένων που λειτουργούν νόμιμα στη χώρα ή άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης, εφόσον συντρέχει περίπτωση, αλλά και από κάθε άλλη νόμιμη διαθέσιμη πηγή. Κατά τα λοιπά η εν λόγω επεξεργασία στηρίζεται στην εκτέλεση της σχετικής σύμβασης, στο εντεύθεν έννομο συμφέρον του πιστωτικού ιδρύματος και στις νομικές υποχρεώσεις αυτού.

Οι τράπεζες προβαίνουν σε επεξεργασία δεδομένων που σχετίζονται με την εκτίμηση της πιστοληπτικής ικανότητας πελάτη, όπου κατά περίπτωση απαιτείται για την εξυπηρέτηση της συναλλακτικής σχέσης.

Το κύριο μέρος της επεξεργασίας των δυσμενών οικονομικών δεδομένων των πελατών των Τραπεζών στην Ελλάδα γίνεται από την «Τειρεσίας Α.Ε.»

[123]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

Η απευθείας πρόσβαση των Τραπεζών στη βάση δεδομένων της «Τειρεσίας Α.Ε.» επιτρέπεται μόνον για τον προληπτικό έλεγχο της πιστοληπτικής ικανότητας των πελατών (υφιστάμενων ή υποψήφιων). Υπάρχει ευθύνη για την σχετική ενημέρωση του υποκειμένου των δεδομένων. Δεν μπορεί να επεκταθεί σε άλλα πρόσωπα, που δεν μετέχουν στη συναλλακτική σχέση.
Οι Τράπεζες συλλέγουν και τηρούν αρχείο με δυσμενή στοιχεία πελατών τους, που ηλεκτρονικά διαβιβάζουν στην «Τειρεσίας Α.Ε.»

Εξυπηρέτηση επενδυτικών προϊόντων και υπηρεσίες φύλαξης και διοικητικής διαχειρίσεως τίτλων.
Η επεξεργασία που αποσκοπεί στην αξιολόγηση της συμβατότητας και κάθε άλλης αξιολόγησης ή κατηγοριοποίησης του πελάτη, όπως κατά περίπτωση απαιτείται, για τη δημιουργία ή διάθεση χρηματοπιστωτικού μέσου ή υπηρεσίας.Για τα επενδυτικά προϊόντα η επεξεργασία αποσκοπεί στην αξιολόγηση της γνώσης και της εμπειρίας του πελάτη ή του υποψηφίου πελάτη στον επενδυτικό τομέα που σχετίζεται με συγκεκριμένο τύπο προσφερόμενου ή ζητούμενου προϊόντος ή υπηρεσίας, των επενδυτικών του στόχων συμπεριλαμβανομένου του ορίου ανοχής του στον κίνδυνο, την οικονομική του κατάσταση και τους επενδυτικούς του στόχους για την διενέργεια των συγκεκριμένων συναλλαγών ή την παροχή συγκεκριμένων επενδυτικών υπηρεσιών.
Η επεξεργασία αποσκοπεί επίσης στη γνώση της προέλευσης των τηρούμενων ή προς τήρηση χρηματοπιστωτικών μέσων σε λογαριασμούς αϋλων τίτλων στα βιβλία του πιστωτικού ιδρύματος, καθώς και στην παρακολούθηση της κατάθεσης χρηματοπιστωτικών μέσων σε λογαριασμούς πελατών σε λογαριασμό ή λογαριασμούς που έχουν ανοιχθεί σε τρίτο, ώστε ανά πάσα στιγμή να μπορούν να παρέχουν πληροφόρηση για την κατοχή και φύλαξη των εν λόγω μέσων και της χρησιμοποίησης αυτών για ίδιο λογαριασμό ή για λογαριασμό άλλων πελατών, όπως το θεσμικό πλαίσιο επιβάλει (Ν.4514/2018, όπως εκάστοτε ισχύει). Κατ΄ ακολουθία η επεξεργασία στηρίζεται στις έννομες υποχρεώσεις του πιστωτικού ιδρύματος και στην εκτέλεση των σχετικών συμβάσεων.
Εξυπηρέτηση προϊόντων μικτών χαρακτηριστικών.
Στην περίπτωση των προϊόντων μικτών χαρακτηριστικών η επεξεργασία των σχετικών προσωπικών δεδομένων εξυπηρετεί τους αντίστοιχους των χαρακτηριστικών τους σκοπούς, κατά τα προαναφερθέντα.[124]
Στην έννοια της προώθησης τραπεζικών προϊόντων και υπηρεσιών για τους σκοπούς του παρόντος κανονισμού εντάσσεται η με οποιονδήποτε τρόπο προώθηση αυτών σε υφιστάμενους ή εν δυνάμει πελάτες των πιστωτικών ιδρυμάτων, εφόσον πρόκειται για φυσικά πρόσωπα, όχι όμως και η απρόσωπη γενική διαφήμιση αυτών.

[124]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 4.2

Προώθηση τραπεζικών προϊόντων και υπηρεσιών

Η προώθηση τραπεζικών προϊόντων και υπηρεσιών αποβλέπει στην ικανοποίηση του έννομου συμφέροντος των πιστωτικών ιδρυμάτων να επεκτείνουν την πελατεία τους ή την διάθεση των προϊόντων και υπηρεσιών τους σε αυτή, και επομένως η επεξεργασία στην περίπτωση αυτή στηρίζεται στο έννομο συμφέρον του πιστωτικού ιδρύματος.

Για την επίτευξη του σκοπού αυτού πέραν της γενικής διαφήμισης, τα πιστωτικά ιδρύματα επεξεργάζονται τα προσωπικά δεδομένα πελατών ή υποψηφίων πελατών τους για την ενημέρωσή τους, για την καλλίτερη αξιοποίηση προϊόντων που τους έχουν ήδη παρασχεθεί ή για την προώθηση νέων προϊόντων του πιστωτικού ιδρύματος, των εταιριών του ομίλου του ή τρίτων επιχειρήσεων που συνεργάζονται με το πιστωτικό ίδρυμα.

Σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων Ε.Ε. 679/2016, όταν γίνεται επεξεργασία προσωπικών δεδομένων για σκοπούς εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται σε κάθε περίπτωση να αντιταχθεί[125] . Όμως όταν πρόκειται για αυτοματοποιημένη επεξεργασία κατάρτισης προφίλ, που παράγει έννομα αποτελέσματα για το υποκείμενο ή το επηρεάζουν σημαντικά, η επεξεργασία με σκοπό την εμπορική προώθηση επιτρέπεται μόνο μετά τη ρητή προς τούτο συγκατάθεση του υποκειμένου [126].

Έχοντας αυτά υπόψη πρέπει να γίνει διάκριση μεταξύ της ενημέρωσης των πελατών των πιστωτικών ιδρυμάτων για προϊόντα ή/και υπηρεσίες που έχουν ήδη λάβει και της προώθησης νέων προϊόντων ή/και υπηρεσιών.

Με την ενημέρωση, το πιστωτικό ίδρυμα γνωστοποιεί στον πελάτη του νέα χαρακτηριστικά ή λειτουργικότητες των προϊόντων που έχει ήδη χορηγήσει ή νέες ευκαιρίες χρήσης αυτών ή τρόπους επωφελέστερης χρήσης τους. Χαρακτηριστικά σχετικά παραδείγματα είναι τα προγράμματα επιβράβευσης της χρήσης καρτών με την επιστροφή στους κατόχους χρημάτων ή εξαργυρώσιμων πόντων.

Η ενημέρωση αυτή δεν αποτελεί προώθηση προϊόντος, εφόσον το προϊόν έχει ήδη χορηγηθεί. Εφόσον δε αυτή αφορά σε χαρακτηριστικά ή λειτουργικότητες που υπήρχαν κατά τη χορήγηση του προϊόντος ή για την προοπτική των οποίων υπήρξε πληροφόρηση, η εν λόγω ενημέρωση αποτελεί μέρος αυτού, που δεν μπορεί να διαχωριστεί για κάποιους μόνο από τους πελάτες των συγκεκριμένων προϊόντων. Πρόκειται συνεπώς για εκτέλεση υπάρχουσας σύμβασης, ώστε δεν τίθεται θέμα προώθησης και συνακόλουθα εναντίωσης για τις συγκεκριμένες ενημερώσεις.[127]

Όσον αφορά στην προώθηση νέων προϊόντων ή και υπηρεσιών, με βάση την τραπεζική πρακτική, στο χώρο των πιστωτικών ιδρυμάτων, κατά κανόνα, αυτής προηγείται η κατάρτιση προφίλ των υποκειμένων, προς τα οποία θα γίνει η προώθηση. Περαιτέρω σημειώνεται ότι λόγω της φύσης των

[125]Άρθρο 21, παρ. 2 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[126] Άρθρο 22, παρ. 1 και 2 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[127]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 4.3

τραπεζικών προϊόντων, κυρίως των χορηγητικών, δεν είναι σε κάθε περίπτωση σαφές πότε από την ως άνω προώθηση ενδέχεται το υποκείμενο να επηρεασθεί σημαντικά και πότε όχι. Κατά συνέπεια είναι πιθανό να δημιουργηθεί σύγχυση στο κοινό στο οποίο τα πιστωτικά ιδρύματα θα απευθύνονται, εφόσον θα υπάρχουν περιπτώσεις προώθησης για τι οποίες θα ζητείται η προηγούμενη σχετική συγκατάθεση και άλλες για τις οποίες θα παρέχεται απλώς το δικαίωμα εναντίωσης.

Για τους ανωτέρω λόγους ασφαλέστερη λύση είναι τα πιστωτικά ιδρύματα να επιδιώκουν την λήψη της προς τούτο συγκατάθεσης, των υποκειμένων, στα οποία πρόκειται να απευθύνουν τις προωθητικές τους ενέργειες.

Σε κάθε περίπτωση πάντως το δικαίωμα αντίρρησης (opt out) πρέπει να παρέχεται στο υποκείμενο σε κάθε εξατομικευμένη προωθητική ενέργεια.

Από την κατά τα ανωτέρω λήψη συγκατάθεσης, ως βάσης για την επεξεργασία προσωπικών δεδομένων για σκοπούς εμπορικής προώθησης, εξαιρούνται τα αμιγώς καταθετικά προϊόντα τα οποία κανένα κίνδυνο συνεπάγονται για τα υποκείμενα των δεδομένων-πελάτες. Παρά ταύτα στις περιπτώσεις αυτές πρέπει να παρέχεται στο υποκείμενο το δικαίωμα εναντίωσης.[128]

Διεξαγωγή έρευνας ικανοποίησης πελατών.

Με τις έρευνες αυτές τα πιστωτικά ιδρύματα επιδιώκουν αφενός να διαπιστώσουν το βαθμό ικανοποίησης των πελατών τους από τα προϊόντα και τις υπηρεσίες που τους έχουν προσφέρει τα ίδια ή οι λοιπές εταιρείες του ομίλου του και αφετέρου να καταγράψουν σχετικές ανάγκες αυτών για να προσπαθήσουν στη συνέχεια να τις καλύψουν με τη βελτίωση των προϊόντων τους ή την ανάπτυξη νέων. Η έρευνα ικανοποίησης δεν αποτελεί συνεπώς προωθητική ενέργεια, αλλά, στο μέτρο που εμπεριέχει επεξεργασία προσωπικών δεδομένων και δεν γίνεται ανώνυμα, εξυπηρετεί το έννομο συμφέρον των πιστωτικών ιδρυμάτων και αποβλέπει στη βελτίωση και αναβάθμιση των υπηρεσιών προς τους πελάτες τους, την ενίσχυση της πελατειακής σχέσης και την προαγωγή της επιχειρηματικής δραστηριότητας με την ανάπτυξη νέων υπηρεσιών, λήψη διορθωτικών μέτρων κλπ.

Συνεπώς, οι έρευνες αγοράς, ακόμα και εάν γίνονται μετά από κατάρτιση προφίλ των πελατών στους οποίους τα πιστωτικά ιδρύματα κατά περίπτωση απευθύνονται, δεν συνεπάγονται για αυτούς έννομες συνέπειες, ούτε τους επηρεάζουν σημαντικά, ενώ σε κάθε περίπτωση η συμμετοχή του υποκειμένου στην έρευνα είναι προαιρετική.

Δημόσια προβολή δραστηριότητας και εταιρικού προφίλ του πιστωτικού ιδρύματος (Δημόσιες Σχέσεις)

Στο πλαίσιο του σκοπού αυτού είναι δυνατό να γίνεται επεξεργασία προσωπικών δεδομένων υποκειμένων που έχουν την ιδιότητα του πελάτη ή και όχι, εφόσον αυτή είναι αναγκαία για την δημόσια προβολή της εικόνας και

[128]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 4.3

της δραστηριότητας του πιστωτικού ιδρύματος. Ως ενδεικτικά παραδείγματα αναφέρονται : επεξεργασία δεδομένων κειμένων εκπροσώπων ΜΜΕ, επεξεργασία δεδομένων υποκείμενων που ευεργετούνται από χορηγίες ή παροχές αριστείας ή άλλες παροχές κοινωνικού ή φιλανθρωπικού χαρακτήρα. Επίσης, δράσεις του πιστωτικού ιδρύματος που προάγουν το κοινό συμφέρον σε θέματα περιβάλλοντος, ανάπτυξης και κοινωνικής ευθύνης. Στις περιπτώσεις αυτές η συμμετοχή των ως άνω προσώπων στις παραπάνω δράσεις, μετά τη σχετική ενημέρωσή τους για το είδος της επεξεργασίας των προσωπικών τους δεδομένων, τους σκοπούς της και τους αποδέκτες τους, συνιστά έμπρακτη συγκατάθεση για αυτή.

Επίσης οι τράπεζες καλούνται να προβούν σε επεξεργασία δεδομένων στο πλαίσιο συμμόρφωσης τους με τις υποχρεώσεις που θεσπίζονται από το εκάστοτε ισχύον νομοθετικό και κανονιστικό πλαίσιο.

Πρόληψη και Εντοπισμός Εγκληματικών ενεργειών.

Τα πιστωτικά ιδρύματα επεξεργάζονται τα προσωπικά δεδομένα των εργαζομένων τους, των πελατών τους, των διερχομένων από τα καταστήματά τους και αυτών που χρησιμοποιούν τις αυτόματες ταμειολογιστικές μηχανές (ATMs) τους, στο πλαίσιο της εκπλήρωσης των εκ του νόμου υποχρεώσεών τους, αλλά και των έννομων συμφερόντων τους, με σκοπό την πρόληψη και αποτροπή εγκληματικών πράξεων κατά της ζωής και της περιουσίας των προαναφερθέντων φυσικών προσώπων και του πιστωτικού ιδρύματος, στην έννοια της οποίας περιλαμβάνονται τα συστήματά του και τα εκάστοτε αποθηκευμένα σε αυτά δεδομένα, ανεξάρτητα εάν αυτές οι εγκληματικές πράξεις προέρχονται από το εσωτερικό της Τράπεζας ή από εξωγενείς παράγοντες. Η ως άνω επεξεργασία περιλαμβάνει την εγκατάσταση και λειτουργία
συστημάτων καταγραφής εικόνας στους χώρους συναλλαγών εντός των καταστημάτων του πιστωτικού ιδρύματος ή εκτός αυτών στις θέσεις των ATMs. Επίσης την εγκατάσταση και λειτουργία συστημάτων ηλεκτρονικού ελέγχου, τόσο της φυσικής πρόσβασης στους χώρους των υπηρεσιών του πιστωτικού ιδρύματος, με την καταγραφή της εισόδου και εξόδου των επισκεπτών και του προσωπικού τους, όσο και της ηλεκτρονικής πρόσβασης ή εκτέλεσης εργασιών με τη χρήση μηχανισμών ταυτοποίησης στα ηλεκτρονικά συστήματα και καταγραφής της ιστορικότητας ενεργειών (audit trails) για την παρακολούθηση και τη δημιουργία αναφορών σχετικά με δραστηριότητες στα ηλεκτρονικά συστήματα των πιστωτικών ιδρυμάτων. Εγκατάσταση και λειτουργία συστημάτων αξιολόγησης της ασφάλειας και εγκυρότητας των τραπεζικών συναλλαγών, τα οποία καταγράφουν ηλεκτρονικά και αξιολογούν τη λειτουργία και αποτελεσματικότητα των μηχανισμών πρόσβασης στα συστήματα του πιστωτικού ιδρύματος, ταυτοποίησης αυτών και καταγραφής της ιστορικότητας των ενεργειών.

Η εγκατάσταση και λειτουργία των συστημάτων αυτών, καθώς και ο χρόνος

τήρησης των σχετικών δεδομένων διέπεται από τις διατάξεις της εκάστοτε σχετικής ισχύουσας νομοθεσίας.

Όπου γίνεται καταγραφή εικόνας, τα πιστωτικά ιδρύματα τοποθετούν ευκρινώς τις κατά νόμο ενημερωτικές πινακίδες και όπου η πρόσβαση είναι ελεγχόμενη υπάρχει σχετική ενημέρωση το αργότερο κατά την παράδοση του μέσου (πχ. ηλεκτρονικού κλειδιού) που επιτρέπει την πρόσβαση.[129]

Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας.

Πρόκειται για μία ιδιαίτερη έννομη υποχρέωση των πιστωτικών ιδρυμάτων που πηγάζει από το νόμο (Ν.4557/2018, όπως εκάστοτε ισχύει) και τις σχετικές κανονιστικού χαρακτήρα διατάξεις της Τράπεζας της Ελλάδος, αλλά και διεθνών οργανισμών.

Προς τούτο τα πιστωτικά ιδρύματα χρησιμοποιούν συστήματα ταυτοποίησης των πελατών και των συναλλαγών που αυτοί πραγματοποιούν και επεξεργασίας αυτών, βάσει σχετικών μοντέλων, πραγματοποιούν ελέγχους σε διεθνείς καταλόγους πολιτικώς εκτεθειμένων προσώπων ή επιβολής κυρώσεων (πχ. περιοριστικά μέτρα, εμπάργκο) κλπ, με σκοπό τη διερεύνηση υπόπτων ή ασυνήθιστων συναλλαγών και την πρόληψη και καταστολή της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, αλλά και άλλων άδικων πράξεων, όπως πχ. της απάτης.[130]

Εξυπηρέτηση μετοχολογίου.

Τα πιστωτικά ιδρύματα τηρούν και επεξεργάζονται τα προσωπικά δεδομένα των υποκειμένων που έχουν εκάστοτε τη μετοχική ιδιότητα στο νομικό πρόσωπο του πιστωτικού ιδρύματος ή είναι ενεχυρούχοι δανειστές των μετόχων. Η επεξεργασία γίνεται για την εκπλήρωση νομικής υποχρέωσης, δεδομένου ότι οι μετοχές των πιστωτικών ιδρυμάτων είναι υποχρεωτικά ονομαστικές, αλλά και για την διευκόλυνση των μετόχων να ασκούν τα εκ του νόμου δικαιώματά τους και την ανταπόκρισή των πιστωτικών ιδρυμάτων στα σχετικά αιτήματα αυτών. [131]

Άσκηση αξιώσεων και υπεράσπισης εννόμων συμφερόντων.

Ιδιαίτερη μορφή επεξεργασίας προσωπικών δεδομένων αποτελεί αυτή που αποσκοπεί στην διασφάλιση των συμφερόντων του πιστωτικού ιδρύματος, την άσκηση των δικαιωμάτων του και την υπεράσπιση αυτών που πηγάζουν από συμβατικές σχέσεις ή/και προκύπτουν από διατάξεις νόμου. Για αυτούς τους σκοπούς το πιστωτικό ίδρυμα κάνει χρήση υπηρεσιών δικηγόρων, δικαστικών επιμελητών, συμβολαιογράφων και απευθύνεται σε αρμόδιους κατά περίπτωση φορείς, αρχές ή υπηρεσίες, προς τους οποίους ή/και οποίες διαβιβάζει τα προσωπικά δεδομένα των εκάστοτε εμπλεκομένων φυσικών

[129]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 4.4

[130]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 4.5

[131]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 4.6

προσώπων (αντιδίκων, ομόδικων, αντικλήτων, κλπ.).
Η νομική βάση για την εν λόγω επεξεργασία και διαβίβαση είναι ακριβώς η διασφάλιση των εννόμων συμφερόντων και η άσκηση των δικαιωμάτων του διαβιβάζοντος πιστωτικού ιδρύματος και η μόνη σχετική προϋπόθεση είναι η προηγούμενη σχετική ενημέρωση των πελατών / υποκειμένων, όχι για κάθε ένα συγκεκριμένο αποδέκτη, αλλά για τις κατά περίπτωση κατηγορίες αποδεκτών (π.χ. δικηγόροι / δικηγορικές εταιρίες, δικαστικοί επιμελητές κλπ.).
Τα ανωτέρω ισχύουν και για τη διαβίβαση προσωπικών δεδομένων πελατών σε εταιρίες ενημέρωσης οφειλετών[132]και εταιρίες διαχείρισης απαιτήσεων[133].

Εκχώρηση απαιτήσεων από χορηγήσεις.

Τα πιστωτικά ιδρύματα συχνά μεταβιβάζουν απαιτήσεις τους από συμβάσεις δανείων ή/και πιστώσεων σε τρίτους, σύμφωνα με τις εκάστοτε σχετικές περί εκχωρήσεως διατάξεις του Αστικού Κώδικα (άρθρο 455 επ.) και τις ειδικότερες διατάξεις του Ν. 3156/2003, για την τιτλοποίηση απαιτήσεων και του Ν. 4354/2015 για τις εταιρείες διαχείρισης απαιτήσεων και τη μεταβίβαση αυτών, όπως εκάστοτε ισχύουν.
Για την ολοκλήρωση αυτών των συμβάσεων είναι απαραίτητη η διαβίβαση των προσωπικών δεδομένων των πελατών-οφειλετών τους στους αποκτώντες τις απαιτήσεις ή και σε αυτούς που αναλαμβάνουν τη διαχείρισή τους. Νομική βάση της συγκεκριμένης επεξεργασίας του πιστωτικού ιδρύματος είναι η ανάγκη εκτέλεσης και υλοποίησης της σύμβασης μεταβίβασης και διαχείρισης ενώ προϋπόθεσή της είναι η σχετική ενημέρωση των οφειλετών-υποκειμένων για την κατηγορία των αποδεκτών, εκτός εάν ειδικότεροι νόμοι θέτουν και άλλες προϋποθέσεις.[134]

Γνωστοποίηση και διαβίβαση στις αρμόδιες Εποπτικές, Ανεξάρτητες, Αστυνομικές, Δικαστικές και εν γένει Δημόσιες Αρχές, καθώς και τρίτα νομίμως αδειοδοτημένα νομικά πρόσωπα, όπου απαιτείται σύμφωνα με την ισχύουσα νομοθεσία.

Τα πιστωτικά ιδρύματα σε πολλές περιπτώσεις καλούνται να διαβιβάσουν προσωπικά δεδομένα πελατών τους ή και εργαζόμενων σε αυτά από φορολογικές, εισαγγελικές ανακριτικές ή δικαστικές αρχές στο πλαίσιο είτε προσδιορισμού της φορολογητέας ύλης (όπως πχ. στην περίπτωση της γνωστοποίησης των τόκων των καταθέσεων), διερεύνησης παράνομων πράξεων (όπως φοροδιαφυγή, απάτη), είτε διεθνών υποχρεώσεων της χώρας (όπως πχ. στην περίπτωση της FATCA[135]).
Στις περιπτώσεις αυτές η διαβίβαση αποτελεί υποχρέωση εκ του νόμου, για

[132]Ν. 3758/2009
[133]Ν. 4354/2015, Ν. 4469/2017
[134]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 4.8
[135] Foreign Account Tax Compliance Act (FATCA) είναι οι Κανόνες για την Φορολογική Συμμόρφωση που σχεδιάστηκαν από τις φορολογικές αρχές των ΗΠΑ (InternalRevenueService "IRS"), με σκοπό την πρόληψη και πάταξη της φοροδιαφυγής των Αμερικανών προσώπων που διατηρούν λογαριασμούς σε χρηματοπιστωτικά ιδρύματα εκτός ΗΠΑ.

την εκπλήρωση της οποίας δεν απαιτείται συγκατάθεση των υποκειμένων των διαβιβαζόμενων δεδομένων και κατά κανόνα ούτε ειδική ενημέρωση αυτών. Επίσης κατά την εφαρμογή της ισχύουσας νομοθεσίας για τις κρατικές ενισχύσεις και της φορολογικής νομοθεσίας, συμπεριλαμβανομένων των διατάξεων που αφορούν την αυτόματη ανταλλαγή πληροφοριών στον φορολογικό τομέα.
Πέραν αυτών πρόσβαση σε προσωπικά δεδομένα μπορεί να έχει η Τράπεζα της Ελλάδος, η Ευρωπαϊκή Κεντρική Τράπεζα, ο Ενιαίος Εποπτικός Μηχανισμός (SSM) ή η Επιτροπή Κεφαλαιαγοράς στο πλαίσιο των εποπτικών τους αρμοδιοτήτων. Και στις περιπτώσεις αυτές δεν απαιτείται συγκατάθεση των υποκειμένων των διαβιβαζόμενων δεδομένων, ούτε σχετική ενημέρωση.

Τήρηση ιστορικού αρχείου

Τα πιστωτικά ιδρύματα τηρούν προσωπικά δεδομένα μετόχων, μελών του Διοικητικού Συμβουλίου ή/και της διοίκησής τους, όπως και πελατών τους που επηρέασαν την πορεία του πιστωτικού ιδρύματος και την οικονομία της χώρας, τόσο για ιστορικούς λόγους, όσο και για λόγους έρευνας. Τέτοια προσωπικά δεδομένα μπορεί να είναι στοιχεία ταυτοπροσωπίας, βιογραφικά σημειώματα, φωτογραφικό υλικό.

2.1.4 Χρονικό διάστημα τήρησης των προσωπικών δεδομένων

Η Τράπεζα δύναται να επεξεργάζεται τα προσωπικά δεδομένα των πελατών της καθ' όλη την διάρκεια που υφίσταται σύμβαση σε ισχύ. Το χρονικό διάστημα τήρησης, εξαρτάται από τον σκοπό της επεξεργασίας, για τον οποίο έχουν υποβληθεί τα στοιχεία και οφείλει να είναι το ελάχιστο δυνατό. Με τη λήξη του απαραίτητου διαστήματος, τα δεδομένα τηρούνται για τον προβλεπόμενο χρόνο που ορίζει το ισχύον θεσμικό πλαίσιο ή για όσο χρόνο απαιτείται για την προάσπιση δικαιωμάτων της τράπεζας ενώπιον δικαστηρίου και άλλης αρμόδιας αρχής. Έπειτα από τη λήξη της σύμβασης ή και της επιχειρηματικής σχέσης η Τράπεζα δύναται να επεξεργάζεται τα δεδομένα για όσο χρονικό διάστημα ορίζεται από το εκάστοτε νομικό ή κανονιστικό πλαίσιο.
Θα πρέπει, επίσης, να γίνει μέριμνα σχετικά με τον τρόπο καταστροφής των προσωπικών δεδομένων, όταν παρέλθει το απαιτούμενο χρονικό διάστημα. Κατόπιν μελέτης πιθανής ανάγκης διατήρησης των προσωπικών δεδομένων, πάντα στα πλαίσια συμμόρφωσης με νομικές και κανονιστικές απαιτήσεις, θα πρέπει να θεσμοθετηθεί αυστηρή διαδικασία, που θα πρέπει να ακολουθείται κατά περίπτωση.
Επιπροσθέτως, θα πρέπει να υπάρξει πρόβλεψη για τα τρίτα μέρη που παρέχουν υπηρεσίες στο όνομα και για λογαριασμό της Τράπεζας, ώστε να δεσμεύονται από τις ρήτρες της διαδικασίας, που θα θεσμοθετηθεί.

Ειδικότερα και ενδεικτικά, όπως παρατίθενται στο από 16.1.2019 Σχέδιο του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο

τραπεζικό σύστημα, που κατέθεσε προς έγκριση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα η Ελληνική Ένωση Τραπεζών[136] :

α) Τα προσωπικά δεδομένα που αφορούν στην κατάρτιση και τη λειτουργία σύμβασης, περιλαμβανομένων των υποστηρικτικών εγγράφων αυτής, όπως και αυτών που παρήχθηκαν κατά τη διάρκεια της ισχύος της (όπως πχ. πρόσθετες πράξεις, επιστολές για την ερμηνεία όρων της, ενημερώσεις για το κατάλοιπο κλπ), με πιστωτικό ίδρυμα ή εγχρήματη συναλλαγή σε αυτό διατηρούνται τουλάχιστον καθ' όλη τη διάρκεια της σχέσης του πιστωτικού ιδρύματος με τον πελάτη, μέχρι την ολοσχερή εξόφληση κάθε σχετικής οφειλής/απαίτησης και τη συμπλήρωση του κατά νόμο χρόνου παραγραφής κάθε τυχόν αξίωσης.

β) Δεδομένα που αφορούν την διαπίστωση της φερεγγυότητας και πιστοληπτικής ικανότητας των πελατών, την αλληλογραφία των πιστωτικών ιδρυμάτων με τους πελάτες τους, καθώς επίσης και οι καταγραφόμενες τηλεφωνικές συνομιλίες με πελάτες μέσω της υπηρεσίας τηλεφωνικής εξυπηρέτησης πελατών κάθε πιστωτικού ιδρύματος, τηρούνται για χρονικό διάστημα τουλάχιστον πέντε ετών από την λήξη της επιχειρηματικής σχέσης του πιστωτικού ιδρύματος με τον πελάτη ή την εκτέλεση κάθε συναλλαγής.

γ) Δεδομένα που αφορούν τηλεφωνικές συνομιλίες με αντικείμενο συναλλαγές επί χρηματοπιστωτικών μέσων, διατηρούνται για χρονικό διάστημα τουλάχιστον πέντε ετών ή για πρόσθετη περίοδο δύο ετών μετά από απόφαση της Επιτροπής Κεφαλαιαγοράς όταν διενεργεί έρευνα για κατάχρηση της αγοράς.[137]

δ) Εικόνες από συστήματα βιντεοεπιτήρησης στους χώρους των συναλλαγών ή στις εισόδους των υπηρεσιών των πιστωτικών ιδρυμάτων, διατηρούνται για χρονικό διάστημα όχι μεγαλύτερο των σαράντα πέντε ημερών από την λήψη. Αν κατά το χρονικό αυτό διάστημα καταγραφούν περιστατικά απάτης ή αμφισβήτησης οικονομικής συναλλαγής, τα σχετικά τμήματα των δεδομένων του συστήματος βιντεοεπιτήρησης δύναται να διατηρηθούν σε ξεχωριστό αρχείο με ανάλογα μέτρα ασφαλείας, για όσο διάστημα απαιτείται για τη διερεύνηση και την πειθαρχική ή δικαστική δίωξη των περιστατικών αυτών.[138]

ε) Οι τηλεφωνικές επικοινωνίες με πελάτες στο πλαίσιο των διατάξεων του Ν. 3758/2009 διατηρούνται υποχρεωτικά για ένα έτος από την πραγματοποίηση της επικοινωνίας. Μετά την πάροδο του έτους η καταγραφή καταστρέφεται, εκτός εάν τη διατήρησή της αιτηθεί ο πελάτης ή μετά από καταγγελία αυτού, η Γενική Γραμματεία Καταναλωτή. [139]

στ) Αρχεία με δεδομένα υποκειμένων που δημιουργούνται από την εφαρμογή του Κώδικα Δεοντολογίας του Ν. 4224 /2013 στο πλαίσιο της διαδικασίας

[136] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.
[137] Άρθρο 43 του ν. 4443/2016
[138] Άρθρο 16 της υπ' αριθ. 1/2011 Οδηγία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
[139] Άρθρο 8 παρ. 2 Ν. 3758/2009

επίλυσης καθυστερήσεων, διατηρούνται για ελάχιστη περίοδο έξι ετών από την ημερομηνία που κάθε στοιχείο περιήλθε στην κατοχή του πιστωτικού ιδρύματος και για όλα τα στοιχεία κάθε δανειολήπτη πελάτη για τουλάχιστον έξι 6 έτη μετά την λήξη της συνεργασίας του με αυτόν. Στο αρχείο αυτό περιλαμβάνονται τα δικαιολογητικά που τεκμηριώνουν την επιδίωξη λύσης με την διαδικασία επίλυσης καθυστερήσεων του Κώδικα ή τους λόγους που εμπόδισαν την επιδίωξη λύσης με την διαδικασία αυτή[140]

ζ) Δεδομένα που αφορούν σε επικοινωνίες με υποκείμενα για την λήψη συγκατάθεσης για επεξεργασία με σκοπό την προώθηση προϊόντων ή υπηρεσιών τηρούνται μέχρι την ανάκλησή της και τα δεδομένα αυτής τηρούνται μέχρι την επαναχορήγηση συγκατάθεσης.

η) Δεδομένα που αφορούν σε επικοινωνίες προς υποκείμενα για σκοπούς προώθησης, διατηρούνται για ένα έτος από τη διενέργεια της τελευταίας επικοινωνίας μαζί τους.

θ) Με την επιφύλαξη τυχόν ειδικότερης νομοθεσίας, τα αρχεία προσωπικών δεδομένων υποκειμένων που δημιουργούνται για την εξυπηρέτηση των πάσης φύσεως συμβάσεων των πιστωτικών ιδρυμάτων με συνεργάτες ή προμηθευτές προϊόντων ή υπηρεσιών, διατηρούνται τουλάχιστον καθ' όλη τη διάρκεια της συμβατικής σχέσης, την ολοσχερή εξόφληση κάθε εντεύθεν οφειλής/απαίτησης και τη συμπλήρωση του χρόνου παραγραφής κάθε αξίωσης που απορρέει από την σύμβαση.

ι) Με την επιφύλαξη τυχόν ειδικότερης νομοθεσίας, δεδομένα πελατών που έχουν υποβάλλει αίτηση δανειοδότησης ή παροχής εγγυοδοσίας υπέρ πελάτη, και το αίτημα δεν ικανοποιήθηκε, διατηρούνται για πέντε χρόνια από την απόρριψή του δηλαδή όσο διαρκεί η 5ετής παραγραφή των αξιώσεων κατά το προσυμβατικό στάδιο, για την προάσπιση των έννομων συμφερόντων του πιστωτικού ιδρύματος που συνίσταται :

(i) στην απόδειξη τήρησης της νομιμότητας για την άντληση δεδομένων οικονομικής συμπεριφοράς του αιτούντος από διατραπεζικά αρχεία πληροφοριών,

(ii) στην αξιολόγηση της πιστοληπτικής ικανότητας του υποψηφίου δανειολήπτη σε περίπτωση που αυτός επανέλθει με νέο αίτημα εντός του ως άνω χρονικού διαστήματος τήρησης και

(iii) στην προάσπιση των συμφερόντων της Τράπεζας, σε περίπτωση προβολής αντιρρήσεων ή ενστάσεων του υποψηφίου πελάτη για την απόρριψη του αιτήματός του ή τη διαδικασία εξέτασης του αιτήματός του.

Με την επιφύλαξη της ΕΤΠΘ 281/2009, τα παραπάνω δεν ισχύουν για τα δικαιολογητικά που έχει προσκομίσει ο πελάτης, τα οποία πρέπει να καταστρέφονται ή να επιστρέφονται σε αυτόν μετά την απόρριψη.

ια) Τα δεδομένα που αφορούν στο μετοχολόγιο πιστωτικού ιδρύματος, όπως και τα ιστορικά αρχεία αυτού τηρούνται χωρίς χρονικό περιορισμό.

[140]Κεφάλαιο 7ο της υπ' αριθ. 195/2016 Απόφασης της Επιτροπής Πιστωτικών και Ασφαλιστικών Θεμάτων της Τράπεζας της Ελλάδος.

2.1.5 Νόμιμοι λόγοι επεξεργασίας δεδομένων.

Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνεται, προς τις αρχές που σχετίζονται με την ποιότητα των δεδομένων και προβλέπονται στο άρθρο 5 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016. Σύμφωνα με μία από τις αρχές αυτές, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να «υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο». Προκειμένου να είναι η επεξεργασία σύννομη, θα πρέπει να βασίζεται σε έναν από τους νόμιμους λόγους που καθιστούν θεμιτή την επεξεργασία δεδομένων, οι οποίοι απαριθμούνται στο άρθρο 6 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 για τα μη ευαίσθητα δεδομένα προσωπικού χαρακτήρα και στο άρθρο 9 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 για τις ειδικές κατηγορίες δεδομένων (ευαίσθητα δεδομένα).[141]

Συγκατάθεση

Πριν από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ενημερώνεται δεόντως το υποκείμενο της επεξεργασίας και παρέχει, όπου απαιτείται, τη συγκατάθεσή του αυτοβούλως και ενεργά (ελεύθερη, ρητή, ειδική και σαφής, η οποία να έχει δοθεί κατόπιν ενημέρωσής του και με πλήρη επίγνωση). Η συγκατάθεσή μπορεί να ανακληθεί ανά πάσα στιγμή, χωρίς βέβαια να θίγεται η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της.

Η συγκατάθεση[142] του υποκείμενου ή η άρνηση αυτής, όπου απαιτείται, παρέχεται ελεύθερα με προσιτό τρόπο, με θετική ενέργεια (όχι δια παραλείψεως), είναι ειδική και παρέχεται μετά από ειδική και κατανοητή ενημέρωσης από το πιστωτικό ίδρυμα. Ελεύθερη συγκατάθεση υπάρχει μόνο εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είναι σε θέση να έχει πραγματική επιλογή και δεν υπάρχει κίνδυνος εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων εάν δεν δώσει τη συγκατάθεσή του.[143] Το δίκαιο της ΕΕ προβλέπει ότι η συγκατάθεση δεν θεωρείται ότι δόθηκε ελεύθερα αν το υποκείμενο των δεδομένων δεν έχει αληθινή ή ελεύθερη επιλογή ή δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί.[144]

Στην εν πλήρει επιγνώσει συγκατάθεση θα παρέχεται συνήθως ακριβής και ευνόητη περιγραφή του θέματος για το οποίο ζητείται συγκατάθεση. Το υποκείμενο των δεδομένων πρέπει να διαθέτει επαρκείς πληροφορίες προτού προβεί στην επιλογή του. Η συγκατάθεση πρέπει να βασίζεται σε εκτίμηση και κατανόηση των πραγματικών περιστατικών και των συνεπειών

[141] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.180

[142] Άρθρο 6 παράγραφος 1 στοιχείο α' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[143] Ομάδα εργασίας του άρθρου 29 (2011), Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, WP 187, 13 Ιουλίου 2011, σ. 12.

[144] Αιτιολογική σκέψη 42του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

της πράξης του υποκειμένου των δεδομένων με την οποία συγκατατίθεται στην επεξεργασία. Το ενδιαφερόμενο άτομο πρέπει να λάβει, με σαφή και κατανοητό τρόπο, κατάλληλη και πλήρη ενημέρωση για όλα τα σχετικά θέματα, όπως οι κατηγορίες των σχετικών δεδομένων, οι σκοποί της επεξεργασίας, οι αποδέκτες ή κατηγορίες αποδεκτών των δεδομένων και τα δικαιώματα του προσώπου στο οποίο αναφέρονται τα δεδομένα.[145] Επίσης, εν πλήρει επιγνώσει συγκατάθεση σημαίνει ότι το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει τουλάχιστον την ταυτότητα του υπευθύνου επεξεργασίας και τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα προσωπικού χαρακτήρα, τα οποία υποβάλλονται σε επεξεργασία.[146] Η ποιότητα των πληροφοριών είναι σημαντική. Ποιότητα των πληροφοριών σημαίνει ότι η γλώσσα των πληροφοριών θα πρέπει να είναι προσαρμοσμένη στους προβλεπόμενους αποδέκτες. Οι πληροφορίες πρέπει να παρέχονται χωρίς τη χρήση ιδιωμάτων, με σαφή και απλή διατύπωση, την οποία ο μέσος χρήστης θα πρέπει να είναι σε θέση να κατανοήσει.[147] Οι πληροφορίες πρέπει επίσης να είναι εύκολα διαθέσιμες στο υποκείμενο των δεδομένων και μπορούν να παρέχονται προφορικά ή γραπτά. Η προσβασιμότητα και η προβολή των πληροφοριών είναι σημαντικά στοιχεία: οι πληροφορίες πρέπει να είναι σαφώς ορατές και εμφανείς. Σε διαδικτυακό περιβάλλον, τα ενημερωτικά σημειώματα πολλαπλών επιπέδων μπορούν να αποτελέσουν μια καλή λύση, καθώς παρέχουν τη δυνατότητα στα υποκείμενα των δεδομένων να επιλέξουν αν θέλουν να έχουν πρόσβαση σε συνοπτική ή εκτενέστερη εκδοχή των πληροφοριών.[148]

Η συγκατάθεση καλύπτει το σύνολο των διαδικασιών επεξεργασίας, που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς. Όταν η επεξεργασία έχει πολλαπλούς ξεχωριστούς σκοπούς, δίνεται ξεχωριστή ενημέρωση και αντίστοιχη συγκατάθεση για κάθε ένα σκοπό, όπου αυτή απαιτείται. Προκειμένου να είναι η συγκατάθεση συγκεκριμένη και έγκυρη, πρέπει επίσης να αφορά συγκεκριμένα τον σκοπό της επεξεργασίας, ο οποίος πρέπει να περιγράφεται σαφώς και με αδιαμφισβήτητο τρόπο. Αυτό συμβαδίζει με την ποιότητα των πληροφοριών που παρέχονται σχετικά με τον σκοπό της συγκατάθεσης. Στο πλαίσιο αυτό, σημασία θα έχουν οι εύλογες προσδοκίες του μέσου υποκειμένου των δεδομένων. Η συγκατάθεση του υποκειμένου των δεδομένων πρέπει να ζητηθεί εκ νέου εάν πρόκειται να προστεθούν ή να τροποποιηθούν πράξεις επεξεργασίας, κατά τρόπο που δεν

[145]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.186
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
[146] Αιτιολογική σκέψη 42του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[147] Ομάδα εργασίας του άρθρου 29 (2011), Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, WP 187, 13 Ιουλίου 2011, σ. 19.
[148]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.187
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

θα μπορούσε να είχε προβλεφθεί εύλογα όταν είχε παρασχεθεί η αρχική συγκατάθεση, οι οποίες έχουν επομένως ως αποτέλεσμα να μεταβάλλεται ο σκοπός της συγκατάθεσης. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς.[149]

Κάθε συγκατάθεση πρέπει να παρέχεται με αδιαμφισβήτητο τρόπο.[150] Αυτό σημαίνει ότι δεν θα πρέπει να υφίσταται εύλογη αμφιβολία για τη βούληση του υποκειμένου των δεδομένων να δηλώσει τη συμφωνία του στην επεξεργασίατων δεδομένων που το αφορούν. Για παράδειγμα, η αδράνεια του υποκειμένου των δεδομένων δεν υποδηλώνει αδιαμφισβήτητη συγκατάθεση. Εάν η συγκατάθεση παρέχεται εγγράφως στο πλαίσιο σύμβασης, η συγκατάθεση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να εξατομικεύεται και, εν πάση περιπτώσει, θα πρέπει να παρέχονται εγγυήσεις που να διασφαλίζουν ότι το υποκείμενο των δεδομένων γνωρίζει αυτό το γεγονός και σε ποιο βαθμό έχει συγκατατεθεί[151].

Η συγκατάθεση μπορεί να παρασχεθεί με οποιοδήποτε κατά τις περιστάσεις πρόσφορο τρόπο, όπως με έγγραφο, μαγνητοφωνημένη τηλεφωνική επικοινωνία ή με ηλεκτρονικό ή άλλο μέσο που επιτρέπει την ταυτοποίηση του υποκειμένου και την απόδειξη της εκδήλωσης της βούλησής του.

Η συγκατάθεση μπορεί σε ειδικές περιπτώσεις να εμπεριέχεται σε θετική ενέργεια του υποκειμένου, όπως όταν αυτό υποβάλει στο πιστωτικό ίδρυμα αίτημα στο οποίο εμπεριέχονται προσωπικά του δεδομένα, η επεξεργασία των οποίων είναι απαραίτητη για την ικανοποίηση αιτήματος, ακόμη και εάν πρόκειται για ειδικά προσωπικά δεδομένα και υπό την προϋπόθεση ότι το αίτημά του εδράζεται σε αυτά και τα επικαλείται, όπως πχ στην περίπτωση υποβολής δεδομένων υγείας για την πραγματοποίηση εμβάσματος στο εξωτερικό ή την ευνοϊκή ρύθμιση οφειλής.[152]

Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει την παρασχεθείσα συγκατάθεσή του ανά πάσα στιγμή. Ο Γενικός Κανονισμός Προστασίας Δεδομένων προβλέπει γενικό δικαίωμα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή.[153] Το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για το δικαίωμα αυτό προτού δώσει τη συγκατάθεσή του και μπορεί να ασκήσει το δικαίωμα αυτό κατά τη διακριτική του ευχέρεια. Δεν θα πρέπει να προβλέπεται απαίτηση αιτιολόγησης της ανάκλησης, και δεν θα πρέπει να υφίσταται κίνδυνος αρνητικών συνεπειών πέραν της παύσης τυχόν οφελών που ενδέχεται να απορρέουν από την προηγουμένως συμφωνηθείσα

---

[149]Αιτιολογική σκέψη 32του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[150] Άρθρο 4 περ.11του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[151]Αιτιολογική σκέψη 42του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[152]Από 18-07-2015 Πράξη Νομοθετικού Περιεχομένου (ΦΕΚ Α' 84), όπως κυρώθηκε με τον ν. 4350/2015 (ΦΕΚ Α' 161/30-11-2015). Καθώς και αρ. πρωτ. ΓΝ/ΕΞ/1862/29.6.17, 1856/29.6.17, 1864/29.6.17, 1860/29.6.17, 1858/29.6.17, 1854/29.6.17 και 2915/5.10.17 έγγραφα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

[153]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.191
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

χρήση των δεδομένων. Η ανάκληση της συγκατάθεσης θα πρέπει να είναι εξίσου εύκολη με την παροχή της.[154] Η ανάκληση της συγκατάθεσης πρέπει επίσης να γίνει με τρόπο που επιτρέπει την ταυτοποίηση του υποκειμένου και την απόδειξη της εκδήλωσης της σχετικής βούλησής του και δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Επαναχορήγηση ανακληθείσας συγκατάθεσης είναι πάντα επιτρεπτή. [155]

Δεν απαιτείται συναίνεση στις παρακάτω περιπτώσεις:

α) για την εκτέλεση σύμβασης που έχει συνάψει πελάτης με την Τράπεζα,

β) προκειμένου να ληφθούν μέτρα σχετικά με αίτημά πελάτη πριν από τη σύναψη σύμβασης,

γ) για τη συμμόρφωση της Τράπεζας ως Υπεύθυνου Επεξεργασίας δεδομένων προσωπικού χαρακτήρα με τις νομικές υποχρεώσεις,

δ) για την προστασία ζωτικών συμφερόντων του πελάτη,

ε) για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας,

στ) Όταν η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει η Τράπεζα, εκτός εάν το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου υπερισχύουν των εν λόγω συμφερόντων.

Σε περίπτωση που δεν έχει ληφθεί συγκατάθεση, να είναι απολύτως αναγκαία για τον επιδιωκόμενο σκοπό και να εξυπηρετεί έννομο συμφέρον του αποδέκτη/ ή του υπεύθυνου επεξεργασίας προφανώς υπέρτερο σε σχέση με το έννομο συμφέρον του πελάτη.[156]

Τα πιστωτικά ιδρύματα θα πρέπει να τηρούν αρχεία των συγκαταθέσεων που συλλέγουν, συμπεριλαμβανομένων των σκοπών της επεξεργασίας που αυτές καλύπτουν, του τρόπου, του χρόνου παροχής τους και τυχόν ανάκλησης αυτών, όπως και των επαναχορηγήσεών τους, για σκοπούς ελέγχου και τεκμηρίωσης.[157]

Αναγκαιότητα για την εκτέλεση σύμβασης.

Στο άρθρο 6 παρ. 1 στοιχ.β' του Γενικού Κανονισμού Προστασίας Δεδομένων προβλέπεται ακόμη μία βάση σύννομης επεξεργασίας, η περίπτωση όπου αυτή είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος. Η διάταξη αυτή καλύπτει και τις προσυμβατικές σχέσεις. Για παράδειγμα, σε περιπτώσεις στις οποίες ένα μέρος προτίθεται να συνάψει σύμβαση, αλλά δεν το έχει πράξει ακόμη, ενδεχομένως επειδή χρειάζεται να διενεργηθούν ορισμένοι ακόμη έλεγχοι. Εάν ένα μέρος χρειάζεται να επεξεργαστεί δεδομένα για τον σκοπό αυτό, η επεξεργασία αυτή είναι σύννομη εφόσον είναι απαραίτητη για να ληφθούν

[154]Άρθρο 7, παρ.3 του Γενικού Κανονισμού Προστασίας ΔεδομένωνΕ.Ε. 679/2016

[155]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 5.

[156]Άρθρο 5 παρ.2 ε' του ν. 2471/1997

[157]Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, Άρθρο 5.5

μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης.[158].

Έννομες υποχρεώσεις του υπευθύνου επεξεργασίας.

Άλλη μία περίπτωση σύννομης επεξεργασίας είναι αυτή που είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 6 παρ. 1 στοιχ. γ' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016. Η διάταξη αυτή αφορά υπευθύνους επεξεργασίας που δραστηριοποιούνται τόσο στον ιδιωτικό, όσο και στον δημόσιο τομέα· οι έννομες υποχρεώσεις υπευθύνων επεξεργασίας δεδομένων στον δημόσιο τομέα μπορούν επίσης να εμπίπτουν στο πεδίο εφαρμογής του άρθρου 6 παρ. 1 στοιχ. ε' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016. Υπάρχουν πολλά παραδείγματα περιπτώσεων στις οποίες ο νόμος υποχρεώνει τους υπευθύνους επεξεργασίας του ιδιωτικού τομέα να επεξεργάζονται δεδομένα σχετικά με συγκεκριμένα υποκείμενα δεδομένων. Για παράδειγμα, οι εργοδότες πρέπει να επεξεργάζονται δεδομένα των υπαλλήλων τους για λόγους κοινωνικής ασφάλισης και για φορολογικούς σκοπούς, και οι επιχειρήσεις πρέπει να επεξεργάζονται δεδομένα των πελατών τους για φορολογικούς σκοπούς. Η έννομη υποχρέωση μπορεί να προκύπτει από το δίκαιο της Ένωσης ή κράτους μέλους, το οποίο θα μπορούσε να αποτελεί τη βάση για μία ή περισσότερες πράξεις επεξεργασίας.[159]

Ζωτικά συμφέροντα του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη εάν είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.[160] Ο νόμιμος αυτός λόγος μπορεί να προβληθεί για την επεξεργασία δεδομένων προσωπικού χαρακτήρα βάσει των ζωτικών συμφερόντων άλλου φυσικού προσώπου μόνο εάν είναι πρόδηλο ότι η επεξεργασία δεν μπορεί να έχει άλλη νομική βάση.[161] Ενίοτε ένα είδος επε¬ξεργασίας ενδέχεται να βασίζεται σε λόγους τόσο δημόσιου συμφέροντος, όσο και ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου προσώπου. Αυτό συμβαίνει, για παράδειγμα, όταν παρακολουθούνται επιδημίες και η εξέλιξή τους ή όταν υπάρχει επείγουσα ανθρωπιστική ανάγκη.[162]

Δημόσιο συμφέρον και άσκηση δημόσιας εξουσίας.

---

[158]Άρθρο 6 παρ. 1 στοιχ. β' Άρθρο του Γενικού Κανονισμού Προστασίας ΔεδομένωνΕ.Ε. 679/2016

[159]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.190
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

[160] Άρθρο 6 παρ.1 στοιχ. δ' Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[161] Αιτιολογική σκέψη 46. Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[162] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.192
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

Τα δεδομένα προσωπικού χαρακτήρα μπορούν να υποβάλλονται νομίμως σε επεξεργασία εάν αυτή είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.[163]

Έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να είναι σύννομη εάν «είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρα¬κτήρα.[164]

Η ύπαρξη έννομου συμφέροντος πρέπει να αξιολογείται προσεκτικά σε κάθε συγκεκριμένη περίπτωση. Εάν προσδιοριστούν τα έννομα συμφέροντα του υπευθύνου επεξεργασίας, αυτά πρέπει στη συνέχεια να σταθμιστούν με τα συμ¬φέροντα ή τα θεμελιώδη δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων.[165] Οι εύλογες προσδοκίες του υποκειμένου των δεδομένων πρέπει να λαμβάνονται υπόψη στο πλαίσιο μιας τέτοιας αξιολόγησης για τη διαπίστωση του αν τα συμφέροντα του υπευθύνου επεξεργασίας υπερισχύουν των συμφε¬ρόντων ή των θεμελιωδών δικαιωμάτων του υποκειμένου των δεδομένων. Εάν τα δικαιώματα του υποκειμένου των δεδομένων υπερισχύουν των έννομων συμφερόντων του υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας μπορεί να λάβει μέτρα και να εφαρμόσει εγγυήσεις ώστε να διασφαλίσει την ελαχιστο¬ποίηση του αντίκτυπου στα δικαιώματα του υποκειμένου των δεδομένων (όπως ψευδωνυμοποίηση των δεδομένων) και να αντιστρέψει την «ισορροπία» για να μπορέσει να επικαλεστεί νομίμως την έγκυρη αυτή βάση για την επεξεργασία.[166]

2.2 Δικαιώματα των υποκειμένων των δεδομένων.

Κάθε πολίτης έχει καταρχήν το δικαίωμα να γνωρίζει εάν τα προσωπικά του δεδομένα έχουν καταχωριστεί σε αρχείο, καθώς και να λαμβάνει αντίγραφα των σχετικών εγγράφων, απευθυνόμενος προς την τράπεζα σχετικά με την εκτέλεση της τραπεζικής του σύμβασης ή της αίτησης δανείου ή τη βαθμολόγηση της πιστοληπτικής του ικανότητας. Έχει ακόμα το δικαίωμα να προβάλλει δικαιολογημένες αντιρρήσεις, εφόσον δεν υπάρχει σχετική υποχρέωση του υπευθύνου επεξεργασίας, από νόμο ή τη σύμβαση, για την

[163] Αιτιολογική σκέψη 45. Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[164] Άρθρο 6 παρ.1 στοιχ. στ' Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[165] Ομάδα εργασίας του άρθρου 29 (2014), Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ, WP 217, 4 Απριλίου 2014.
[166] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.195
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

επεξεργασία αυτή, καθώς επίσης να ζητεί τη διόρθωση αυτών.[167]

Ως υποκείμενα δεδομένων προσωπικού χαρακτήρα νοούνται τα φυσικά πρόσωπα που διενεργούν οποιαδήποτε συναλλαγή με Τράπεζα, όπως ενδεικτικά οι πελάτες που διατηρούν μόνιμη σχέση συνεργασίας με κάποια Τράπεζα, οι διερχόμενοι πελάτες , οι νόμιμοι εκπρόσωποι πελατών (πληρεξούσιοι, εκπρόσωποι, αντιπρόσωποι), οι ειδικοί ή καθολικοί διάδοχοί τους, οι εκπρόσωποι νομικών προσώπων και κάθε φυσικό πρόσωπο που υπό οποιαδήποτε ιδιότητα έχει συναλλακτικές σχέσεις με το εκάστοτε τραπεζικό ίδρυμα. Υποκείμενα δεδομένων προσωπικού χαρακτήρα μπορούν να είναι τόσο οι ενεργοί, όσο και οι υποψήφιοι και οι πρώην πελάτες μίας τράπεζας. Επίσης, τα φυσικά πρόσωπα που έχουν παράσχει εγγύηση ή ασφάλεια υπέρ των ανωτέρω αναφερόμενων προσώπων, προμηθευτές και συνεργάτες της τράπεζας, ομολογιούχοι δανειστές, πραγματικοί δικαιούχοι οντοτήτων, τρίτα πρόσωπα που σχετίζονται με πελάτες της τράπεζας υπό την ιδιότητα του συνεργάτη, μετόχου, αντισυμβαλλόμενου, δικηγόρου ή αντικλήτου. Η ενημέρωση των υποκειμένων των δεδομένων (πελατών της τράπεζας εν ευρεία έννοια) σχετικά με τα δικαιώματά τους, όσον αφορά την προστασία προσωπικών δεδομένων, είναι υψίστης σημασίας.

Δικαίωμα ενημέρωσης.

Οι υπεύθυνοι πράξεων επεξεργασίας υποχρεούνται να ενημερώνουν το υποκείμενο των δεδομένων κατά τη συλλογή των δεδομένων προσωπικού χαρακτήρα που το αφορούν σχετικά με τη σκοπούμενη επεξεργασία τους. Η υποχρέωση αυτή δεν εξαρτάται από αίτημα του υποκειμένου των δεδομένων, αλλά αντιθέτως ο υπεύ¬θυνος επεξεργασίας πρέπει να συμμορφώνεται προς αυτήν προδραστικά, ανε¬ξάρτητα από το αν το υποκείμενο των δεδομένων θα εκφράσει ενδιαφέρον για την ενημέρωση.

Τα συμβαλλόμενα μέρη πρέπει να προβλέ¬πουν ότι οι υπεύθυνοι επεξεργασίας θα ενημερώνουν τα υποκείμενα των δεδο¬μένων σχετικά με την ταυτότητα και τη συνήθη διαμονή τους, τη νομική βάση και τον σκοπό της επεξεργασίας, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, τους αποδέκτες των δεδομένων προσωπικού χαρακτήρα που τα αφορούν και τον τρόπο με τον οποίο μπο¬ρούν να ασκήσουν τα προβλεπόμενα δικαιώματά τους, στα οποία περιλαμβάνονται τα δικαιώματα πρόσβασης, διόρθωσης και προσφυγής. Κάθε άλλη πρόσθετη πληροφορία η οποία θεωρείται αναγκαία για τη διασφάλιση αντικειμενικής και διαφανούς επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει επίσης να γνωστοποιείται στα υποκείμενα των δεδομένων. Οι πλη¬ροφορίες που παρουσιάζονται στα υποκείμενα των δεδομένων θα πρέπει να είναι προσβάσιμες, ευανάγνωστες, κατανοητές και προσαρμοσμένες στα οικεία

[167]https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/xrimatopistotika/pistwtika_xrhmatodotika

υποκείμενα των δεδομένων.[168]
Ο πελάτης έχει το δικαίωμα να ενημερώνεται με σαφή και κατανοητό τρόπο, σε εύκολα προσβάσιμο αρχείο, για την επεξεργασία στην οποία υποβάλλονται τα προσωπικά του δεδομένα, για ποιο σκοπό και για ποιο διάστημα διατηρούνται. Η ενημέρωση των υποκειμένων-πελατών των πιστωτικών ιδρυμάτων είναι μια καταρχάς ανεξαίρετη υποχρέωση των υπευθύνων επεξεργασίας-πιστωτικών ιδρυμάτων, που μπορεί να περιορισθεί μόνο με διάταξη νόμου, όπως στην περίπτωση της επεξεργασίας με σκοπό την ανίχνευση περιπτώσεων νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή τη χρηματοδότηση της τρομοκρατίας.[169]
Οι υπεύθυνοι πράξεων επεξεργασίας υποχρεούνται να ενημερώνουν το υποκείμενο των δεδομένων κατά τη συλλογή των δεδομένων προσωπικού χαρακτήρα που το αφορούν σχετικά με τη σκοπούμενη επεξεργασία τους. Η υποχρέωση αυτή δεν εξαρτάται από αίτημα του υποκειμένου των δεδομένων, αλλά αντιθέτως ο υπεύθυνος επεξεργασίας πρέπει να συμμορφώνεται προς αυτήν προδραστικά, ανεξάρτητα από το αν το υποκείμενο των δεδομένων θα εκφράσει ενδιαφέρον για την ενημέρωση.[170]
Η αρχή της διαφάνειας απαιτεί κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα να είναι γενικά διαφανής για τα φυσικά πρόσωπα. Τα φυσικά πρόσωπα έχουν το δικαίωμα να γνωρίζουν ποια δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται ή υποβάλλονται άλλως σε επεξεργασία, και με ποιον τρόπο, καθώς και να ενημερώνονται για τους κινδύνους, τις εγγυήσεις και τα δικαιώματά τους σε σχέση με την επεξεργασία. [171]
Στα άρθρα 13 και 14 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 εξετάζεται το δικαίωμα ενημέρωσης των υποκειμένων των δεδομένων σε περιπτώσεις στις οποίες τα δεδομένα προσωπικού χαρακτήρα συλλέγονται απευθείας από αυτά και σε περιπτώσεις στις οποίες δεν συλλέγονται από αυτά, αντίστοιχα.
Όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από τον πελάτη-υποκείμενο των δεδομένων, το πιστωτικό ίδρυμα, παρέχει στο υποκείμενο των δεδομένων τις απαραίτητες πληροφορίες κατά τη λήψη αυτών. Η απαραίτητη πληροφόρηση συμπεριλαμβάνει την ταυτότητά του πιστωτικού ιδρύματος και τα στοιχεία επικοινωνίας με αυτά, τις κατηγορίες των υπό επεξεργασία δεδομένων, τους σκοπούς της επεξεργασίας, τη νομική βάση της επεξεργασίας, τις κατηγορίες των αποδεκτών των δεδομένων, το εάν στην

[168] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.259
[169] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019., άρθρο 17.
[170]Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ. 260
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
[171]Αιτιολογική σκέψη 39του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

επεξεργασία περιλαμβάνεται αυτοματοποιημένη λήψη απόφασης ή λήψη απόφασης ως αποτέλεσμα κατάρτισης προφίλ, το εάν τα δεδομένα θα διαβιβασθούν σε τρίτη χώρα, όπως και για την άσκηση των κατά τον Κανονισμό και του παρόντα Κώδικα δικαιωμάτων των πελατών-υποκειμένων, περιλαμβανομένης και της υποβολής καταγγελίας στην Αρχή.[172]

Όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από τον πελάτη, το πιστωτικό ίδρυμα παρέχει σε αυτόν τις κατά την προηγούμενη παράγραφο πληροφορίες εντός εύλογης προθεσμίας, όχι μεγαλύτερης του ενός μηνός από τη συλλογή τους.[173] Εφόσον οι κατηγορίες των δεδομένων και οι κατηγορίες των αποδεκτών, ανεξάρτητα εάν προέρχονται από το ίδιο το υποκείμενο ή όχι, είναι γνωστές στο πιστωτικό ίδρυμα κατά την πρώτη επικοινωνία με τον πελάτη, η ενημέρωση γίνεται για το σύνολο των δεδομένων που πρόκειται να τεθούν σε επεξεργασία στην ίδια χρονική στιγμή. Στις περιπτώσεις που τα δεδομένα χρησιμοποιούνται για επικοινωνία του πιστωτικού ιδρύματος με το υποκείμενο ή ανακοινώνονται σε άλλους αποδέκτες, η ενημέρωση γίνεται κατά την πρώτη επικοινωνία ή ανακοίνωση.

Το πιστωτικό ίδρυμα δεν έχει υποχρέωση παροχής πληροφοριών όταν το υποκείμενο των δεδομένων διαθέτει ήδη τις πληροφορίες. Όταν το πιστωτικό ίδρυμα έχει συλλέξει τα δεδομένα από άλλη πηγή, δεν υποχρεούται σε ενημέρωση εφόσον η παροχή πληροφοριών στο υποκείμενο αποδεικνύεται αδύνατη ή θα απαιτούσε δυσανάλογη προσπάθεια , όπως εάν είναι ανύπαρκτα ή ελλιπή τα στοιχεία επικοινωνίας με τους πελάτες-υποκείμενα ή είναι πιθανόν να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της επεξεργασίας. Εάν για παράδειγμα αφορά παροχή στοιχείων που αποδυναμώνουν την άσκηση νόμιμου δικαιώματος.[174] Επίσης, εφόσον η απόκτηση ή η κοινολόγηση των δεδομένων προβλέπεται ρητώς σε νόμο που παρέχει τα κατάλληλα μέτρα για την προστασία των εννόμων συμφερόντων των υποκειμένων (ΓΕΜΗ, φορολογική αρχή), ή η πληροφορία υπόκειται σε επαγγελματικό απόρρητο. [175]

Η υποχρέωση για διαφάνεια στην επεξεργασία των προσωπικών δεδομένων εκτείνεται σε όλα τα στάδια της επεξεργασίας ήτοι, από την έναρξη της επεξεργασίας, καθ΄ όλη την διάρκεια αυτής και μέχρι την λήξη της (π.χ. όταν γίνει παραβίαση της προστασίας ή υπάρχουν ουσιώδεις αλλαγές στην επεξεργασία). Ειδικά στην περίπτωση ουσιωδών αλλαγών στην επεξεργασία, που μπορεί να έχουν επίπτωση στα υποκείμενα, το πιστωτικό ίδρυμα παρέχει την πληροφόρηση πριν λάβει χώρα η αλλαγή, ο δε τρόπος επικοινωνίας των πιστωτικών ιδρυμάτων με τα υποκείμενα σχετικά με την αλλαγή πρέπει να

[172] Άρθρο 13, παρ 1 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[173] Άρθρο 14 παρ.3 περ. α' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[174] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.. άρθρο 17.4
[175] Άρθρο 14 παρ 5' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 και Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.. άρθρο 17.4

είναι αποτελεσματικός.

Δικαίωμα πρόσβασης

Εφόσον το επιθυμεί, ο πελάτης έχει το δικαίωμα πρόσβασης στα προσωπικά του δεδομένα όταν υφίστανται επεξεργασία. Το δικαίωμα πρόσβασης του φυσικού προσώπου στα δεδομένα που το αφορούν αναγνωρίζεται ρητώς στο άρθρο 15 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016.Το δικαίωμα του φυσικού προσώπου να έχει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που το αφορούν είναι βασικό στοιχείο του ευρωπαϊκού δικαίου για την προστασία δεδομένων.

Η πρόσβαση του υποκειμένου των δεδομένων στα δεδομένα προσωπικού χαρακτήρα που το αφορούν θα το βοηθήσει να διαπιστώσει αν αυτά είναι ακριβή. Επομένως, είναι σημαντικό να ενημερώνεται το υποκείμενο των δεδομένων με κατανοητό τρόπο όχι μόνο για τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία αυτά καθαυτά, αλλά και για τις κατηγορίες υπό τις οποίες τα εν λόγω δεδομένα υποβάλλονται σε επεξεργασία, όπως για παράδειγμα: ονοματεπώνυμο, αριθμός πιστωτικής κάρτας κ.λ.π.[176]

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από το πιστωτικό ίδρυμα επιβεβαίωση για το κατά πόσον ή όχι δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία. Σε περίπτωση που υφίσταται επεξεργασία, το υποκείμενο έχει το δικαίωμα να ζητά και να λαμβάνει τις ακόλουθες τουλάχιστον πληροφορίες: τον σκοπό της επεξεργασίας (πχ. κατάρτιση και λειτουργία χρηματοδοτικής σύμβασης), τις κατηγορίες των αποδεκτών των δεδομένων (πχ. εταιρείες ενημέρωσης οφειλετών του Ν. 3758/2009 όπως ισχύει, εταιρείες διαχείρισης απαιτήσεων του Ν. 4354/2015, δικηγόροι κλπ.), εάν αυτά διαβιβάζονται σε τρίτη χώρα ή διεθνή οργανισμό (όπως πχ. στην περίπτωση εκτέλεσης εντολής πληρωμής σε τρίτη χώρα), πληροφορίες για την προέλευσή τους (πχ. από τον οφειλέτη, από την εταιρεία ΤΕΙΡΕΣΙΑΣ ΑΕ ή άλλα αρχεία δεδομένων οικονομικής συμπεριφοράς, από υποθηκοφυλακεία κλπ.), πληροφορίες για την άσκηση των δικαιωμάτων του, περιλαμβανομένου του δικαιώματος καταγγελίας στην εποπτική Αρχή, την πληροφορία εάν στην επεξεργασία περιλαμβάνεται αυτοματοποιημένη λήψη απόφασης ή κατάρτιση προφίλ. [177]

Το υποκείμενο των δεδομένων, μετά την ως άνω πληροφόρηση δικαιούται να επανέλθει και να ζητήσει αντίγραφο των υπό επεξεργασία δεδομένων του. Στην περίπτωση αυτή το πιστωτικό ίδρυμα υποχρεούται να δώσει στον αιτούντα πελάτη τις πλέον πρόσφατες σχετικές πληροφορίες που

[176] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018, σελ.275
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

[177] Άρθρο 15, παρ.1 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 και Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019., άρθρο 19.1

παράγονται, ανά προϊόν ή υπηρεσία, από τα συστήματα πληροφορικής που διαθέτει. Αναπαραγωγή και αποστολή δεδομένων που έχουν ήδη διατεθεί στον πελάτη και αναπαραγωγή με διαφορετικό τρόπο μπορεί να γίνει μόνο εάν είναι ευχερώς συστημικά εφικτό και μπορεί να γίνει με την επιβάρυνση του αιτούντος πελάτη με το σχετικό κόστος.[178]

Το πιστωτικό ίδρυμα ενδέχεται να μην είναι σε θέση να ικανοποιήσει το δικαίωμα πρόσβασης, εάν πληροφορίες που αφορούν το υποκείμενο τηρούνται σε αρχεία που δεν συνδέονται άμεσα με αυτό, όπως για παράδειγμα αρχεία αποβιωσάντων στα οποία περιέχονται στοιχεία κληρονόμων. Επίσης εάν το δικαίωμα πρόσβασης του πελάτη επηρεάζει δυσμενώς τα δικαιώματα άλλων. [179] Εάν στο αρχείο πελάτη που ασκεί το δικαίωμα πρόσβασης περιέχονται προσωπικά δεδομένα που αναφέρονται σε τρίτα φυσικά πρόσωπα (πχ. περιπτώσεις κοινών λογαριασμών καταθετικών ή χορηγητικών), το πιστωτικό ίδρυμα μπορεί να αρνηθεί να το ικανοποιήσει, εκτός εάν έχει λάβει τη συγκατάθεση του τρίτου προσώπου ή στηρίζεται σε άλλη νόμιμη βάση.

Στην περίπτωση αυτοματοποιημένης επεξεργασίας ή κατάρτισης προφιλ, το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης σε πληροφορίες για τη λογική που ακολουθείται, καθώς και για τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το ίδιο. Από την ως άνω πληροφόρηση αποκλείονται πληροφορίες που εμπίπτουν στο επιχειρηματικό απόρρητο του πιστωτικού ιδρύματος, όπως π.χ. ειδικές πληροφορίες σχετικά με τον αλγόριθμο που χρησιμοποιεί, τη βαρύτητα των δεδομένων που χρησιμοποιούνται κλπ.[180]

Δικαίωμα διόρθωσης

Τα υποκείμενα των δεδομένων έχουν το δικαίωμα να απαιτήσουν από τον υπεύθυνο επεξεργασίας τη διόρθωση των δεδομένων προ¬σωπικού χαρακτήρα που τα αφορούν, χωρίς αδικαιολόγητη καθυστέρηση. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.[181] Η ακρίβεια των δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη προκειμένου να διασφαλίζεται υψηλό επίπεδο προστασίας για τα υποκείμενα των δεδομένων.[182]

Στις περιπτώσεις που διαπιστώνονται ανακρίβειες ή ελλείψεις στα προσωπικά δεδομένα, ο πελάτης έχει την υποχρέωση και το δικαίωμα να

[178] Άρθρο 15, παρ.3 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 και Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019. Άρθρο 19.2

[179] Άρθρο 15, παρ.4 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[180] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, άρθρο 19.5

[181] Άρθρο 16 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[182] Αιτιολογική σκέψη 65 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

απαιτήσει από το πιστωτικό ίδρυμα την, χωρίς αδικαιολόγητη καθυστέρηση, διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν την ή συμπλήρωσή τους.
Το πιστωτικό ίδρυμα προβαίνει στην διόρθωση ή συμπλήρωση στους προβλεπόμενους χρόνους ανταπόκρισης, υπό την προϋπόθεση ότι το υποκείμενο των δεδομένων θα υποβάλει σε αυτό την απαιτούμενη κατά περίπτωση πλήρη σχετική τεκμηρίωση.
Ενόσω εκκρεμεί αστική αγωγή ή προσφυγή ενώπιον δημόσιας αρχής προκειμένου να αποφασιστεί αν τα δεδομένα είναι ορθά ή μη, το υποκείμενο των δεδομένων μπορεί να ζητήσει να προστεθεί στον φάκελό του καταχώριση ή σημείωση στην οποία θα αναφέρεται ότι η ακρίβειά αμφισβητείται και ότι εκκρεμεί η έκδοση επίσημης απόφασης.[183] Κατά το διάστημα αυτό, ο υπεύθυνος επεξεργασίας δεν πρέπει να παρουσιάζει τα δεδομένα ως ορθά ή μη υποκείμενα σε τροποποίηση, ιδίως σε τρίτους.

Δικαίωμα διαγραφής

Η παροχή στα υποκείμενα των δεδομένων του δικαιώματος διαγραφής των δεδομένων που τα αφορούν είναι ιδιαίτερα σημαντική για την αποτελεσματική εφαρμογή των αρχών περί προστασίας των δεδομένων, και ιδίως της αρχής της ελαχιστοποίησης των δεδομένων. Το δικαίωμα του φυσικού προσώπου να ζητεί τη διαγραφή των δεδομένων προ¬σωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση ισχύει όταν τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.[184]
Επίσης, όταν το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία.[185]
Όταν το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία.[186]
Όταν τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα.[187]
Όταν τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κρά¬τους μέλους στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.[188]
Όταν τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί στο πλαίσιο της παροχής υπηρεσιών της κοινωνίας των πληροφοριών σε παιδιά βάσει του

[183] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ. 276
[184] Άρθρο 17 παρ 1, περ α'του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[185] Άρθρο 12, παρ.1, περ β' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[186] Άρθρο 12, παρ.1, περ γ' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[187] Άρθρο 12, παρ.1, περ δ' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[188] Άρθρο 12, παρ.1, περ ε' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

άρθρου 8 παρ.1 του Γενικού Κανονισμού Προστασίας Δεδομένων. [189]
Το βάρος της απόδειξης της νομιμότητας της επεξεργασίας των δεδομένων φέρουν οι υπεύθυνοι επεξεργασίας, καθώς είναι υπεύθυνοι για τη νομιμότητα της επεξεργασίας. Σύμφωνα με την αρχή της λογοδοσίας, ο υπεύθυνος επε¬ξεργασίας οφείλει να είναι ανά πάσα στιγμή σε θέση να αποδείξει την ύπαρξη ορθής νομικής βάσης για την επεξεργασία των δεδομένων, διαφορετικά η επε¬ξεργασία πρέπει να παύσει[190].
Ο Γενικός Κανονισμός Προστασίας Δεδομένων προβλέπει εξαιρέσεις[191] στο δικαίωμα διαγραφής, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση, την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους στο οποίο υπάγεται ο υπεύ¬θυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας, για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.
Το πιστωτικό ίδρυμα, ως υπεύθυνος επεξεργασίας, προβαίνει στη διαγραφή των σχετικών δεδομένων από το φυσικό και από το ηλεκτρονικό αρχείο στους προβλεπόμενους[192] χρόνους ανταπόκρισης, εκτός εάν η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με νομική υποχρέωση ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον, για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς. Σε κάθε περίπτωση τα δεδομένα δεν διαγράφονται πριν από την εξάντληση του προβλεπόμενου χρόνου τήρησης αυτών, εκτός εάν πρόκειται για επουσιώδη δεδομένα που ουδεμία επιρροή ασκούν στα δικαιώματα και τα έννομα συμφέροντα του πιστωτικού ιδρύματος. [193]

Δικαίωμα περιορισμού της επεξεργασίας

Τα υποκείμενα των δεδομένων έχουν το δικαίωμα να ζητήσουν από τον υπεύθυνο επεξεργασίας τον προσωρινό περιορισμό της επε¬ξεργασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν υπό τις προϋποθέσεις του άρθρου 18, παρ1 του Γενικού Κανονισμού Προστασίας Δεδομένων.

Σε ότι αφορά στα πιστωτικά ιδρύματα, το υποκείμενο των δεδομένων

[189] Άρθρο 12, παρ.1, περ στ' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[190] Άρθρο 5, παρ 2 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[191] Άρθρο 17, παρ.3 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[192] Άρθρο 12, παρ. 3 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[193] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

δικαιούται να εξασφαλίζει από το πιστωτικό ίδρυμα τον περιορισμό της επεξεργασίας, όταν ισχύει κάποια από τις παρακάτω περιπτώσεις.

Όταν η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στο πιστωτικό ίδρυμα να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα.

Όταν η επεξεργασία έχει κριθεί παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων και ζητεί, αντί αυτής, τον περιορισμό της χρήσης τους.

Όταν το πιστωτικό ίδρυμα δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.

Όταν το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το δικαίωμα εναντίωσης, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του πιστωτικού ιδρύματος υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

Όταν η επεξεργασία έχει περιοριστεί σύμφωνα με τους ανωτέρω λόγους, τα εν λόγω δεδομένα προσωπικού χαρακτήρα, εκτός της αποθήκευσης, πρέπει αφενός να είναι διακριτά και να περιορίζεται η πρόσβαση σε αυτά και αφετέρου να υφίστανται άλλη επεξεργασία μόνο με τη συγκατάθεση του υποκειμένου ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημόσιου συμφέροντος.

Στην περίπτωση που η επεξεργασία των δεδομένων του υποκειμένου έχει περιοριστεί σύμφωνα με τα παραπάνω, τα πιστωτικά ιδρύματα ενημερώνουν το υποκείμενο για την άρση του περιορισμού πριν αυτή επέλθει.[194]

Δικαίωμα εναντίωσης

Τα υποκείμενα των δεδομένων δεν έχουν γενικό δικαίωμα να αντιτάσσονται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Μπορούν να επικαλούνται το δικαίωμά τους να αντιτάσσονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή τους και στην επεξεργασία δεδομένων για σκοπούς απευθείας εμπορικής προώθησης. Το δικαίωμα εναντίω¬σης μπορεί να ασκείται με αυτοματοποιημένα μέσα.

Στο υποκείμενο των δεδομένων παρέχεται η δυνατότητα[195] να εγείρει αντιρρήσεις για λόγους που σχετίζονται με την ιδιαί¬τερη κατάστασή του

[194] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.
[195] Άρθρο 21 παρ. 1 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

όταν η νομική βάση για την επεξεργασία είναι η εκτέλεση καθήκοντος για λόγους δημόσιου συμφέροντος από τον υπεύθυνο επεξεργασίας ή όταν η επεξεργασία βασίζεται στα έννομα συμφέροντα του υπευθύνου επε¬ξεργασίας . Το δικαίωμα εναντίωσης εφαρμόζεται στις δραστηριότητες κατάρ¬τισης προφίλ. Το δικαίωμα εναντίωσης για λόγους που σχετίζονται με την ιδιαίτερη κατάσταση του υποκειμένου των δεδομένων αποσκοπεί στην επίτευξη της κατάλληλης ισορ¬ροπίας μεταξύ, αφενός, των δικαιωμάτων προστασίας δεδομένων του υποκει¬μένου των δεδομένων και, αφετέρου, των νόμιμων δικαιωμάτων των τρίτων για επεξεργασία των δεδομένων του. Βασικό δικαίωμα του πελάτη είναι το δικαίωμα να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία προσωπικών του δεδομένων που τον αφορούν και η Τράπεζα οφείλει να το σεβαστεί. Το αποτέλεσμα της επιτυχούς εναντίωσης είναι ότι ο υπεύθυνος επεξεργασίας δεν επιτρέπεται πλέον να επεξεργάζεται τα επίμαχα δεδομένα.[196] Στην περίπτωση αυτή το πιστωτικό ίδρυμα δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου. Τέτοια περίπτωση συντρέχει όταν η επεξεργασία των δεδομένων είναι απαραίτητη για τη λειτουργία σύμβασης και μέχρι την εξάντληση του χρόνου τήρησης αυτών. Ωστόσο, οι πρά¬ξεις επεξεργασίας που έχουν εκτελεστεί επί των δεδομένων αυτών παραμένουν νόμιμες.[197]

Επίσης, προβλέπεται ειδικό δικαίωμα εναντίωσης στη χρήση δεδομένων προσωπικού χαρακτήρα για σκοπούς απευθείας εμπο¬ρικής προώθησης.[198] Το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιτάσσεται ανά πάσα στιγμή και χωρίς επιβάρυνση στη χρήση των δεδομένων προσωπικού χαρακτήρα που το αφορούν για σκοπούς απευθείας εμπορικής προώθησης. Εφόσον η εν λόγω προώθηση γίνεται με ηλεκτρονικά μέσα, το πιστωτικό ίδρυμα εφαρμόζει τις σχετικές διατάξεις για τις ηλεκτρονικές επικοινωνίες που αφορούν την αποστολή προωθητικών ενεργειών μέσω αυτομάτων συστημάτων κλήσης, ηλεκτρονικών μηνυμάτων, γραπτών μηνυμάτων σε κινητό τηλέφωνο, κ.α.[199]

Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για το εν λόγω δικαίωμα με σαφή τρόπο, ξέχωρα από κάθε άλλη πληροφόρηση.[200]

Το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί, για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν, σε περίπτωση που τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς

[196] Άρθρο 21 παρ. 3 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[197] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.288

[198] Άρθρο 21 παρ. 2 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[199] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

[200] Άρθρο 21 παρ. 4 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς , εκτός εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που ασκείται για λόγους δημόσιου συμφέροντος.
Το πιστωτικό ίδρυμα θα πρέπει να διαχειρίζεται ξεχωριστά τα αιτήματα των υποκειμένων ανάλογα αν αυτά αφορούν δεδομένα που υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης η επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.[201]

Δικαίωμα σε ανθρώπινη παρέμβαση στα πλαίσια απόφασης μέσω αυτοματοποιημένης διαδικασίας

Σε περιπτώσεις που λαμβάνονται αποφάσεις, ως αποτέλεσμα αυτοματοποιημένης επεξεργασίας των προσωπικών του δεδομένων, ο πελάτης έχει το δικαίωμα να ζητήσει την εξαίρεσή του, εφόσον συντρέχουν συγκεκριμένοι λόγοι.
Οι αυτοματοποιημένες αποφάσεις είναι αποφάσεις οι οποίες λαμβάνονται με τη χρήση δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργα¬σία αποκλειστικά με αυτόματα μέσα, χωρίς ανθρώπινη παρέμβαση. Τα υποκείμενα των δεδομένων δεν πρέπει να υπόκεινται σε αυτο¬ματοποιημένες αποφάσεις που παράγουν έννομα αποτελέσματα ή έχουν παρό¬μοιες σημαντικές συνέπειες. Εάν οι εν λόγω αποφάσεις είναι πιθανό να έχουν σημαντικό αντίκτυπο στη ζωή των φυσικών προσώπων επειδή σχετίζονται, για παράδειγμα, με την πιστοληπτική ικανότητα, τις ηλεκτρονικές προσλήψεις, τις επιδόσεις στην εργασία ή την ανάλυση συμπεριφοράς ή αξιοπιστίας, τότε απαι¬τείται ειδική προστασία για να αποφευχθούν αρνητικές επιπτώσεις. Η λήψη αυτοματοποιημένων αποφάσεων περιλαμβάνει την κατάρτιση προφίλ, η οποία συνίσταται σε οποιαδήποτε μορφή αυτόματης αξιολόγησης προσωπικών πτυ¬χών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή τα ενδιαφέροντα, την αξιοπιστία ή τη συμπερι¬φορά, τη θέση ή τις μετακινήσεις του υποκειμένου των δεδομένων.[202]
Η αυτοματοποιημένη λήψη αποφάσεων που παράγουν έννομα αποτελέσματα ή επηρεάζουν σημαντικά τα φυσικά πρό¬σωπα ενδέχεται να είναι αποδεκτή εάν είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υπευθύνου επεξεργασίας δεδομένων και του υποκειμένου των δεδομένων ή εάν το υποκείμενο των δεδομένων έχει παρά¬σχει τη ρητή συγκατάθεσή του. Επίσης, η αυτοματοποιημένη λήψη αποφάσεων είναι αποδεκτή εάν επιτρέπεται από τον νόμο και εάν προστατεύονται δεόντως τα δικαιώματα, οι ελευθερίες και τα έννομα συμφέροντα του υποκειμένου των δεδομένων.[203]

[201] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.
[202] Αιτιολογική σκέψη 71 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[203] Άρθρο 22, παρ. 2, του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

Ως παράδειγμα. για την ταχεία αξιολόγηση της πιστοληπτικής ικανότητας ενός μελλοντικού πελάτη, οι υπηρεσίες πληροφοριών πιστοληπτικής ικανότητας συγκεντρώνουν ορισμένα δεδομένα, όπως την κατάσταση των πιστωτικών λογαριασμών και των λογαριασμών υπηρεσιών/παροχών κοινής ωφέλειας του πελάτη, τα στοιχεία των προηγούμενων διευθύνσεων του πελάτη, καθώς και πληροφορίες από δημόσιες πηγές, όπως εκλογικούς καταλόγους, δημόσια μητρώα (συμπεριλαμβανομένων δικαστικών αποφάσεων) ή δεδομένα πτώχευσης και αφερεγγυότητας. Τα εν λόγω δεδομένα προσωπικού χαρακτήρα εισάγονται στη συνέχεια σε έναν αλγόριθμο βαθμολόγησης, ο οποίος υπολογίζει τη συνολική αξία της πιστοληπτικής ικανότητας του δυνητικού πελάτη.[204]

Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση του πιστωτικού ιδρύματος που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζουν σημαντικά. Η λήψη απόφασης που λαμβάνεται βάσει αποκλειστικά αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, δύναται να επιτρέπεται όταν είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ υποκειμένου των δεδομένων και του πιστωτικού ιδρύματος, όπως στην περίπτωση κατάρτισης του πιστοληπτικού προφίλ (credit scoring) του αιτούντος δάνειο ή πίστωσης ή του δανειολήπτη. Επίσης όταν προβλέπεται ρητά από το δίκαιο της Ένωσης ή κράτους μέλους, στο οποίο υπόκειται το πιστωτικό ίδρυμα, όπως μεταξύ άλλων για σκοπούς παρακολούθησης και πρόληψης της απάτης και της φοροδιαφυγής σύμφωνα με τους κανονισμούς, τα πρότυπα και το νομικό, κανονιστικό ή νομολογιακό πλαίσιο των οργάνων της Ένωσης ή των εθνικών οργάνων εποπτείας και προκειμένου να διασφαλιστεί η ασφάλεια και η αξιοπιστία της υπηρεσίας που παρέχει ο υπεύθυνος επεξεργασίας, καθώς και όταν το υποκείμενο των δεδομένων παρέσχε τη ρητή προς τούτο συγκατάθεσή του. Στις προαναφερόμενες περιπτώσεις, το πιστωτικό ίδρυμα εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων των υποκειμένων για την εξασφάλιση ανθρώπινης παρέμβασης στη λήψη απόφασης και την έκφραση άποψης και αμφισβήτησης της απόφασης από το υποκείμενο. [205]

Δικαίωμα φορητότητας

Τα υποκείμενα των δεδομένων απολαύουν του δικαιώματος στη φορητότητα των δεδομένων σε περιπτώσεις στις οποίες τα δεδομένα προσωπικού χαρακτήρα τα οποία έχουν παράσχει σε υπεύθυνο επε¬ξεργασίας

[204] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.293
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

[205] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

υποβάλλονται σε επεξεργασία με αυτοματοποιημένα μέσα βάσει συγκατάθεσης ή σε περιπτώσεις στις οποίες η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης και διενεργείται με αυτοματοποιημένα μέσα. Εάν είναι εφαρμοστέο το δικαίωμα στη φορητότητα των δεδομένων, τα υποκείμενα των δεδομένων δικαιούνται να ζητούν την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα τους από έναν υπεύθυνο επεξεργασίας σε άλλον, εάν αυτό είναι τεχνικά εφικτό.[206] Προς διευκόλυνση της διαδικασίας αυτής, ο υπεύθυνος επεξεργασίας θα πρέπει να αναπτύξει διαλειτουργικούς μορφότυπους που επιτρέπουν τη φορητότητα των δεδομένων για τα υποκείμενα των δεδομένων. Οι μορφότυποι αυτοί πρέπει να είναι δομημένοι, κοινώς χρησιμοποιούμενοι και αναγνώσιμοι από μηχανήματα προκει¬μένου να διευκολύνουν τη διαλειτουργικότητα.[207] Η διαλειτουργικότητα μπορεί να οριστεί υπό ευρεία έννοια ως η ικανότητα των συστημάτων πληροφοριών να ανταλλάσσουν δεδομένα και να επιτρέπουν την κοινή χρήση πληροφοριών.

Ο κάθε πελάτης έχει το δικαίωμα να ζητήσει από την Τράπεζα να λάβει τα δεδομένα προσωπικού χαρακτήρα που έχει παραχωρήσει, σε κοινώς χρησιμοποιούμενο και αναγνώσιμο αρχείο ή να σταλούν σε άλλο πάροχο.

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, τα οποία έχει παράσχει στο πιστωτικό ίδρυμα, κατά τα αναφερόμενα στην αμέσως επόμενη παράγραφο και να ζητά από το πιστωτικό ίδρυμα να διαβιβάζει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, κατά τα κατωτέρω, σε άλλον υπεύθυνο επεξεργασίας, χωρίς αντίρρηση από το πιστωτικό ίδρυμα, στις περιπτώσεις που η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου ή αφορά στην εκτέλεση σύμβασης και διενεργείται με αυτοματοποιημένα μέσα.

Περίπτωση φορητότητας στο χώρο των πιστωτικών ιδρυμάτων είναι αυτή που αφορά στη μεταβίβαση σύμβασης δανείου ή πίστωσης σε άλλο πιστωτικό ίδρυμα ή στην μεταφορά καταθετικού λογαριασμού σε άλλο πιστωτικό ίδρυμα. Το πιστωτικό ίδρυμα, ανταποκρινόμενο σε κατά την προηγούμενη παράγραφο αίτημα υποκειμένου, είτε παρέχει σε αυτό τα δεδομένα, είτε διαβιβάζει αυτά σε άλλον υπεύθυνο επεξεργασίας, με τη χρήση δομημένου, κοινώς χρησιμοποιούμενου και αναγνωρίσιμου από τα μηχανογραφικά συστήματα του αποστολέα και του αποδέκτη μορφότυπο, εφόσον αυτό είναι τεχνικά εφικτό. Σε κάθε περίπτωση, τα πιστωτικά ιδρύματα πρέπει να αξιολογούν τους κινδύνους που συνεπάγεται η φορητότητα και να λαμβάνουν τα ενδεδειγμένα μέτρα για το μετριασμό τους, όπως πχ. κρυπτογράφηση. Δεν περιλαμβάνονται στο πεδίο εφαρμογής του δικαιώματος στη φορητότητα τα προσωπικά δεδομένα που παράγονται ή συνάγονται από την επεξεργασία, όπως για παράδειγμα η κατάρτιση πιστοληπτικού προφιλ, διότι δεν πρόκειται για δεδομένα που παρέχονται από το υποκείμενο, αλλά από την ανάλυση

[206] Άρθρο 20 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[207] Αιτιολογική σκέψη 68 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

δεδομένων που δεν αφορούν μόνο στην τυχόν χορηγητική σύμβαση μεταξύ πιστωτικού ιδρύματος και υποκειμένου. [208]

Προκειμένου να διευκολύνει τη άσκηση των συγκεκριμένων δικαιωμάτων των πελατών της, η Τράπεζα οφείλει να μεριμνήσει για την ανάπτυξη εσωτερικών διαδικασιών ώστε να είναι εφικτή η έγκαιρη και αποτελεσματική ανταπόκριση στα αιτήματά της, τα οποία η πελατεία μπορεί να υποβάλλει σε οποιοδήποτε κατάστημά της με ειδικά διαμορφωμένα έντυπα. Ειδικά δε για θέματα σχετικά με την επεξεργασία προσωπικών δεδομένων, οι πελάτες θα πρέπει να έχουν δυνατότητα να απευθύνονται εγγράφως στο γραφείο υπεύθυνου προστασίας δεδομένων (ταχυδρομικώς, με e-mail ή μέσω οποιουδήποτε καταστήματος της τράπεζας). Σε περιπτώσεις δε, που οι πελάτες θεωρούν ότι θίγονται τα δικαιώματά τους κατά οποιονδήποτε τρόπο, θα πρέπει να υπάρξει μέριμνα ώστε να είναι δυνατή η σχετική επικοινωνία μέσω ιστοσελίδας, τηλεφώνου, φυσικής ή ηλεκτρονικής αλληλογραφίας.

2.3 Υποχρεώσεις της Τράπεζας

Η Τράπεζα οφείλει αφενός να σέβεται τα δικαιώματα της πελατείας της, και αφετέρου να τηρεί τις υποχρεώσεις της για την προστασία των προσωπικών δεδομένων.

Απαιτείται να γίνεται μέριμνα σε δύο επίπεδα για την προστασία των προσωπικών δεδομένων που έχει στη διάθεσή της.

Σε πρώτο επίπεδο θα πρέπει να διασφαλιστεί τη ασφάλεια και το απόρρητο της επεξεργασίας. Αυτό επιτυγχάνεται όταν η επεξεργασία των προσωπικών δεδομένων γίνεται αποκλειστικά από πρόσωπα που δρουν υπό τον έλεγχο της Τράπεζας και τα οποία έχουν επιλεγεί με αυστηρά κριτήρια, και υπάρχει μέριμνα ώστε να παρέχονται επαρκείς εγγυήσεις από πλευράς γνώσης του νομικού πλαισίου και δέσμευσης για την τήρηση του απορρήτου. Παράλληλα θα πρέπει να χρησιμοποιούνται εφαρμογές που πληρούν πρότυπα ασφαλείας υψηλού επιπέδου. Επιπροσθέτως, θα πρέπει να υπάρχει μέριμνα για τη διενέργεια ελέγχων σε τακτικά χρονικά διαστήματα, προκειμένου να εξασφαλίζεται ότι τηρούνται οι προβλεπόμενες διαδικασίες και εφαρμόζονται πιστά τα κριτήρια που ισχύουν.

Παράλληλα, θα πρέπει να ληφθούν οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχόν περιστατικά αθέμιτης επεξεργασίας, όπως παραβίαση, καταστροφή, απώλεια, αλλοίωση, διάδοση, πρόσβαση από μη εξουσιοδοτημένα πρόσωπα. Το επίπεδο ασφαλείας θα πρέπει να βρίσκεται σε αναλογία με τους κινδύνους που συνεπάγεται η επεξεργασία των προσωπικών δεδομένων της πελατείας.

Σε δεύτερο επίπεδο θα πρέπει να εγγυάται την ασφάλεια των πληροφοριακών συστημάτων. Με τη θέσπιση πολιτικής και εγχειριδίων ασφαλείας οφείλει να

[208] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

μεριμνά για την προστασία των δεδομένων κατά την διακίνησή τους μέσω των δικτύων, να ελέγχεται η πρόσβαση των χρηστών στα πληροφοριακά συστήματα και να εντοπίζονται έγκαιρα και να προλαμβάνονται περιστατικά παραβίασης ασφάλειας, ούτως ώστε το σύνολο των προσωπικών δεδομένων της πελατείας της, που καταχωρείται στα πληροφοριακά της συστήματα, να είναι θωρακισμένο.

Οι τράπεζες , ως υπεύθυνοι επεξεργασίας, οφείλουν να ενημερώνουν τα υποκείμενα των δεδομένων με ακρίβεια και σαφήνεια για τη συλλογή και χρήση (επεξεργασία) των προσωπικών τους δεδομένων, σύμφωνα με την αρχή της διαφάνειας (σχετ. άρθρα 12-14 Γενικού Κανονισμού Προστασίας Δεδομένων). Η ενημέρωση πρέπει να είναι συνοπτική, διαφανής, κατανοητή, εύκολα προσβάσιμη και διατυπωμένη σε απλή και σαφή γλώσσα. Η ενημέρωση πρέπει να περιλαμβάνει, μεταξύ άλλων, ιδίως τις εξής πληροφορίες: τον σκοπό της επεξεργασίας των δεδομένων, τις πηγές τους (όταν η συλλογή γίνεται από άλλες πηγές κι όχι από το ίδιο το υποκείμενο), το χρονικό διάστημα τήρησής τους, τους τυχόν αποδέκτες τους, καθώς και ενημέρωση για τα δικαιώματα που τους παρέχει ο Γ.Κ.Π.Δ. και τον τρόπο άσκησής τους.

Τα άρθρα 13 και 14 του Γενικού κανονισμού προστασίας Δεδομένων Ε.Ε. 679/2016 εξειδικεύουν ποιες ακριβώς πληροφορίες πρέπει να περιλαμβάνει η ενημέρωση, όταν η συλλογή γίνεται από τα ίδια τα υποκείμενα ή από άλλες πηγές, καθώς και τον χρόνο στον οποίο πρέπει να γίνει: α) τη στιγμή της συλλογής, όταν αυτή γίνεται απευθείας από τα υποκείμενα των δεδομένων, και β) σε εύλογο χρονικό διάστημα από τη συλλογή των δεδομένων (το αργότερο σε ένα μήνα), όταν αυτή γίνεται από άλλες πηγές. Η ως άνω υποχρέωση ενημέρωσης εξειδικεύεται περαιτέρω στα άρθρα 31 και 32 του εθνικού νόμου ν. 4624/2019 για την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων [209].

Η υποχρέωση ενημέρωσης, κατά τον Γενικό Κανονισμό Προστασίας Δεδομένων, σε κάποιες περιπτώσεις δεν υφίσταται (άρθρα 13 παρ. 4 και 14 παρ. 5) ή μπορεί να περιορισθεί (άρθρο 23). Στο άρθρο 14, παρ.5 στοιχ. β' προβλέπονται τρεις ξεχωριστές περιπτώσεις όπου αίρεται η υποχρέωση παροχής πληροφοριών του άρθρου 14 παρ.1,2 και 4. Όταν αποδεικνύεται αδύνατη (ιδίως για σκοπούς αρχειοθέτησης, σκοπούς επιστημονικής/ ιστορικής έρευνας ή στατιστικούς σκοπούς), όταν συνεπάγεται δυσανάλογη προσπάθεια (ιδίως για σκοπούς αρχειοθέτησης, σκοπούς επιστημονικής/ ιστορικής έρευνας ή στατιστικούς σκοπούς) και όταν η παροχή των πληροφοριών που απαιτούνται σύμφωνα με το άρθρο 14, παρ.1 θα καθιστούσε αδύνατη ή θα έβλαπτε σε μεγάλο βαθμό την επίτευξη των σκοπών της επεξεργασίας.

[209]https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/xrimatopistotika/pistwtika_xrhmatodotika

Για την τελευταία αυτή περίπτωση όπου η παροχή των πληροφοριών των δεδομένων από τον υπεύθυνο επεξεργασίας σε ένα υποκείμενο των δεδομένων είναι πιθανόν να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της επεξεργασίας, παρατίθεται[210] το παρακάτω παράδειγμα: «Η Τράπεζα (Α) υποχρεώνεται, σύμφωνα με τη νομοθεσία σχετικά με την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, στην υποχρεωτική απαίτηση να αναφέρει στην αρμόδια αρχή επιβολής του χρηματοπιστωτικού δικαίου οποιαδήποτε ύποπτη δραστηριότητα που σχετίζεται με λογαριασμούς που τηρούνται σε αυτήν. Η τράπεζα ενημερώνεται από άλλη τράπεζα σε άλλο κράτος μέλος για ύποπτες δραστηριότητες μεταφοράς χρηματικών ποσών σε λογαριασμό που τηρείται σε αυτήν από ύποπτο συναλλασσόμενο. Η Τράπεζα (Α) διαβιβάζει αυτά τα δεδομένα τα σχετικά με τον ύποπτο κάτοχο του λογαριασμού της και τις ύποπτες δραστηριότητες στην αρμόδια αρχή επιβολής χρηματοπιστωτικού δικαίου. Σύμφωνα με τη νομοθεσία σχετικά με την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, συνιστά ποινικό αδίκημα μια Τράπεζα που υποβάλλει αναφορά να προειδοποιεί τον κάτοχο του λογαριασμού ότι ενδέχεται να έχουν κινηθεί έρευνες από ρυθμιστική αρχή εις βάρος του. Σε αυτήν την περίπτωση εφαρμόζεται το άρθρο 14, παρ.5 στοιχ. β', διότι η παροχή στο υποκείμενο των δεδομένων των πληροφοριών του άρθρου 14 σχετικά με την επεξεργασία των δεδομένων του θα βλάψει σε σημαντικό βαθμό τους στόχους της νομοθεσίας, οι οποίοι περιλαμβάνουν την αποτροπή των άτυπων προειδοποιήσεων. Ωστόσο, σε όλους τους κατόχους λογαριασμού στην Τράπεζα (Α), θα πρέπει να παρέχεται η γενική ενημέρωση κατά το άνοιγμα του λογαριασμού ότι τα δεδομένα προσωπικού χαρακτήρα ους ενδέχεται να υποβληθούν σε επεξεργασία για σκοπούς καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.»

2.4. Γνωστοποίηση προσωπικών δεδομένων σε τρίτα μέρη και διασυνοριακή διαβίβαση δεδομένων.

Σύμφωνα με τις διατάξεις του Γενικού Κανονισμού, αλλά και των κανονιστικών διατάξεων των Τραπεζών, στα πλαίσια της νόμιμης λειτουργίας τους, τα δεδομένα που έχει η εκάστοτε Τράπεζα στην κατοχή της μπορούν να κοινοποιηθούν σε φυσικά ή νομικά πρόσωπα, δημόσιες αρχές, υπηρεσίες ή άλλους φορείς, υπό την προϋπόθεση ότι έχει προβεί σε ειδική ενημέρωση των πελατών της για την ενδεχόμενη διαβίβαση των δεδομένων.
Οι εν δυνάμει παραλήπτες των δεδομένων δυνητικά είναι:
1) Εταιρίες του ομίλου της εκάστοτε τράπεζας
2) Τρίτα πρόσωπα που ενεργούν κατ' εντολή και για λογαριασμό της.

[210] Σωτηρόπουλος Β., «Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019, σελ.411

Ενδεικτικά αναφέρονται: Εταιρείες για την ενημέρωση των οφειλετών για τις πριν ή μετά την καταγγελία οφειλές τους και την διενέργεια των απαιτούμενων προπαρασκευαστικών ενεργειών για την εξώδικη και δικαστική επιδίωξη της είσπραξης από την τράπεζα των ληξιπροθέσμων και απαιτητών οφειλών τους σύμφωνα με τα προβλεπόμενα στο Ν 3758/2009
Εταιρείες διαχείρισης απαιτήσεων από δάνεια και πιστώσεις του Ν 35/2015 όπως ισχύει.
Εταιρείες τήρησης και καταστροφής αρχείων.
Εταιρείες υπηρεσιών τηλεφωνικής εξυπηρέτησης πελατών
Εταιρείες προμήθειας και υποστήριξης πληροφοριακών συστημάτων
Εταιρείες ανάλυσης και έρευνας αγοράς και προώθησης προϊόντων
Εταιρείες φύλαξης και ασφάλειας
Εταιρείες παροχής υπηρεσιών θεματοφυλακής
Εταιρείες παροχής συμβουλευτικών υπηρεσιών συμπεριλαμβανομένων οικονομικών συμβουλών και ελεγκτών της τράπεζας
Πάροχοι αναφοράς δεδομένων
Ασφαλιστικές εταιρείες και ασφαλιστικοί διαμεσολαβητές στο πλαίσιο παροχής ασφαλιστικών προϊόντων.
Εκτιμητές ακινήτων
Οι ανωτέρω εταιρείες οφείλουν να συμμορφώνονται πλήρως με τις οδηγίες της τράπεζας και να τηρούν συγκεκριμένες διαδικασίες, όπως αυτές αναφέρονται σε συμβατικά κείμενα εξωτερικής ανάθεσης (outsourcing)
3) Εταιρείες ειδικού σκοπού στις οποίες μεταβιβάζονται απαιτήσεις της τράπεζας στο πλαίσιο τιτλοποίησης των απαιτήσεων καθώς και εταιρείες απόκτησης απαιτήσεων από δάνεια και πιστώσεις σύμφωνα με τον Ν 4354/2015
4) Εθνικοί και Ευρωπαϊκοί οργανισμοί που συμπράττουν με την Τράπεζα στην χορήγηση δανείων
5) Η «Διατραπεζικά Συστήματα ΑΕ» (ΔΙΑΣ ΑΕ) για την εξυπηρέτηση διατραπεζικών συναλλαγών, η ΤΕΙΡΕΣΙΑΣ ΑΕ για την προστασία της πίστης και των οικονομικών συναλλαγών, το Ταμείο Εγγύησης Καταθέσεων και Επενδύσεων, η Ελληνική Ένωση Τραπεζών, η Ελληνικά Χρηματιστήρια ΑΕ, Τράπεζες και Χρηματοπιστωτικοί οίκοι της Ελλάδας και του εξωτερικού
6) Ασφαλιστικοί φορείς, δημόσιοι οργανισμοί, επιμελητήρια και δημόσιες επιχειρήσεις 7) Πιστωτικά ιδρύματα, ιδρύματα πληρωμών, ιδρύματα ηλεκτρονικού χρήματος, ανώνυμες εταιρείες παροχής επενδυτικών υπηρεσιών (ΑΕΠΕΥ), ανώνυμες εταιρείες διαχείρισης αμοιβαίων κεφαλαίων (ΑΕΔΑΚ), τόποι εκτέλεσης και διαπραγμάτευσης, εταιρείες και συστήματα εκκαθάρισης και διακανονισμού συναλλαγών, αρχεία καταγραφής συναλλαγών
8) Εθνικές και Ευρωπαϊκές εποπτικές αρχές (Τράπεζα της Ελλάδος, Ευρωπαϊκή Κεντρική Τράπεζα, Ευρωπαϊκή Επιτροπή Ανταγωνισμού, Επιτροπή Κεφαλαιαγοράς, Ελληνική Επιτροπή Ανταγωνισμού, ΣΔΟΕ), δικαστικές αρχές (δικαστήρια, εισαγγελίες, ανακριτικοί υπάλληλοι, συμβολαιογράφοι,

δικαστικοί επιμελητές, υποθηκοφυλακεία, δικηγόροι) , ανεξάρτητες και λοιπές αρχές (Οικονομική αστυνομία, δημόσιες αρχές της Ελλάδος και του εξωτερικού) για την εκπλήρωση των υποχρέωσης της Τράπεζας βάσει νόμου, κανονιστικής διάταξης ή δικαστικής απόφασης.

Ειδικά για τις αρμόδιες εποπτικές, ανεξάρτητες, αστυνομικές , δικαστικές και εν γένει δημόσιες αρχές, η Τράπεζα ενδέχεται να γνωστοποιήσει τα στοιχεία όπου επιβάλλεται, σε τακτική ή έκτακτη βάση, εφόσον υποβληθεί σχετικό αίτημα ή εφόσον οφείλει να υποβάλλει αναφορά με τα εν λόγω στοιχεία χωρίς προηγούμενη ειδική ενημέρωση στους πελάτες. Ως παράδειγμα αναφέρεται η πληροφόρηση της Φορολογικής Αρχής από τους παρόχους υπηρεσιών πληρωμών (π.χ. πιστωτικά ιδρύματα) ως προς τις συναλλαγές αγορών με ηλεκτρονικά μέσα πληρωμών.

9) Ορκωτοί λογιστές και ελεγκτικές εταιρείες

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων προβλέπει την ελεύθερη ροή των δεδομένων εντός της Ευρωπαϊκής Ένωσης. Ωστόσο, περιλαμβάνει ειδικές απαιτήσεις που αφορούν τις διαβιβάσεις δεδο¬μένων προσωπικού χαρακτήρα σε χώρες εκτός ΕΕ και σε διεθνείς οργανισμούς. Ο κανονισμός αναγνωρίζει τη σημασία των εν λόγω διαβιβάσεων, ειδικότερα για τους σκοπούς του διεθνούς εμπορίου και της διεθνούς συνεργασίας, αλλά ταυ¬τόχρονα και τον αυξημένο κίνδυνο για τα δεδομένα προσωπικού χαρακτήρα.[211] Στο πλαίσιο άσκησης της δραστηριότητάς και των εργασιών της, η εκάστοτε Τράπεζα δύναται να προβαίνει στην διαβίβαση δεδομένων προσωπικού χαρακτήρα προς και από τις θυγατρικές της εταιρείες στο εξωτερικό καθώς και σε διασύνδεση ορισμένων αρχείων, εφόσον αυτό απαιτείται. Σύμφωνα με τις διατάξεις του Γενικού Κανονισμού, προβλέπεται η διαβίβαση σε εταιρείες που εδρεύουν εντός Ευρωπαϊκού οικονομικού χώρου και δεσμεύονται από αυτόν ή σε εταιρείες εκτός Ευρωπαϊκού χώρου εφόσον είναι σύμφωνη με το κατά τόπους νομοθετικό πλαίσιο και παρέχουν επαρκές επίπεδο προστασίας των προσωπικών δεδομένων. Στις περιπτώσεις που η χώρα εκτός Ευρωπαϊκού οικονομικού χώρου δεν παρέχει επαρκές επίπεδο προστασίας δεδομένων, τα προσωπικά δεδομένα μπορούν να διαβιβαστούν μόνο εφόσον θωρακίζονται από κάποια συμφωνία διαβίβασης δεδομένων η οποία εξασφαλίζει ένα επαρκές επίπεδο προστασίας. Η Τράπεζα οφείλει να θεσπίσει κατάλληλες διαδικασίες, ώστε να πραγματοποιούνται οι απαιτούμενες ενέργειες από τις κατά τόπους αρμόδιες αρχές στο εξωτερικό, και να διασφαλίσει ότι κάθε εμπλεκόμενη εταιρεία του ομίλου της, μεριμνά για την ασφαλή επεξεργασία των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται ή διασυνδέονται.

[211] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ.314

Το πιστωτικό ίδρυμα κατά τη λειτουργία και τη δραστηριότητά τόσο του ίδιου, όσο και των εταιρειών του ομίλου του, μπορεί να γνωστοποιεί προσωπικά δεδομένα σε αυτές, υπό τον όρο της προηγούμενης σχετικής ενημέρωσης των υποκειμένων. Η διαβίβαση στηρίζεται στις εποπτικές νομικές υποχρεώσεις του πιστωτικού ιδρύματος (πχ. ενοποιημένη εκτίμηση αναλαμβανόμενων κινδύνων, ενοποιημένες οικονομικές καταστάσεις κλπ) και στο έννομο συμφέρον αυτών για λόγους ενιαίας διαχείρισης του ομίλου και των πελατών του στον Ευρωπαϊκό Οικονομικό Χώρο (Ε.Ο.Χ).[212]
Η κατά τα λοιπά διαβίβαση προσωπικών δεδομένων εντός της Ευρωπαϊκής Ένωσης είναι ελεύθερη, εάν πληρούνται οι όροι και οι προϋποθέσεις του Κανονισμού.
Η διαβίβαση προσωπικών δεδομένων από το πιστωτικό ίδρυμα εκτός Ευρωπαϊκής Ένωσης σε εταιρίες του ομίλου του, σε εκτελούντες την επεξεργασία, σε τρίτους αποδέκτες και σε διεθνείς οργανισμούς διέπεται από τις διατάξεις των άρθρων 44 επομ. του Κανονισμού, καθώς και των διατάξεων των επόμενων παραγράφων του παρόντος άρθρου.
Η διασυνοριακή διαβίβαση προσωπικών δεδομένων από τα πιστωτικά ιδρύματα προς τρίτες χώρες ή διεθνείς οργανισμούς επιτρέπεται, χωρίς να απαιτείται ειδική προς τούτο άδεια, εφόσον υπάρχει απόφαση της Ευρωπαϊκής Επιτροπής, σύμφωνα με την οποία διασφαλίζεται επαρκές επίπεδο προστασίας από την τρίτη χώρα ή από συγκεκριμένο τομέα τρίτης χώρας ή από τον διεθνή οργανισμό. Τούτο, μεταξύ άλλων, ισχύει και για αποδέκτες που συμμετέχουν στο "EU-US Privacy Shield" στις ΗΠΑ, υπό τις ειδικότερες προϋποθέσεις που θέτει η σχετική απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής.
Ελλείψει απόφασης επάρκειας της Ευρωπαϊκής Επιτροπής, το πιστωτικό ίδρυμα μπορεί να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς μόνο εάν το πιστωτικό ίδρυμα, πριν την διαβίβαση, έχει παράσχει τις κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται δικαιώματα που μπορούν ευχερώς να ασκηθούν από τα υποκείμενα των δεδομένων και αποτελεσματικά ένδικα μέσα για την προστασία τους, όπως είναι το δικαίωμα άσκησης αποτελεσματικής διοικητικής ή δικαστικής προσφυγής και αξίωσης αποζημίωσης, στην τρίτη χώρα. Αυτές οι κατάλληλες εγγυήσεις μπορεί να συνίστανται στη χρήση ενός νομικά δεσμευτικού μέσου μεταξύ δημοσίων αρχών, δεσμευτικών εταιρικών κανόνων, πρότυπων συμβατικών ρητρών προστασίας των δεδομένων που θεσπίζονται από την Ευρωπαϊκή Επιτροπή ή έχουν εγκριθεί από αυτή, ή συμβατικών ρητρών, μηχανισμών πιστοποίησης και κωδίκων δεοντολογίας που εγκρίθηκαν από αρμόδια εποπτική αρχή.

[212] Απόφαση του Συμβουλίου και της Επιτροπής, της 13ης Δεκεμβρίου 1993, για τη σύναψη συμφωνίας σχετικά με τον Ευρωπαϊκό Οικονομικό Χώρο μεταξύ των Ευρωπαϊκών Κοινοτήτων, των κρατών μελών αυτών και της Δημοκρατίας της Αυστρίας, της Δημοκρατίας της Φινλανδίας, της Δημοκρατίας της Ισλανδίας, του Πριγκιπάτου του Λιχτενστάιν, του Βασιλείου της Νορβηγίας, του Βασιλείου της Σουηδίας και της Ελβετικής Συνομοσπονδίας (ΕΕ 1994 L 1).

Τα πιστωτικά ιδρύματα μπορούν να συνάπτουν δεσμευτικούς εταιρικούς κανόνες (BCRs) με τις θυγατρικές τους εταιρίες σε τρίτες χώρες, για τις διεθνείς διαβιβάσεις στις εταιρίες του ομίλου τους, που ασκούν κοινή οικονομική δραστηριότητα. Οι εν λόγω εταιρικοί κανόνες εγκρίνονται από αρμόδια εποπτική αρχή και πρέπει να είναι συμβατοί με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων.[213]

2.5 Ασφάλεια δεδομένων προσωπικού χαρακτήρα

Τα πιστωτικά ιδρύματα, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, λαμβάνουν τεχνικά και οργανωτικά μέτρα που θεωρούν κατάλληλα και αναλογικά προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των δεδομένων προσωπικού χαρακτήρα έναντι των κινδύνων. Ως παραβίαση προσωπικών δεδομένων ορίζεται η παραβίαση της ασφαλείας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.[214]

Στη γνωμοδότηση της 03/2014 σχετικά με τη γνωστοποίηση παραβιάσεων προσωπικών δεδομένων, η Ομάδα Εργασίας του άρθρου 29 εξήγησε ότι οι παραβιάσεις μπορούν να κατηγοριοποιηθούν σύμφωνα με τις ακόλουθες τρεις ευρέως γνωστές αρχές ασφάλειας πληροφοριών:

Παραβίαση απορρήτου, όταν υπάρχει μη εξουσιοδοτημένη ή τυχαία αποκάλυψη δεδομένων προσωπικού χαρακτήρα ή μη εξουσιοδοτημένη ή τυχαία πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.

Παραβίαση ακεραιότητας, όταν υπάρχει μη εξουσιοδοτημένη ή τυχαία αλλοίωση δεδομένων προσωπικού χαρακτήρα.

Παραβίαση διαθεσιμότητας, όταν υπάρχει τυχαία ή μη εξουσιοδοτημένη απώλεια πρόσβασης σε δεδομένα προσωπικού χαρακτήρα ή τυχαία ή μη εξουσιοδοτημένη καταστροφή δεδομένων προσωπικού χαρακτήρα.[215]

Η Τράπεζα, ως υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη την διαθέσιμη τεχνολογία, το κόστος υλοποίησης, τη φύση, το πεδίου εφαρμογής, τις περιστάσεις και τους σκοπούς της επεξεργασίας, καθώς και την πιθανότητα και σοβαρότητα των κινδύνων επεξεργασίας για τα υποκείμενα των δεδομένων, οφείλει να λαμβάνει τα απαραίτητα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίσει ένα επίπεδο ασφάλειας κατάλληλο για τον

[213] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019, αρθρο 12

[214] Άρθρο 4 περ.12 Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 και αρ.44ι Ν.4964/2019

[215] Σωτηρόπουλος Β, «Υπεύθυνος Προστασίας Δεδομένων Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», Εκδόσεις Σάκκουλα, 2019, σελ.196

κίνδυνο κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ιδίως όσον αφορά την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Τα μέτρα αυτά μπορεί να περιλαμβάνουν μεταξύ άλλων την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα, εφόσον τα εν λόγω μέσα είναι δυνατά για τους σκοπούς της επεξεργασίας. Θα πρέπει να διασφαλίζουν την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών που σχετίζονται με την επεξεργασία και τη δυνατότητα να αποκατασταθεί έγκαιρα η διαθεσιμότητα και η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα σε περίπτωση φυσικού ή τεχνικού συμβάντος.

Σε σχέση με την αυτοματοποιημένη επεξεργασία, μετά από αξιολόγηση των κινδύνων, η Τράπεζα ως υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει μέτρα που έχουν ως σκοπό:

α) την απαγόρευση της πρόσβασης μη εξουσιοδοτημένων προσώπων σε εξοπλισμό που χρησιμοποιείται για την επεξεργασία (έλεγχος πρόσβασης σε εξοπλισμό)

β) την αποτροπή της μη εξουσιοδοτημένης ανάγνωσης, αντιγραφής, τροποποίησης ή αφαίρεσης μέσων αποθήκευσης (έλεγχος μέσων αποθήκευσης)

γ) την αποτροπή της μη εξουσιοδοτημένης εισαγωγής δεδομένων προσωπικού χαρακτήρα και του μη εξουσιοδοτημένου ελέγχου, τροποποίησης ή διαγραφής αποθηκευμένων δεδομένων προσωπικού χαρακτήρα (έλεγχος αποθήκευσης)

δ) την αποτροπή της χρήσης συστημάτων αυτοματοποιημένης επεξεργασίας από μη εξουσιοδοτημένα πρόσωπα που χρησιμοποιούν εξοπλισμό επικοινωνίας δεδομένων (έλεγχος χρηστών)

ε) την εξασφάλιση ότι πρόσωπα που είναι εξουσιοδοτημένα να χρησιμοποιούν ένα σύστημα αυτοματοποιημένης επεξεργασίας έχουν πρόσβαση μόνο σε δεδομένα προσωπικού χαρακτήρα που καλύπτει η εξουσιοδότησή τους (έλεγχος πρόσβασης στα δεδομένα)

στ) την εξασφάλιση ότι είναι δυνατόν να επαληθευτεί και εξακριβωθεί σε ποιους φορείς διαβιβάστηκαν ή διατέθηκαν ή ενδέχεται να διαβιβαστούν ή να διατεθούν δεδομένα προσωπικού χαρακτήρα με τη χρήση εξοπλισμού επικοινωνίας δεδομένων (έλεγχος επικοινωνίας)

ζ) την εξασφάλιση ότι είναι δυνατόν να επαληθευτεί και να εξακριβωθεί εκ των υστέρων ποια δεδομένα προσωπικού χαρακτήρα εισήχθησαν σε συστήματα αυτοματοποιημένης επεξεργασίας, καθώς και πότε και από ποιόν (έλεγχος εισαγωγής)

η) την αποτροπή της μη εξουσιοδοτημένης ανάγνωσης, αντιγραφής, τροποποίησης ή διαγραφής δεδομένων προσωπικού χαρακτήρα κατά τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα ή κατά τη μεταφορά μέσων αποθήκευσης δεδομένων (έλεγχος διαβίβασης)

θ) την εξασφάλιση ότι η λειτουργία των εγκαταστημένων συστημάτων

μπορεί να αποκατασταθεί σε περίπτωση διακοπής της (αποκατάσταση)
ι) την εξασφάλιση ότι οι λειτουργίες του συστήματος εκτελούνται, ότι η εμφάνιση σφαλμάτων στις λειτουργίες αναφέρεται χωρίς υπαίτια καθυστέρηση (αξιοπιστία) και ότι τα αποθηκευμένα δεδομένα προσωπικού χαρακτήρα παραμένουν αναλλοίωτα σε περίπτωση δυσλειτουργίας του συστήματος (ακεραιότητα)
ια) την εξασφάλιση ότι τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για λογαριασμό του υπεύθυνου επεξεργασίας μπορούν να υποβληθούν σε επεξεργασία μόνο σύμφωνα με τις οδηγίες του υπεύθυνου επεξεργασίας (έλεγχος επεξεργασίας)
ιβ) την εξασφάλιση ότι τα δεδομένα προσωπικού χαρακτήρα προστατεύονται από απώλεια και καταστροφή (έλεγχος της διαθεσιμότητας).[216]
Μολονότι νέες τεχνολογίες, όπως η κρυπτογράφηση, παρέχουν περισσότερες δυνατότητες για την ενίσχυση της ασφάλειας της επεξεργασίας, οι παραβιάσεις δεδομένων αποτελούν ακόμη ένα κοινό φαινόμενο. Οι αιτίες των παραβιάσεων μπορούν να ποικίλουναπό τυχαία λάθη ανθρώπων που εργάζονται σε έναν οργανισμό μέχρι τις εξωτερικές απειλές από χάκερς και οργανώσεις κυβερνοεγκλήματος, όπως αναγνωρίζει το Εγχειρίδιο ευρωπαϊκού δικαίου προστασίας δεδομένων.[217] Οι παραβιάσεις δεδομένων μπορεί να είναι εξαιρετικά επιβλαβείς για την ιδιωτικότητα και την προστασία δεδομένων των ατόμων, που λόγω της παραβίασης χάνουν τον έλεγχο επί των προσωπικών τους δεδομένων. Οι παραβιάσεις μπορεί να έχουν ως αποτέλεσμα την κλοπή ταυτότητας ή την απάτη, οικονομική απώλεια ή υλικές ζημιές. Η Ομάδα Εργασίας του άρθρου 29, στις «κατευθυντήριες γραμμές για την κοινοποίηση παραβίασης δεδομένων κατά τον Κανονισμό 2016/679» εκθέτει ότι οι παραβιάσεις μπορεί να έχουν τρείς κατηγορίες επιπτώσεων στα προσωπικά δεδομένα: την κοινοποίηση, την απώλεια και την τροποποίηση. Εκτός από την υποχρέωση λήψης μέτρων για την ενίσχυση της ασφάλειας της επεξεργασίας, εξίσου σημαντικό είναι να κατοχυρωθεί ότι ο υπεύθυνος επεξεργασίας (Τράπεζα) μπορεί καταλλήλως αλλά και εγκαίρως να αντιμετωπίσει τυχόν παραβιάσεις δεδομένων. [218]
Οι Τράπεζες και τα πιστωτικά ιδρύματα εφαρμόζουν μία δέσμη πολιτικών για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Διενεργούν αξιολογήσεις κινδύνου, όπου εξετάζουν τα αποτελέσματα της συνεχούς παρακολούθησης των απειλών για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται, λαμβάνοντας υπόψη τις τεχνολογικές λύσεις που χρησιμοποιούν, τις υπηρεσίες που αναθέτουν σε εξωτερικούς παρόχους και το τεχνικό περιβάλλον των πελατών. Εξετάζουν τους κινδύνους που συνδέονται με τις επιλεγμένες τεχνολογικές πλατφόρμες, με την

[216] Άρθρο 32 Γ.Κ.Π.Δ, και άρθρο 62 Ν.4624/2019
[217]Handbook on European data protection law, 2018 edition,σελ 171
[218] Σωτηρόπουλος Β.«Υπεύθυνος Προστασίας Δεδομένων Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», Εκδόσεις Σάκκουλα , 2019, σελ.192

αρχιτεκτονική των εφαρμογών, με τις τεχνικές και τις ρουτίνες προγραμματισμού τόσο από τη δική τους πλευρά όσο και από την πλευρά των πελατών τους, καθώς και τα αποτελέσματα της διαδικασίας παρακολούθησης περιστατικών ασφάλειας.[219]

Βάσει των ανωτέρω, τα πιστωτικά ιδρύματα καθορίζουν κατά πόσον και σε ποιο βαθμό ενδέχεται να απαιτούνται αλλαγές στα υπάρχοντα μέτρα ασφάλειας, στις τεχνολογίες που χρησιμοποιούνται και στις διαδικασίες ή τις υπηρεσίες που προσφέρονται. Τα πιστωτικά ιδρύματα λαμβάνουν υπόψη τον χρόνο που απαιτείται για την εφαρμογή των αλλαγών (περιλαμβανομένου του χρόνου της υιοθέτησής τους από τους πελάτες) και λαμβάνουν τα κατάλληλα προσωρινά μέτρα για την ελαχιστοποίηση των περιστατικών ασφάλειας, καθώς και των ενδεχόμενων δυσλειτουργιών.

Τα πιστωτικά ιδρύματα οφείλουν να προβαίνουν σε επανεξέταση των σεναρίων κινδύνου και των υφιστάμενων μέτρων ασφάλειας ύστερα από σημαντικά περιστατικά, πριν από την πραγματοποίηση σημαντικών αλλαγών στην υποδομή ή στις διαδικασίες και μετά τον εντοπισμό νέων απειλών μέσω διαδικασιών παρακολούθησης του κινδύνου. Οφείλουν, επίσης, να εφαρμόζουν μέτρα ασφάλειας τα οποία ενσωματώνουν πολλαπλά επίπεδα ασφάλειας, στο πλαίσιο των οποίων η αποτυχία μίας γραμμής άμυνας αντιμετωπίζεται από την επόμενη γραμμή άμυνας. Εφαρμόζουν δέσμη μέτρων με τα οποία εξασφαλίζεται ότι η φυσική και λογική πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, παρέχεται με εξουσιοδοτήσεις και περιορισμούς βάσει απαιτήσεων εμπορικής λειτουργίας και ασφάλειας.

Κατά τον σχεδιασμό, την ανάπτυξη και τη συντήρηση ψηφιακών υπηρεσιών, τα πιστωτικά ιδρύματα δίνουν ιδιαίτερη προσοχή στον επαρκή διαχωρισμό των καθηκόντων στα περιβάλλοντα τεχνολογίας της πληροφορίας (π.χ. τα περιβάλλοντα ανάπτυξης, δοκιμής και παραγωγής) και στην ορθή εφαρμογή της αρχής των ελάχιστων προνομίων ως βάση για τη χρηστή διαχείριση της ταυτότητας και της πρόσβασης. Κατά το στάδιο αυτό, τα πιστωτικά ιδρύματα διασφαλίζουν ότι η ελαχιστοποίηση των δεδομένων, ήτοι η συλλογή των ελάχιστων αναγκαίων προσωπικών στοιχείων για την εκτέλεση μίας συγκεκριμένης λειτουργίας, συνιστά ουσιώδες στοιχείο της βασικής λειτουργικότητας. Η συλλογή, η δρομολόγηση, η αποθήκευση και η αρχειοθέτηση, καθώς και η απεικόνιση δεδομένων προσωπικού χαρακτήρα διατηρούνται στα απολύτως αναγκαία επίπεδα. [220]

Εφαρμόζουν κατάλληλες λύσεις ασφάλειας για την προστασία των δικτύων, των δικτυακών τόπων, των εξυπηρετητών, των βάσεων δεδομένων και των ζεύξεων επικοινωνίας από περιστατικά κατάχρησης ή από επιθέσεις. Εφαρμόζουν, επίσης, κατάλληλες διαδικασίες παρακολούθησης, ιχνηλασίας

[219] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

[220] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

και περιορισμού της πρόσβασης σε: i) δεδομένα προσωπικού χαρακτήρα, και ii) κρίσιμους λογικούς και φυσικούς πόρους, όπως μεταξύ άλλων δίκτυα, συστήματα, βάσεις δεδομένων, υποσυστήματα ασφάλειας κ.λπ. Τα πιστωτικά ιδρύματα δημιουργούν, αποθηκεύουν και αναλύουν κατάλληλα αρχεία καταγραφής και ίχνη ελέγχου.
Τα μέτρα ασφάλειας για τις ψηφιακές υπηρεσίες υποβάλλονται σε δοκιμές προκειμένου να διασφαλίζεται η ανθεκτικότητα και η αποτελεσματικότητά τους. Όλες οι αλλαγές υπόκεινται σε επίσημη διαδικασία διαχείρισης των αλλαγών που διασφαλίζει ότι οι αλλαγές προγραμματίζονται, υποβάλλονται σε δοκιμές, τεκμηριώνονται και εγκρίνονται δεόντως. Βάσει των αλλαγών που πραγματοποιούνται και των απειλών για την ασφάλεια που παρατηρούνται, οι δοκιμές επαναλαμβάνονται ανά τακτά χρονικά διαστήματα και περιλαμβάνουν σενάρια συναφών, γνωστών πιθανών επιθέσεων.[221]

Προστασία από απόπειρες ηλεκτρονικής υποκλοπής δεδομένων (phising)

Η Τράπεζα οφείλει να μεριμνά για την προστασία της πελατείας της από κακόβουλες ενέργειες τρίτων. Ενδεικτικά αναφέρεται η απόπειρα ηλεκτρονικής υποκλοπής των στοιχείων των πελατών. Στα εναλλακτικά δίκτυα που έχει στην διάθεσή της, φροντίζει να δίνονται σαφείς οδηγίες για την προφύλαξή των προσωπικών δεδομένων τους στους χρήστες και εφιστά την προσοχή τους στις συνήθεις μεθόδους που χρησιμοποιούνται για την υποκλοπή των στοιχείων τους, καθώς και για τους κινδύνους που απορρέουν από το phising. Συνήθως η εκάστοτε Τράπεζα επισημαίνει ρητώς ότι σε καμία περίπτωση δεν ζητά προσωπικά δεδομένα των πελατών της μέσω ηλεκτρονικού ταχυδρομείου και οποιοδήποτε μήνυμα έχει τέτοιο περιεχόμενο θα πρέπει να διαγράφεται και να ακολουθεί σχετική ενημέρωση για το περιστατικό από τον πελάτη προς την Τράπεζα.

2.6 Ειδικά Θέματα

2.6.1 Κλειστά κυκλώματα τηλεόρασης και καταγραφή τηλεφωνικών συνδιαλέξεων για λόγους ασφαλείας

Σύμφωνα με το ισχύον κανονιστικό πλαίσιο, η Τράπεζα, δύναται να τοποθετεί στις εγκαταστάσεις της κλειστά κυκλώματα τηλεόρασης με σκοπούς την πρόληψη κλοπής αγαθών, την αποτροπή εγκληματικών ενεργειών , την προστασία του συναλλακτικού κοινού και την ασφάλεια του προσωπικού. Τα δεδομένα που συλλέγονται από τα εν λόγω κυκλώματα, τηρούνται και φυλάσσονται σύμφωνα με τις διατάξεις του Γενικού Κανονισμού.
Επιπλέον, σύμφωνα με το ισχύον θεσμικό πλαίσιο, και κατόπιν ειδικής

[221] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.

ενημέρωσης των πελατών για καταγραφή των συνδιαλέξεων, η Τράπεζα δύναται να χρησιμοποιεί τεχνικά μέσα καταγραφής διαλόγων με πελάτες στα πλαίσια εξυπηρέτησης των συναλλαγών που διενεργούν με συγκεκριμένες υπηρεσίες της.
Όταν το υποκείμενο των δεδομένων ασκεί το δικαίωμα πρόσβασης για δεδομένα του που τηρούνται σε σύστημα βιντεοεπιτήρησης, οφείλει να υποδείξει την ακριβή ώρα και τον τόπο που ευρέθη στην εμβέλεια των καμερών. Το δε πιστωτικό ίδρυμα ανταποκρινόμενο χορηγεί αντίγραφο του τμήματος της εγγραφής σήματος εικόνας όπου έχει καταγραφεί το υποκείμενο των δεδομένων ή έντυπη σειρά στιγμιότυπων από τις καταγεγραμμένες εικόνες ή ενημερώνει εγγράφως το ενδιαφερόμενο πρόσωπο είτε ότι δεν απεικονίζεται είτε ότι το σχετικό τμήμα τη εγγραφής έχει καταστραφεί, εφόσον έχει παρέλθει ο κατά νόμο χρόνος τήρησης. Εναλλακτικά, εφόσον συμφωνεί και το υποκείμενο των δεδομένων, το πιστωτικό ίδρυμα μπορεί απλώς να επιδείξει το ανωτέρω τμήμα. Όταν χορηγεί αντίγραφο εικόνας, το πιστωτικό ίδρυμα οφείλει να καλύπτει την εικόνα τρίτων προσώπων (π.χ. με θόλωση τμήματος της εικόνας), εφόσον ενδέχεται να παραβιάζεται το δικαίωμά τους στην ιδιωτική ζωή. Στην περίπτωση της απλής επίδειξης, η κάλυψη της εικόνας τρίτων προσώπων δεν είναι αναγκαία.
1 Όταν το υποκείμενο των δεδομένων ασκεί το δικαίωμα πρόσβασης για δεδομένα μαγνητοφωνημένης επικοινωνίας του με το πιστωτικό ίδρυμα, αυτό παρέχει στο υποκείμενο την απομαγνητοφωνημένη συνομιλία, εκτός εάν δεν υπάρχει τέτοια ή έχει καταστραφεί εφόσον έχει παρέλθει ο κατά νόμο χρόνος τήρησης, οπότε ενημερώνει σχετικά τον αιτούντα.[222]

2.6.2 Παροχή Ηλεκτρονικών Υπηρεσιών

Στους πελάτες της, που είναι χρήστες των ηλεκτρονικών της υπηρεσιών, η Τράπεζα γνωστοποιεί ότι συλλέγει προσωπικά δεδομένα (αποκλειστικά εφόσον οι ίδιοι οι χρήστες τα παρέχουν εκουσίως) με σκοπό την παροχή υπηρεσιών που είναι διαθέσιμες ηλεκτρονικά. Τα προσωπικά δεδομένα που συλλέγονται στην ιστοσελίδα της εκάστοτε Τράπεζας, εξαρτώνται από την υπηρεσία, την οποία αιτείται ο πελάτης, και συνήθως περιορίζονται στα δεδομένα που απαριθμούνται παρακάτω: ονοματεπώνυμο, πατρώνυμο, αριθμός ταυτότητας, ημερομηνία γέννησης, ηλικία, φύλο, επαγγελματική ιδιότητα, Α.Φ.Μ, μορφωτικό επίπεδο, διεύθυνση κατοικίας, αριθμοί τηλεφωνικής επικοινωνίας, e-mail.
Το σύνολο ή τμήμα των παραπάνω στοιχείων, που παρέχονται από τον πελάτη στην Τράπεζα είναι δυνατόν να τύχει επεξεργασίας, με σκοπό την παροχή

[222] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019.άρθρο 19.6 και19.7

υπηρεσιών που είναι διαθέσιμες ηλεκτρονικά καθώς επίσης και για στατιστικούς λόγους, και για σκοπούς βελτίωσης των παρεχόμενων υπηρεσιών.
Η Τράπεζα οφείλει να διευκρινίζει ότι για τα links που περιλαμβάνονται στην ιστοσελίδα της, δεν φέρει ουδεμία ευθύνη για την προστασία των προσωπικών δεδομένων στις ιστοσελίδες που αυτά τα links οδηγούν. Επίσης, θα πρέπει να γίνεται ειδική αναφορά στην συλλογή στοιχείων από τους χρήστες μέσω των cookies και την παρακολούθηση διευθύνσεων πρωτοκόλλου Internet (IP). Τα cookies είναι μικρά αρχεία κειμένου που αποθηκεύονται στο σκληρό δίσκο κάθε χρήστη και χρησιμοποιούνται είτε προς διευκόλυνση της πρόσβασης του χρήστη σε συγκεκριμένες υπηρεσίες ή προϊόντα, είτε για στατιστικούς λόγους, είτε προς αναγνώριση περιοχών που είναι χρήσιμες ή δημοφιλείς, χωρίς όμως να λαμβάνουν γνώση οποιουδήποτε εγγράφου ή αρχείου από τον υπολογιστή του χρήστη. Πρέπει να παρέχεται στον χρήστη επιλογή, ώστε να ρυθμίσει τον browser προκειμένου είτε να τον προειδοποιεί για την χρήση cookies σε συγκεκριμένες υπηρεσίες, είτε να μην επιτρέπει την αποδοχή της χρήσης cookies σε καμία περίπτωση. Θα πρέπει παράλληλα να διευκρινίζεται στον πελάτη, ότι σε περίπτωση που δεν επιτρέψει την χρήση cookies για την αναγνώριση του, πιθανώς να καταστεί αδύνατη η παροχή ορισμένων υπηρεσιών από την Τράπεζα (πχ πραγματοποίηση συναλλαγών Internet Banking) ή να μην του παρασχεθεί δυνατότητα λήψης πληροφοριών που ενδέχεται να τον αφορούν.
Η εκάστοτε Τράπεζα μπορεί να αξιοποιήσει επιπλέον τις δυνατότητες που παρέχονται μέσω του google analytics, και ειδικότερα του display advertising αξιοποιώντας τα χαρακτηριστικά του επαναληπτικού marketing (remarketing). Με το εργαλείο αυτό δύναται να προωθήσει προϊόντα και υπηρεσίες της στο διαδίκτυο, πάντα υπό την αίρεση ότι οι επισκέπτες της ιστοσελίδας της τράπεζας έχουν την επιλογή να αποκλείσουν ή να διακόψουν την αποδοχή σχετικών μηνυμάτων καθώς και να εξαιρεθούν μελλοντικά από σχετικές ενέργειες (στο πλαίσιο της προσαρμογής των διαφημίσεων που λαμβάνουν).

3 Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων.

3.1 Ο θεσμός του Υπευθύνου Προστασίας Προσωπικών Δεδομένων

Οι Υπεύθυνοι Προστασίας Δεδομένων αποτελούν βασική συνιστώσα του νέου συστήματος διακυβέρνησης προσωπικών δεδομένων.[223] Με την Οδηγία (Ε.Ε.) 2016/680, η οποία ενσωματώθηκε στο εθνικό δίκαιο με το Ν.4624/2019, καθώς και με το Γενικό Κανονισμό Προστασίας Δεδομένων της Ε.Ε. 679/2016 ο θεσμός του Υπευθύνου Προστασίας Δεδομένων (Υ.Π.Δ.) έγινε υποχρεωτικός για τις δημόσιες αρχές και τους δημόσιους φορείς(ανεξαρτήτως του είδους δεδομένων που επεξεργάζονται), καθώς και

[223] Δελτίο Τύπου . Γ/ΕΞ/568 της 23.01.2020 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

για πληθος εταιριών του ιδιωτικού τομέα, που ενεργούν ως υπεύθυνοι επεξεργασίαςκαι ως εκτελούντες την επεξεργασία. Η υποχρέωση αυτή, σύμφωνα με το άρθρο 37 παράγραφος 1 του Γενικού Κανονισμού Προστασίας Δεδομένων, ισχύει για τις εταιρίες και οργανισμούς του ιδιωτικού τομέα που έχουν ως κύρια δραστηριότητα τη συστηματική παρακολούθηση φυσικών προσώπων σε μεγάλη κλίμακα, ή την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα σε μεγάλη κλίμακα.[224]

Σύμφωνα με το άρθρο 37 παράγραφος 4 του Γενικού Κανονισμού Προστασίας Δεδομένων, το δίκαιο της Ένωσης ή των κρατών μελών είναι δυνατό να επιβάλλει τον ορισμό υπευθύνου προστασίας δεδομένων και σε άλλες περιπτώσεις.

Εκτός από τις περιπτώσεις όπου είναι προφανές ότι ένας οργανισμός δεν υποχρεούται να ορίσει υπεύθυνο προστασίας δεδομένων, η ομάδα του άρθρου 29 συνιστά[225] στους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να καταγράφουν την εσωτερική ανάλυση που διενεργούν προκειμένου να προσδιορίσουν αν πρέπει ή όχι να διοριστεί υπεύθυνος προστασίας δεδομένων, ώστε να μπορούν να αποδείξουν ότι λήφθηκαν δεόντως υπόψη οι σχετικοί παράγοντες. Η εν λόγω ανάλυση αποτελεί μέρος της απαιτούμενης τεκμηρίωσης δυνάμει της αρχής της λογοδοσίας. Μπορεί να ζητηθεί από την εποπτική αρχή και θα πρέπει να επικαιροποιείται όταν κρίνεται απαραίτητο, για παράδειγμα αν οι υπεύθυνοι επεξεργασίας ή οι εκτελούντες την επεξεργασία αναλαμβάνουν νέες δραστηριότητες ή παρέχουν νέες υπηρεσίες που εμπίπτουν ενδεχομένως στις περιπτώσεις του άρθρου 37 παρ.1 του Γενικού Κανονισμού Προστασίας Δεδομένων.

Επίσης, εκτός από τις περιπτώσεις που ο Γενικός Κανονισμός Προστασίας Δεδομένων απαιτεί ρητώς τον ορισμό υπευθύνου προστασίας δεδομένων, υπάρχουν περιπτώσεις ιδιωτικών εταιριών ή Οργανισμών που κρίνουν σκόπιμο να ορίσουν υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση.

Η ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29[226]ενθάρρυνε τέτοιου είδους

[224]Σύμφωνα με το άρθρο 37 παράγραφος 1 του Γενικού Κανονισμού Προστασίας Δεδομένων, ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός σε τρεις συγκεκριμένες περιπτώσεις : α) όταν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα β) όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή γ) όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

[225]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.7

[226]Η επονομαζόμενη «Ομάδα Εργασίας του άρθρου 29» συστάθηκε βάσει του άρθρου 29 της Οδηγίας 95/46/ΕΚ και είχε ως τακτικά μέλη τους προέδρους ή εκπροσώπους των Αρχών Προστασίας Προσωπικών Δεδομένων των 28 κρατών μελών της Ευρωπαϊκής Ένωσης, εκπρόσωπο του Ευρωπαίου Επόπτη Προστασίας Δεδομένων και εκπρόσωπο της Ευρωπαϊκής Επιτροπής. Είναι η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως τις 25 Μαΐου 2018 (έναρξη ισχύος του ΓΚΠΔ), οπότε και

εθελοντικές ενέργειες, με το σκεπτικό ότι ο ορισμός του μπορεί να διευκολύνει τη συμμόρφωση και επιπλέον να αποτελέσει ανταγωνιστικό πλεονέκτημα για τις επιχειρήσεις. Εκτός από τον ρόλο που έχουν σε επίπεδο συμμόρφωσης μέσω της εφαρμογής εργαλείων λογοδοσίας (όπως διευκόλυνση διενέργειας εκτιμήσεων αντικτύπου σχετικά με την προστασία των δεδομένων και διενέργεια ή διευκόλυνση διενέργειας ελέγχων), οι υπεύθυνοι προστασίας δεδομένων ενεργούν και ως μεσολαβητές μεταξύ των διαφόρων ενδιαφερομένων (π.χ., εποπτικές αρχές, υποκείμενα των δεδομένων και επιχειρησιακές μονάδες του ίδιου οργανισμού).[227] Όταν ένας οργανισμός ορίζει υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση, σε σχέση με τον ορισμό, τη θέση και τα καθήκοντά του θα ισχύουν οι απαιτήσεις των άρθρων 37 έως 39 του Γενικού κανονισμού προστασίας Δεδομένων ωσάν ο ορισμός να ήταν υποχρεωτικός.

Οι οργανισμοί που δεν υποχρεούνται, βάσει της νομοθεσίας, να ορίσουν υπεύθυνο προστασίας δεδομένων και που δεν επιθυμούν να ορίσουν υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση μπορούν κάλλιστα να απασχολούν υπαλλήλους ή εξωτερικούς συμβούλους επιφορτισμένους με καθήκοντα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Σ’ αυτές τις περιπτώσεις, είναι σημαντικό να διασφαλίζεται ότι δεν υπάρχει σύγχυση ως προς τον τίτλο, το καθεστώς, τη θέση και τα καθήκοντα των εν λόγω υπαλλήλων ή συμβούλων. Θα πρέπει, επομένως, να διευκρινίζεται, τόσο στο πλαίσιο της ενδοεταιρικής επικοινωνίας, όσο και στις αρχές προστασίας δεδομένων, τα υποκείμενα των δεδομένων και το ευρύ κοινό, ότι ο εν λόγω υπάλληλος ή σύμβουλος δεν φέρει τον τίτλο του Υπευθύνου Προστασίας Δεδομένων[228].

Οι τράπεζες και τα πιστωτικά ιδρύματα υποχρεούνται από το Γενικό Κανονισμό Προστασίας Δεδομένων να ορίσουν Υπεύθυνο Προστασίας Δεδομένων, καθώς για την άσκηση της δραστηριότητάς τους απαιτείται τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, και αναφέρονται ρητώς από την Ομάδα του Άρθρου 29[229](ως παράδειγμα επεξεργασίας σε μεγάλη κλίμακα), με επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε εθνικό

αντικαταστάθηκε από το Ευρωπαϊκό Συμβούλιο προστασίας δεδομένων
http://ec.europa.eu/newsroom/article29/news.cfm?item_ type=1360

[227]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων: σελ.6

[228]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.7

[229]«Παραδείγματα επεξεργασίας σε μεγάλη κλίμακα είναι, μεταξύ άλλων, τα ακόλουθα: … η επεξεργασία δεδομένων πελατών στο πλαίσιο της συνήθους λειτουργίας μιας ασφαλιστικής εταιρείας ή μιας τράπεζας», Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.11

επίπεδο[230].

Η έννοια της τακτικής και συστηματικής παρακολούθησης των υποκειμένων των δεδομένων δεν ορίζεται μεν στον Γενικό Κανονισμό Προστασίας Δεδομένων, όμως στην αιτιολογική σκέψη 24 του Γενικού Κανονισμού αναφέρεται η έννοια της «παρακολούθησης της συμπεριφοράς των υποκειμένων των δεδομένων» στην οποία περιλαμβάνονται ξεκάθαρα όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο.

Η ομάδα του άρθρου 29 δίνει[231] στο επίθετο «τακτική» μία ή περισσότερες από τις ακόλουθες ερμηνείες: παρακολούθηση λαμβάνουσα χώρα σε συνεχή βάση ή σε συγκεκριμένα χρονικά διαστήματα για συγκεκριμένη χρονική περίοδο,λαμβάνουσα χώρα τακτικά ή κατ' επανάληψη σε σταθερές χρονικές στιγμές είτε λαμβάνουσα χώρα αδιαλείπτως ή περιοδικά.

Αντιστοίχως, δίνεται στο επίθετο «συστηματική» μία ή περισσότερες από τις ακόλουθες ερμηνείες: παρακολούθηση λαμβάνουσα χώρα σύμφωνα με κάποιο σύστημα, προκαθορισμένη, οργανωμένη ή μεθοδική, είτε λαμβάνουσα χώρα στο πλαίσιο γενικότερου σχεδίου για τη συλλογή δεδομένων, είτε διενεργούμενη στο πλαίσιο στρατηγικής. Ως παραδείγματα δραστηριοτήτων που συνιστούν ενδεχομένως τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων αναφέρονται ενδεικτικά οι δραστηριότητες μάρκετινγκ βάσει δεδομένων, η διαμόρφωση προφίλ και η βαθμολόγηση για σκοπούς εκτίμησης κινδύνου (π.χ. για σκοπούς βαθμολόγησης πιστοληπτικής ικανότητας, προσδιορισμού ασφαλίστρων, καταπολέμησης της απάτης, εντοπισμού πρακτικών νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες), ο εντοπισμός θέσης, για παράδειγμα, μέσω εφαρμογών για κινητά τηλέφωνα, τα προγράμματα επιβράβευσης αφοσιωμένων πελατών.

Στο πλαίσιο άσκησης της τραπεζικής δραστηριότητας συναντώνται οι περισσότερες από τις προαναφερόμενες πράξεις. Γίνεται επεξεργασία των δεδομένων των πελατών για την επιδίωξη διασταυρούμενων πωλήσεων και ενεργειών προώθησης περεταίρω προϊόντων (π.χ. τραπεζοασφαλιστικών προγραμμάτων). Η διαμόρφωση προφίλ και η βαθμολόγηση για σκοπούς εκτίμησης κινδύνων επίσης λαμβάνει χώρα στις Τράπεζες για όλους τους σκοπούς που προαναφέρθηκαν. Εφαρμογές για φορητές συσκευές και κινητά τηλέφωνα διατίθενται πλέον από όλες τις ελληνικές Τράπεζες στο πλαίσιο απομακρυσμένης παροχής τραπεζικών υπηρεσιών (ηλεκτρονική τραπεζική) και έχουν υιοθετηθεί επίσης και προγράμματα επιβράβευσης αφοσιωμένων πελατών Τραπεζών για τη χρήση εναλλακτικών δικτύων (π.χ. χρήση χρεωστικής κάρτας αντί μετρητών στις αγορές). Όλες οι προαναφερόμενες

[230]Άρθρο 37 παρ.1β σε συνδυασμό με την Αιτιολογική σκέψη 24 και την Αιτιολογική σκέψη 91 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[231]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.11-12

πράξεις μπορούν να θεωρηθούν «βασικές δραστηριότητες» του άρθρου 37, παρ. 1 του Γενικού Κανονισμού Προστασίας Δεδομένων της Ε.Ε. 679/201, ως καίριες πράξεις που είναι αναγκαίες για την επίτευξη των στόχων της Τράπεζας - υπευθύνου επεξεργασίας ή των συνεργαζομένων εταιριών-εκτελούντων την επεξεργασία.

Σε συμμόρφωση με την προαναφερθείσα υποχρέωσή τους, οι Τράπεζες, ως υπεύθυνοι επεξεργασίας, σύμφωνα με το άρθρο 37 παρ.7 του Γενικού Κανονισμού Προστασίας Δεδομένων πρέπει να δημοσιεύουν[232] τα στοιχεία επικοινωνίας του Υπευθύνου Προστασίας Δεδομένων και να ανακοινώνουν στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα τον ορισμό και κάθε μελλοντική αντικατάσταση του.[233]Ο στόχος αυτών των απαιτήσεων είναι να διασφαλιστεί η εύκολη και απευθείας επικοινωνία των υποκειμένων των δεδομένων (τόσο εντός όσο και εκτός του οργανισμού) και των εποπτικών αρχών με τον υπεύθυνο προστασίας δεδομένων χωρίς να απαιτείται επικοινωνία με άλλο τμήμα του οργανισμού. Εξίσου σημαντική είναι και η παράμετρος της εμπιστευτικότητας. Για παράδειγμα, οι εργαζόμενοι μπορεί να διστάζουν να υποβάλουν καταγγελία στον υπεύθυνο προστασίας δεδομένων αν δεν διασφαλίζεται το απόρρητο των επικοινωνιών τους. Ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους, σύμφωνα με το άρθρο 38 παρ. 5 του Γενικού Κανονισμού Προστασίας Δεδομένων. Στα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων θα πρέπει να περιλαμβάνονται πληροφορίες που διευκολύνουν την επικοινωνία των υποκειμένων των δεδομένων και των εποπτικών αρχών μαζί του (ταχυδρομική διεύθυνση, συγκεκριμένος τηλεφωνικός αριθμός και συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου). Εφόσον ενδείκνυται, για σκοπούς επικοινωνίας με το κοινό, θα μπορούσαν να παρέχονται και άλλα μέσα επικοινωνίας όπως ειδική ανοικτή τηλεφωνική γραμμή ή ειδικό έντυπο επικοινωνίας υπ’ όψιν του υπευθύνου προστασίας δεδομένων στον δικτυακό τόπο του οργανισμού. Το άρθρο 37 παράγραφος 7 δεν απαιτεί τη συμπερίληψη του ονόματος του υπευθύνου προστασίας δεδομένων στα στοιχεία επικοινωνίας που δημοσιεύονται. Μολονότι η δημοσίευση του ονόματος θα μπορούσε να αποτελέσει ορθή πρακτική, είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και του υπευθύνου προστασίας δεδομένων να αποφασίζουν εάν είναι αναγκαία ή σκόπιμη, ανάλογα με τις ιδιαιτερότητες κάθε περίπτωσης . Η ανακοίνωση, πάντως, του ονόματος του υπευθύνου προστασίας δεδομένων στην εποπτική αρχή είναι καίριας σημασίας προκειμένου ο υπεύθυνος προστασίας δεδομένων να

[232]Άρθρο 32 παρ.4 της Οδηγίας (Ε.Ε.) 2016/680

[233] https://www.dpa.gr/el/foreis/dpo_upef/orismos_DPO

ενεργεί ως σημείο επικοινωνίας ανάμεσα στον οργανισμό και την εποπτική αρχή, σύμφωνα με το άρθρο 39 παρ.1 ε' του Γενικού Κανονισμού Προστασίας Δεδομένων.[234]

3.2 Προσόντα

Στο άρθρο 37 παρ.5 του Γενικού Κανονισμού Προστασίας Δεδομένων ορίζεταιότι «ο Υπεύθυνος Προστασίας Δεδομένων διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39 του Γενικού Κανονισμού Προστασίας Δεδομένων».

Στην αιτιολογική σκέψη 97 του Γενικού Κανονισμού Προστασίας Δεδομένων αναφέρεται ότι το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία.

Αν και το απαιτούμενο επίπεδο εμπειρογνωμοσύνης δεν καθορίζεται αυστηρά, σε κάθε περίπτωση πρέπει να είναι ανάλογο της ευαισθησίας, της πολυπλοκότητας και της ποσότητας των δεδομένων που επεξεργάζεται ο οργανισμός. Για παράδειγμα, όταν μια δραστηριότητα επεξεργασίας δεδομένων είναι ιδιαίτερα πολύπλοκη, ή όταν εμπλέκεται μεγάλος όγκος ευαίσθητων δεδομένων, ο υπεύθυνος προστασίας δεδομένων είναι πιθανό να χρειάζεται υψηλότερο επίπεδο εμπειρογνωμοσύνης και υποστήριξης. Διαφορά υπάρχει επίσης και όταν ο οργανισμός διαβιβάζει συστηματικά δεδομένα προσωπικού χαρακτήρα εκτός της Ευρωπαϊκής Ένωσης ή όταν οι διαβιβάσεις αυτές είναι περιστασιακές. Ο υπεύθυνος προστασίας δεδομένων θα πρέπει επομένως να επιλέγεται προσεκτικά, λαμβάνοντας δεόντως υπόψη τα ζητήματα προστασίας δεδομένων που ανακύπτουν στο εσωτερικό του οργανισμού. Μολονότι το άρθρο 37 παράγραφος 5 δεν προσδιορίζει τα επαγγελματικά προσόντα που θα πρέπει να λαμβάνονται υπόψη κατά τον ορισμό του υπευθύνου προστασίας δεδομένων, ο τελευταίος πρέπει να διαθέτει εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, τόσο σε εθνικό όσο και ευρωπαϊκό επίπεδο, και επιπλέον να έχει άριστη γνώση του Γενικού Κανονισμού Προστασίας Δεδομένων. Χρήσιμη θεωρείται δε η γνώση του τομέα δραστηριότητας καθώς και του οργανισμού του υπευθύνου επεξεργασίας. Ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει καλή γνώση των πράξεων επεξεργασίας που διενεργούνται, καθώς και των τομέα των τεχνολογιών και

[234]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.17

των συστημάτων πληροφορικής, και των αναγκών του υπευθύνου επεξεργασίας σε επίπεδο ασφάλειας και προστασίας των δεδομένων. Η ικανότητα εκπλήρωσης των καθηκόντων που βαρύνουν τον υπεύθυνο προστασίας δεδομένων θα πρέπει να ερμηνεύεται τόσο σε σχέση με τις προσωπικές ικανότητες και γνώσεις του, όσο και με τη θέση που κατέχει εντός του οργανισμού. Στις προσωπικές ικανότητες θα πρέπει να περιλαμβάνονται, μεταξύ άλλων, η ακεραιότητα και το υψηλό αίσθημα επαγγελματικής δεοντολογίας, ενώ πρωταρχικό μέλημα του υπευθύνου προστασίας δεδομένων θα πρέπει να είναι η μέγιστη δυνατή συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων. Ο υπεύθυνος προστασίας δεδομένων διαδραματίζει καίριο ρόλο στην ανάπτυξη νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού και συμβάλλει στην εφαρμογή ουσιωδών στοιχείων του Γενικού Κανονισμού Προστασίας Δεδομένων, όπως οι αρχές της επεξεργασίας δεδομένων, τα δικαιώματα των υποκειμένων των δεδομένων, η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, τα αρχεία των δραστηριοτήτων επεξεργασίας, η ασφάλεια των δεδομένων προσωπικού χαρακτήρα, και η γνωστοποίηση και ανακοίνωση παραβίασης δεδομένων. [235]

Ο Υπεύθυνος Προστασίας δεδομένων μιας Τράπεζας πρέπει εκτός από άριστη γνώση του Κανονισμού, και την ουσιαστική γνώση και εμπειρία στο δίκαιο και τις πρακτικές για την προστασία των προσωπικών δεδομένων να διαθέται και καλή γνώση της λειτουργίας των πιστωτικών ιδρυμάτων, των πράξεων επεξεργασίας που αυτά διενεργούν, καθώς και των συστημάτων πληροφορικής και των ειδικών αναγκών ασφαλείας. Όπως ισχύοι για όλους τους Υπεύθυνους Προστασίας Δεδομένων θα πρέπει να χαρακτηρίζεται από επαγγελματική και προσωπική ακεραιότητα, υψηλό αίσθημα επαγγελματικής δεοντολογίας και ικανότητα εκπλήρωσης των προβλεπόμενων στον Κανονισμό καθηκόντων του, με την ανάλογη θεσμική θωράκιση. Τα πιστωτικά ιδρύματα παρέχουν στους ΥΠΔ τους απαραίτητους πόρους για την άσκηση των καθηκόντων τους και λαμβάνουν ιδιαίτερη μέριμνα για την πλήρη και έγκαιρη ενημέρωσή τους για κάθε θέμα που αφορά σε επεξεργασία προσωπικών δεδομένων, όπως πχ. σχεδιασμός προϊόντος ή υπηρεσίας που απευθύνεται (και) σε φυσικά πρόσωπα.[236]

3.3 Θέση του Υπευθύνου Προστασίας Δεδομένων

Υπάρχει πληθώρα διατάξεων, με τις οποίες κατοχυρώνεται ο ρόλος / η θέση του Υπευθύνου Προστασίας Δεδομένων, παρέχοντας ένα επίπεδο προστασίας για το κύρος και την υπόστασή του μέσα στην οντότητα που έχει οριστεί για

[235]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.15-16

[236] Ελληνική Ένωση Τραπεζών, «Κώδικας Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα», Σχέδιο 16.1.2019., άρθρο 29

να προστατεύει τα προσωπικά δεδομένα.[237]

Στο άρθρο 33 της Οδηγίας (Ε.Ε.) 2016/680 γίνεται πρόβλεψη των δεσμευτικών εγγυήσεων για τη θέση του Υπευθύνου Προστασίας Δεδομένων, ώστε να θωρακιστεί με τις απαραίτητες εξασφαλίσεις που θα του επιτρέψουν να ασκήσει το έργο του. Προβλέπεται ότι ο υπεύθυνος επεξεργασίας διασφαλίζει ότι ο Υπεύθυνος Προστασίας Δεδομένων συμμετέχει δεόντως και εγκαίρως σε όλα τα ζητήματα τα οποία σχετίζονται μετην προστασία δεδομένων προσωπικού χαρακτήρα και υποστηρίζειτον Υπεύθυνο Προστασίας Δεδομένων στην άσκηση των καθηκόντων του, παρέχοντάς του τους αναγκαίους πόρους για την εκτέλεση των καθηκόντων αυτών και την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και για τη διατήρηση της εμπειρογνωμοσύνης του.

Αντίστοιχα, στο άρθρο 38 παρ 1 και 2 του Γενικού Κανονισμού Προστασίας Δεδομένων επαναλαμβάνονται οι προαναφερθείσες εγγυήσεις με την προσθήκη και του υπευθύνου επεξεργασίας στο ρόλο του υπόχρεου σε υποστήριξη του Υπευθύνου Προστασίας Δεδομένων. Ανάλογα με το ποιος πληροί τα κριτήρια περί υποχρεωτικού ορισμού, σε κάποιες περιπτώσεις η υποχρέωση ορισμού υπευθύνου προστασίας δεδομένων βαρύνει μόνο τον υπεύθυνο επεξεργασίας ή μόνο τον εκτελούντα την επεξεργασία, ενώ σε άλλες περιπτώσεις αμφότερους τον υπεύθυνο επεξεργασίας και τον δικό του εκτελούντα την επεξεργασία (στην πορεία θα πρέπει να συνεργάζονται όλοι μεταξύ τους)[238].

Δέουσα και έγκαιρη συμμετοχή σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία θα πρέπει να διασφαλίζουν ότι ο Υπεύθυνος Προστασίας Δεδομένων συμμετέχει δεόντως και εγκαίρως σε όλα τα ζητήματα , τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το Άρθρο 38, παρ.1 του Γενικού Κανονισμού Προστασίας Δικαιωμάτων Ε.Ε. 679/2016. Η ενημέρωση του Υπευθύνου Προστασίας Δεδομένων και η διαβούλευση μαζί του από το αρχικό κιόλας στάδιο θα διευκολύνουν τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων και θα προωθήσουν την προσέγγιση της προστασίας της ιδιωτικής ζωής ήδη από το στάδιο του σχεδιασμού. Θα πρέπει, επομένως, να αποτελούν συνήθη διαδικασία στο πλαίσιο της διακυβέρνησης του οργανισμού. Σημαντικό είναι επίσης ο υπεύθυνος προστασίας δεδομένων να αντιμετωπίζεται ως συνομιλητής στους κόλπους του οργανισμού και να συμμετέχει στις ομάδες εργασίας που ασχολούνται με δραστηριότητες επεξεργασίας δεδομένων εντός του οργανισμού.

---

[237] Σωτηρόπουλος Β., Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα, εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019 : 311σελ

[238] Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.13

Συνεπώς, ο οργανισμός, ως υπεύθυνος επεξεργασίας, θα πρέπει να διασφαλίζει, ενδεικτικά, τις παρακάτω ενέργειες. Να καλείται ο Υπεύθυνος Προστασίας Δεδομένων να συμμετέχει τακτικά στις συσκέψεις των ανώτερων και μεσαίων στελεχών της διοίκησης. Να είναι παρών όταν λαμβάνονται αποφάσεις που έχουν επιπτώσεις στην προστασία δεδομένων. Όλες οι σχετικές πληροφορίες πρέπει να διαβιβάζονται εγκαίρως στον υπεύθυνο προστασίας δεδομένων ώστε να είναι σε θέση να παράσχει κατάλληλες συμβουλές. Πρέπει να δίδεται πάντοτε η δέουσα βαρύτητα στη γνώμη του υπευθύνου προστασίας δεδομένων. Σε περίπτωση διαφωνίας, η ομάδα του άρθρου 29 συνιστά, ως ορθή πρακτική, να καταγράφονται οι λόγοι για τους οποίους δεν ακολουθήθηκαν οι συμβουλές του υπευθύνου προστασίας δεδομένων. Να ζητείται απαραιτήτως άμεσα η γνώμη του υπευθύνου προστασίας δεδομένων σε περίπτωση παραβίασης δεδομένων ή άλλου σχετικού συμβάντος. Κατά περίπτωση, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα μπορούσαν επίσης να αναπτύξουν κατευθυντήριες γραμμές ή προγράμματα για την προστασία των δεδομένων όπου θα αναφέρεται συγκεκριμένα σε ποιες περιπτώσεις πρέπει να ζητείται η γνώμη του υπευθύνου προστασίας δεδομένων.[239]

Παροχή πόρων και πρόσβαση στα δεδομένα.

Σύμφωνα με το άρθρο 38 παράγραφος 2 του ΓΚΠΔ, ο οργανισμός στηρίζει τον υπεύθυνο προστασίας δεδομένων του «παρέχοντας απαραίτητους πόρους για την άσκηση των καθηκόντων [του] και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του». Αναλόγως της φύσης των πράξεων επεξεργασίας και των δραστηριοτήτων και του μεγέθους του οργανισμού, ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει στη διάθεσή του τους ακόλουθους πόρους: Ενεργή στήριξη του υπευθύνου προστασίας δεδομένων από τα ανώτερα διοικητικά στελέχη(π.χ. σε επίπεδο διοικητικού συμβουλίου). Επάρκεια χρόνου ώστε να μπορούν οι υπεύθυνοι προστασίας δεδομένων να επιτελούν τα καθήκοντά τους. Αυτό είναι ιδιαίτερα σημαντικό όταν ο ορισθείς εσωτερικός υπεύθυνος προστασίας δεδομένων τελεί υπό καθεστώς μερικής απασχόλησης ή όταν ο εξωτερικός υπεύθυνος προστασίας δεδομένων ασχολείται με την προστασία των δεδομένων επιπλέον των λοιπών καθηκόντων που επιτελεί. Ειδάλλως, οι αντικρουόμενες προτεραιότητες του υπευθύνου προστασίας δεδομένων ενδέχεται να έχουν ως συνέπεια την παραμέληση των καθηκόντων του. Η εξασφάλιση επαρκούς χρόνου είναι μείζονος σημασίας προκειμένου να μπορεί ο υπεύθυνος προστασίας δεδομένων να ασχολείται απερίσπαστος με τα καθήκοντά του. Συνιστά ορθή πρακτική να ορίζεται συγκεκριμένο ποσοστό χρόνου ενασχόλησης με τα καθήκοντα του υπευθύνου προστασίας δεδομένων όταν

[239]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.18

δεν επιτελούνται υπό καθεστώς πλήρους απασχόλησης. Ορθές πρακτικές είναι επίσης ο καθορισμός του χρόνου που απαιτείται για την επιτέλεση των καθηκόντων του υπευθύνου προστασίας δεδομένων, η ιεράρχηση των εν λόγω καθηκόντων κατά σειρά προτεραιότητας και ο προσδιορισμός του χρόνου που χρειάζεται ο υπεύθυνος προστασίας δεδομένων (ή ο οργανισμός) για να καταρτίσει σχέδιο εργασίας. Προσήκουσα στήριξη σε επίπεδο οικονομικών πόρων, υποδομών (χώρων, εγκαταστάσεων, εξοπλισμού) και προσωπικού, κατά περίπτωση. Επίσημη ανακοίνωση του ορισμού του υπευθύνου προστασίας δεδομένων σε όλο το προσωπικό ώστε να διασφαλιστεί ότι η ύπαρξη και τα καθήκοντά του είναι γνωστά σε όλον τον οργανισμό. Απαραίτητη πρόσβαση σε άλλα τμήματα, όπως το τμήμα ανθρωπίνων πόρων, το τμήμα ασφάλειας, το νομικό τμήμα, το τμήμα πληροφορικής κ.λπ., ώστε οι υπεύθυνοι προστασίας δεδομένων να μπορούν να λαμβάνουν ουσιαστική στήριξη, συνδρομή και πληροφόρηση απ' αυτά. Συνεχής κατάρτιση. Πρέπει να δίδεται στους υπεύθυνους προστασίας δεδομένων η ευκαιρία να παρακολουθούν τις εξελίξεις στον τομέα της προστασίας των δεδομένων. Ο στόχος θα πρέπει να είναι η διαρκής βελτίωση του επιπέδου εμπειρογνωσίας των υπευθύνων προστασίας δεδομένων. Θα πρέπει να ενθαρρύνονται να συμμετέχουν σε σεμινάρια κατάρτισης για την προστασία των δεδομένων και σε άλλες μορφές επαγγελματικής επιμόρφωσης. Αναλόγως του μεγέθους και της δομής του οργανισμού, μπορεί ενδεχομένως να απαιτείται η σύσταση ομάδας υπευθύνου προστασίας δεδομένων (να υπάρχει δηλαδή υπεύθυνος προστασίας δεδομένων με δικό του προσωπικό). Σε τέτοιες περιπτώσεις, θα πρέπει να καθορίζεται με σαφήνεια η εσωτερική δομή της ομάδας, καθώς και τα καθήκοντα και οι αρμοδιότητες των επιμέρους μελών της. Ομοίως, όταν τα καθήκοντα του υπευθύνου προστασίας δεδομένων ασκούνται από εξωτερικό πάροχο υπηρεσιών, η αποτελεσματική άσκησή τους είναι δυνατό να εξασφαλιστεί με τη σύσταση ομάδας στους κόλπους της εν λόγω οντότητας, τα μέλη της οποίας συνεργάζονται μεταξύ τους υπό την ευθύνη ατόμου το οποίο έχει οριστεί επικεφαλής επικοινωνίας για κάθε πελάτη. Γενικώς, όσο πιο περίπλοκες και/ή ευαίσθητες είναι οι πράξεις επεξεργασίας, τόσο περισσότεροι πόροι πρέπει να διατίθενται στον υπεύθυνο προστασίας δεδομένων. Ο υπεύθυνος προστασίας δεδομένων πρέπει να μπορεί να ασκεί αποτελεσματικά τα καθήκοντά του και να έχει στη διάθεσή του επαρκείς πόρους σε σχέση με τη διενεργούμενη επεξεργασία δεδομένων.[240]

Ανεξαρτησία του Υπεύθυνου Προστασίας Δεδομένων.

Το άρθρο 38 παράγραφος 3 θεσπίζει ορισμένες βασικές εγγυήσεις ώστε να διασφαλίζεται ότι οι υπεύθυνοι προστασίας δεδομένων είναι σε θέση να εκτελούν τα καθήκοντά τους με επαρκή βαθμό αυτονομίας στους κόλπους

[240]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.19-20

του οργανισμού όπου απασχολούνται. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζει ότι ο υπεύθυνος προστασίας δεδομένων δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του. Δεν απολύεται, ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του, λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία.[241]

Στην αιτιολογική σκέψη 97 του Γενικού Κανονισμού Προστασίας Δεδομένων αναφέρεται επιπροσθέτως ότι οι υπεύθυνοι προστασίας δεδομένων, «ανεξάρτητα από το κατά πόσον είναι υπάλληλοι του υπευθύνου επεξεργασίας, θα πρέπει να είναι σε θέση να εκτελούν τις υποχρεώσεις και τα καθήκοντά τους με ανεξάρτητο τρόπο». Αυτό σημαίνει ότι, κατά την άσκηση των καθηκόντων τους που απορρέουν από το άρθρο 39 του Γενικού Κανονισμού Προστασιας Δεδομένων, οι υπεύθυνοι προστασίας δεδομένων δεν πρέπει να λαμβάνουν εντολές για τον τρόπο με τον οποίο θα χειριστούν την εκάστοτε υπόθεση. Ενδεικτικά αναφέρεται: τι αποτέλεσμα θα πρέπει να επιτευχθεί, πώς πρέπει να γίνει η διερεύνηση μιας καταγγελίας ή εάν θα ζητηθεί ή όχι η γνώμη της εποπτικής αρχής. Επιπλέον, δεν πρέπει να λαμβάνουν εντολές προκειμένου να υιοθετήσουν συγκεκριμένη στάση για ένα ζήτημα σε σχέση με τη νομοθεσία περί προστασίας των δεδομένων (να ερμηνεύσουν με συγκεκριμένο τρόπο τη νομοθεσία).

Η διασφάλιση της αυτονομίας των υπεύθυνων προστασίας δεδομένων δεν σημαίνει, όμως, ότι αποκτούν εξουσίες λήψης αποφάσεων καθ’ υπέρβαση των καθηκόντων τους, όπως αυτά ορίζονται στο άρθρο 39 του Γενικού κανονισμού προστασίας Δεδομένων. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι αυτός που εξακολουθεί να φέρει την ευθύνη της συμμόρφωσης με το δίκαιο περί προστασίας των δεδομένων και πρέπει να είναι σε θέση να αποδείξει την εν λόγω συμμόρφωση, όπως ρητά διευκρινίζει περί λογοδοσίας το Άρθρο 5 παρ.2 Του Γενικού κανονισμού Προστασίας Δεδομένων.

Αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία λαμβάνει αποφάσεις που έρχονται σε σύγκρουση με τον Γενικό Κανονισμό Προστασίας Δικαιωμάτων και με τις συμβουλές του υπευθύνου προστασίας δεδομένων, τότε ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει τη δυνατότητα να γνωστοποιήσει την αντίθετη γνώμη του στο ανώτατο διοικητικό επίπεδο του οργανισμού και στους υπεύθυνους λήψης των αποφάσεων. Το άρθρο 38 παρ. 3 του Γενικού Κανονισμού Προστασίας Δικαιωμάτων προβλέπει σχετικά ότι ο υπεύθυνος προστασίας δεδομένων «λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία». Με την απευθείας λογοδοσία διασφαλίζεται η πλήρης ενημέρωση της ανώτερης διοίκησης για τις συμβουλές και τις συστάσεις που διατυπώνει ο υπεύθυνος προστασίας δεδομένων στο πλαίσιο του καθήκοντός

[241] Άρθρο 38 παρ.3 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

του να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία. Απευθείας λογοδοσία αποτελεί και η κατάρτιση ετήσιας έκθεσης δραστηριοτήτων από τον υπεύθυνο προστασίας δεδομένων και η υποβολή της στο ανώτατο διοικητικό επίπεδο.[242]

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζει ότι ο υπεύθυνος προστασίας δεδομένων δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του. Δεν απολύεται, ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του, λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία.[243]

Απόλυση και κυρώσεις του Υπεύθυνου Προστασίας Δεδομένων.

Σύμφωνα με το άρθρο 38 παρ. 3 του γενικού κανονισμού Προστασίας Δικαιωμάτων, ο υπεύθυνος προστασίας δεδομένων «δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του». Ενισχύεται η αυτονομία των υπευθύνων προστασίας δεδομένων και βοηθάει να διασφαλιστεί ανεξαρτησία και επαρκής προστασίας κατά την επιτέλεση των καθηκόντων τους που σχετίζονται με θέματα προστασίας των δεδομένων. Η επιβολή κυρώσεων απαγορεύεται μόνο στην περίπτωση που αυτές επιβάλλονται απλώς επειδή ο υπεύθυνος προστασίας δεδομένων επιτέλεσε τα καθήκοντά του που απορρέουν από τη συγκεκριμένη ιδιότητα. Ένα παράδειγμα που αναφέρεται από την Ομάδα του άρθρου 29 ενδεικτικά, είναι η περίπτωση που ο Υπεύθυνος Προστασίας Δεδομένων εκτιμά ότι μια συγκεκριμένη επεξεργασία ενδέχεται να συνεπάγεται υψηλό κίνδυνο και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία να διενεργήσει εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, όμως ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν συμφωνεί με την άποψη του υπευθύνου προστασίας δεδομένων. Σε μια τέτοια περίπτωση, ο Υπεύθυνος Προστασίας Δεδομένων δεν μπορεί να απολυθεί απλώς επειδή παρείχε τη συγκεκριμένη συμβουλή[244].

Ως κυρώσεις νοούνται άμεσες ή ή παραλείψεις, που μπορούν να λάβουν ποικίλες μορφές. Η στέρηση ή η μεγάλη καθυστέρηση μιας προαγωγής του Υπευθύνου Προστασίας Δεδομένων, η υπονόμευση της εξέλιξης της σταδιοδρομίας του και άρνηση χορήγησης κάποιας παροχής που λαμβάνουν άλλοι εργαζόμενοι., μπορούν να θεωρηθούν επίσης κυρώσεις. Ακόμη, δεν απαιτείται να επιβληθεί μια κύρωση, αρκεί η απειλή της επιβολής της, εφόσον χρησιμοποιούνται προκειμένου να τιμωρηθεί ο Υπεύθυνος

[242]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.19-20

[243]Άρθρο 38 παρ.3 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[244]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.21

Προστασίας Δεδομένων για λόγους που σχετίζονται με τις δραστηριότητες τις οποίες εκτελεί υπό τη συγκεκριμένη ιδιότητα.[245]

Ασφαλώς ο Υπεύθυνος Προστασίας Δεδομένων μπορεί κάλλιστα να απολυθεί νομίμως για λόγους που δεν σχετίζονται με την επιτέλεση των καθηκόντων που απορρέουν από τη συγκεκριμένη ιδιότητα, σύμφωνα με τους συνήθεις κανόνες διοίκησης και όπως ισχύει για οποιονδήποτε υπάλληλο ή ανάδοχο δυνάμει των διατάξεων του εφαρμοστέου εθνικού δικαίου περί συμβάσεων, καθώς και του εφαρμοστέου εθνικού εργατικού και ποινικού δικαίου, που διέπουν τους υπαλλήλους και τους αναδόχους, όπως ενδεικτικά αναφέρονται περιπτώσεις κλοπής, σωματικής, ψυχολογικής ή σεξουαλικής παρενόχλησης ή συναφούς σοβαρού παραπτώματος. Ο Γενικός Κανονισμός Προστασίας Δικαιωμάτων δεν προσδιορίζει ρητώς με ποιους τρόπους και σε ποιες περιπτώσεις μπορεί να απολυθεί ο υπεύθυνος προστασίας δεδομένων ή να αντικατασταθεί από άλλο πρόσωπο. Εάν η σύμβαση του Υπευθύνου Προστασίας δεδομένων είναι στέρεα και παρέχονται επαρκείς εγγυήσεις κατά της καταχρηστικής απόλυσης, τόσο αυξάνουν οι πιθανότητες να μπορεί να ενεργεί με ανεξάρτητο τρόπο.[246]

Επικοινωνία με τον Υπεύθυνο Προστασίας Δεδομένων.

Προβλέπεται[247] ότι τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον Υπεύθυνο Προστασίας Δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και την άσκηση των δικαιωμάτων τους.Ο υπεύθυνος προστασίας δεδομένων, συνεπικουρούμενος από ομάδα εφόσον απαιτείται, πρέπει να είναι σε θέση να επικοινωνεί με τα υποκείμενα των δεδομένων και να συνεργάζεται με τις ενδιαφερόμενες εποπτικές αρχές με αποτελεσματικό τρόπο. Αυτό σημαίνει ότι η επικοινωνία πρέπει να γίνεται στη γλώσσα ή στις γλώσσες που χρησιμοποιούν οι ενδιαφερόμενες εποπτικές αρχές και τα οικεία υποκείμενα των δεδομένων. Η διαθεσιμότητα του υπευθύνου προστασίας δεδομένων (είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας) είναι καθοριστικής σημασίας για τη διασφάλιση της δυνατότητας επικοινωνίας των υποκειμένων των δεδομένων μαζί του.[248]

Για τη διασφάλιση της προσβασιμότητας στον υπεύθυνο προστασίας δεδομένων, η ομάδα του άρθρου 29 συνιστά[249] να είναι εγκατεστημένος ο

[245]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.21

[246]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.21

[247]άρθρο 38 παρ.4 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[248]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.29

[249]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του

τελευταίος εντός Ευρωπαϊκής Ένωσης, ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι ή όχι εγκατεστημένοι στην Ευρωπαϊκή Ένωση. Δεν αποκλείεται, πάντως, σε κάποιες περιπτώσεις στις οποίες ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν είναι εγκατεστημένοι εντός Ευρωπαϊκής Ένωσης, ο υπεύθυνος προστασίας δεδομένων να είναι σε θέση να εκτελεί τις δραστηριότητές του αποτελεσματικότερα εάν είναι εγκατεστημένος εκτός ΕΕ.

Δέσμευση απορρήτου.

Ορίζεται[250] ότι ο Υπεύθυνος Προστασίας Δεδομένων δεσμεύεται από την τήρηση του απορρήτουή της εμπιστευτικότητας σχετικά με τηνεκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ε.Ε ή του κράτους μέλους.Η υποχρέωση τήρησης του απορρήτου/της εμπιστευτικότητας δεν σημαίνει, πάντως, ότι ο υπεύθυνος προστασίας δεδομένων απαγορεύεται να επικοινωνήσει με την εποπτική αρχή και να της ζητήσει συμβουλές.[251]

Στο άρθρο 7 παρ.5 του ν.4624/2019 ρητά ορίζεται ότι ο Υπεύθυνος Προστασίας Δεδομένων είναι υποχρεωμένος να διατηρεί εμπιστευτικότητα ως προς την ταυτότητα των υποκειμένων των δεδομένων και σχετικά με τις περιστάσεις, που επιτρέπουν την εξαγωγή συμπερασμάτων, ως προς το υποκείμενο των δεδομένων, εκτος εάν η ταυτότητα του υποκειμένου αποκαλύπτεται από αυτό.

Συνδυασμός καθηκόντων και σύγκρουση συμφερόντων.

Επιπλέον, προβλέπεται[252] ότι ο Υπεύθυνος Προστασίας Δεδομένων μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις, με τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία να οφείλουν να διασφαλίσουν ότι τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων.Η απουσία σύγκρουσης συμφερόντων συνδέεται στενά με την απαίτηση της επιτέλεσης των καθηκόντων με ανεξάρτητο τρόπο. Μολονότι οι Υπεύθυνοι Προστασίας Δεδομένων επιτρέπεται να επιτελούν και άλλα καθήκοντα, η ανάθεση σ’ αυτούς άλλων καθηκόντων και υποχρεώσεων είναι δυνατή μόνο υπό την προϋπόθεση ότι δεν προκύπτουν συγκρούσεις συμφερόντων. Αυτό συνεπάγεται συγκεκριμένα ότι ο υπεύθυνος προστασίας δεδομένων δεν μπορεί να κατέχει στους κόλπους του οργανισμού θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Οι θέσεις στις οποίες εντοπίζονται συνήθως συγκρούσεις συμφερόντων στους κόλπους ενός οργανισμού είναι, μεταξύ άλλων, οι θέσεις της ανώτερης διοίκησης αλλά και

Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.30

[250]Άρθρο 38 παρ.5 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[251]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.25

[252]Άρθρο 38 παρ.6του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

θέσεις κατώτερων βαθμίδων της οργανωτικής δομής, από τις οποίες είναι δυνατός ο καθορισμός των σκοπών και των μέσων της επεξεργασίας.

Σύγκρουση συμφερόντων μπορεί επίσης να προκύψει σε περίπτωση που ζητηθεί από εξωτερικό Υπεύθυνο Προστασίας Δεδομένων να εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ενώπιον των δικαστηρίων σε υποθέσεις που σχετίζονται με ζητήματα προστασίας των δεδομένων.[253]Κατά την επιτέλεση των καθηκόντων τους οι Υπεύθυνοι Προστασίας Δεδομένων απολαύουν αυτοτέλειας και ανεξαρτησίας, η οποία δεν είναι συμβατή με την υποστήριξη της νομιμότητας πράξεων επεξεργασίας προσωπικών δεδομένων από μέρους του υπευθύνου επεξεργασίας. Για το λόγο αυτό δεν είναι επιτρεπτή η εκπροσώπησή του υπευθύνου επεξεργασίας ενώπιον της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από τον Υπεύθυνο Προστασίας Δεδομένων, διότι ενδέχεται να δημιουργεί σύγκρουση καθηκόντων.[254]

Από την Ομάδα Εργασίας του άρθρου 29 προτείνονται οι ακόλουθες πρακτικές, αναλόγως των δραστηριοτήτων, του μεγέθους και της δομής του εκάστοτε οργανισμού, για τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία. Η προσπάθεια εντοπισμού των θέσεων που είναι ενδεχομένως ασύμβατες με τα καθήκοντα του Υπευθύνου Προστασίας Δεδομένων. Η κατάρτιση εσωτερικού κανονισμού για τον εκάστοτε συγκεκριμένο σκοπό επεξεργασίας, με γνώμονα την αποτροπή των συγκρούσεων συμφερόντων. Η γενική εξήγηση των συγκρούσεων συμφερόντων. Η ανακοίνωση ότι δεν υφίσταται σύγκρουση συμφερόντων για τον υπεύθυνο προστασίας δεδομένων που έχουν ορίσει όσον αφορά την άσκηση των καθηκόντων του υπό τη συγκεκριμένη ιδιότητα, ως έναν τρόπο ενίσχυσης της ευαισθητοποίησης γύρω από τη συγκεκριμένη απαίτηση. Η λήψη εγγυήσεων στον εσωτερικό κανονισμό του οργανισμού. Η διασφάλιση ότι η ανακοίνωση για την πλήρωση της θέσης του Υπευθύνου Προστασίας δεδομένων ή η σύμβαση παροχής υπηρεσιών είναι επαρκώς ακριβείς και λεπτομερείς ώστε να αποτρέπονται οι συγκρούσεις συμφερόντων.

Στο πλαίσιο αυτό, θα πρέπει να σημειωθεί ότι οι συγκρούσεις συμφερόντων μπορούν να λάβουν διάφορες μορφές ανάλογα με το εάν ο προσληφθείς Υπεύθυνος Προστασίας δεδομένων είναι μέλος του προσωπικού ή εξωτερικός συνεργάτης.[255] Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή να ασκεί

[253]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.22

[254] Δελτίο Τύπου . Γ/ΕΞ/568 της 23.01.2020 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

[255]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.22

τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών. Αυτό σημαίνει ότι ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι εξωτερικός, και σ' αυτήν την περίπτωση, τα καθήκοντά του μπορούν να ασκηθούν βάσει σύμβασης παροχής υπηρεσιών η οποία συνάπτεται με φυσικό πρόσωπο ή οργανισμό. Όταν τα καθήκοντα του υπευθύνου προστασίας δεδομένων ασκούνται από εξωτερικό πάροχο υπηρεσιών, η αποτελεσματική άσκησή τους είναι δυνατό να εξασφαλιστεί με τη σύσταση ομάδας στους κόλπους της εν λόγω οντότητας, τα μέλη της οποίας θα συνεργάζονται μεταξύ τους υπό την ευθύνη ενός ατόμου, το οποίο έχει οριστεί επικεφαλής επικοινωνίας και υπεύθυνος για κάθε πελάτη. Σ' αυτήν την περίπτωση, είναι σημαντικό κάθε μέλος του εξωτερικού οργανισμού που ασκεί καθήκοντα υπευθύνου προστασίας δεδομένων να πληροί όλες τις ισχύουσες απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων. Για λόγους νομικής σαφήνειας, καλής οργάνωσης και αποφυγής των συγκρούσεων συμφερόντων για τα μέλη της ομάδας, οι κατευθυντήριες γραμμές συνιστούν να υπάρχει, στη σύμβαση παροχής υπηρεσιών, σαφής καταμερισμός των καθηκόντων στους κόλπους της ομάδας του εξωτερικού Υπευθύνου Προστασίας Δεδομένων και να ορίζεται ένα μόνο άτομο ως επικεφαλής επικοινωνίας και υπεύθυνος για κάθε πελάτη.[256]

3.4 Καθήκοντα του Υπευθύνου Προστασίας Δεδομένων

Στο άρθρο 39 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016 ορίζονται τα καθήκοντα του Υπευθύνου Προστασίας Δεδομένων, με ενδεικτική απαρίθμηση.

Καθηκον για ενημέρωση και παροχή συμβουλών.

Αρχικά, ο Υπεύθυνος Προστασίας Δεδομένων έχει υπόχρέωση να ενημερώνει και συμβουλεύει τον Υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τα δεδομένα σχετικά με τις υποχρεώσεις τους που απορρέουν από το Γενικό Κανονισμό Προστασίας Δεδομένων Ε.Ε.679/2016 και από τις άλλες διατάξεις της Ε.Ε. ή του κράτους μέλους σχετικά με την προστασία δικαιωμάτων[257].

Ο Υπέυθυνος Προστασίας Δεδομένων συνδράμει τον υπεύθυνο επεξεργασίας για τη συμμόρφωσή του με το θεσμικό πλαίσιο προστασίας προσωπικών δεδομένων, χωρίς, ωστόσο, η γνώμη του να δεσμεύει τον υπεύθυνο επεξεργασίας. Είναι ο υπεύθυνος επεξεργασίας που έχει την υποχρέωση να προβαίνει στις αναγκαίες ενέργειες και να λαμβάνει τα αναγκαία μέτρα προκειμένου η επεξεργασία προσωπικών δεδομένων να είναι σύμφωνη με το κανονιστικό πλαίσιο και να αποδεικνύει την εν λόγω συμμόρφωση (λογοδοσία).

Στην πράξη, ο αρχικός σχεδιασμός και η οργάνωση ενός προγράμματος

[256]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.30

[257] Άρθρο 39, παρ1, στοιχ. α' του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

συνολικής διαχείρισης συμμόρφωσης με το Γενικό Κανονισμό Προστασίας Δεδομένων προϋποθέτει τη στενή συνεργασία του Υπεύθυνου Προστασίας Δεδομένων με το τμήμα ΙΤ[258], το τμήμα ασφαλείας, το νομικό τμήμα, το τμήμα εξυπηρέτησης πελατείας.Γίνεται διερεύνηση των αναγκών, υιοθέτηση της φιλοσοφίας και του τρόπου οργάνωσης με βάσει κατάλληλα γενικά πρότυπα και πρότυπα ιδιωτικότητας και ασφαλείας, επιλογή καιεφαρμογή ολοκληρωμένων μηχανογραφικών εφαρμογών για την υποστήριξη της συμμόρφωσης με το Γενικό Κανονισμό Προστασίας Δεδομένων.[259]

Καθήκον για παρακολούθηση συμμόρφωσης.

Σύμφωνα με το άρθρο 39 παρ. 1 στοιχ. β «οι Υπεύθυνοι Προστασίας Δεδομένων έχουν, μεταξύ άλλων, το καθήκον να παρακολουθούν τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων». Στην αιτιολογική σκέψη 97 διευκρινίζεται περαιτέρω ότι ο υπεύθυνος προστασίας δεδομένων «θα πρέπει να παρέχει συνδρομή στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία κατά την παρακολούθηση της εσωτερικής συμμόρφωσης προς τον παρόντα κανονισμό». Στο πλαίσιο των καθηκόντων παρακολούθησης της συμμόρφωσης, οι υπεύθυνοι προστασίας δεδομένων μπορούν συγκεκριμένα να συλλέγουν πληροφορίες με σκοπό τον προσδιορισμό δραστηριοτήτων επεξεργασίας, να αναλύουν και να ελέγχουν τη συμμόρφωση των δραστηριοτήτων επεξεργασίας, να ενημερώνουν τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, να τους παρέχουν συμβουλές και να εκδίδουν συστάσεις υπ’ όψη τους.

Το γεγονός ότι ο Υπεύθυνος Προστασίας Δεδομένων είναι επιφορτισμένος με το καθήκον της παρακολούθησης της συμμόρφωσης δεν σημαίνει ότι ο φέρει προσωπική ευθύνη σε περίπτωση μη συμμόρφωσης. Ο Γενικός Κανονισμός Προστασίας Δεδομένων καθιστά σαφές ότι υπεύθυνος να « εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό είναι ο υπεύθυνος επεξεργασίας, και όχι ο υπεύθυνος προστασίας δεδομένων. Η συμμόρφωση με τους κανόνες προστασίας των δεδομένων είναι εταιρική ευθύνη του υπευθύνου επεξεργασίας, και όχι του υπευθύνου προστασίας δεδομένων.[260]

Όσον αφορά τα αρχεία των δραστηριοτήτων επεξεργασίας, η τήρησή τους είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, και όχι του υπευθύνου προστασίας δεδομένων[261]. Πάντως, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί κάλλιστα να αναθέτει στον υπεύθυνο προστασίας δεδομένων το καθήκον να τηρεί τα

[258]ΙΤ (στα ελληνικά ΤΠΕ), τεχνολογία πληροφοριών και επικοινωνίας ή τεχνολογία της πληροφορίας είναι το σύνολο των επαγγελματικών χώρων οι οποίοι σχετίζονται με τη μελέτη, σχεδίαση, ανάπτυξη, υλοποίηση, συντήρηση και διαχείριση υπολογιστικών πληροφοριακών συστημάτων, κυρίως όσον αφορά εφαρμογές λογισμικού και υλικού υπολογιστών

[259]Κανέλος Λεωνίδας.: «The GDPR handbook. Για DPOs, Επιχειρήσεις & Οργανισμούς», εκδόσεις Νομική Βιβλιοθήκη,2020, σελ.84

[260]Άρθρο 24, παρ1 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

[261]Άρθρο 30 παρ 1 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016

αρχεία των πράξεων επεξεργασίας για τις οποίες είναι υπεύθυνος ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία.[262] Τα εν λόγω αρχεία θα πρέπει να θεωρούνται ως ένα από τα εργαλεία που επιτρέπουν στον υπεύθυνο προστασίας δεδομένων να επιτελεί δύο από τα καθήκοντά του, την ενημέρωση και παροχή συμβουλών στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία[263] και την παρακολούθηση της συμμόρφωσης.[264] Σε κάθε περίπτωση, το αρχείο που επιβάλλεται να τηρείται δυνάμει του άρθρου 30 του Γενικού Κανονισμού Προστασίας Δεδομένων θα πρέπει να αντιμετωπίζεται ως εργαλείο που επιτρέπει στον υπεύθυνο επεξεργασίας και την εποπτική αρχή, κατόπιν αιτήματος, να έχουν μια επισκόπηση όλων των δραστηριοτήτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα που επιτελεί ένας οργανισμός. Αποτελεί επομένως προϋπόθεση συμμόρφωσης και, κατά συνέπεια, αποτελεσματικό μέτρο λογοδοσίας.[265]

Είναι ζωτικής σημασίας η ενσωμάτωση της εφαρμογής των απαιτήσεων του Γενικού Κανονισμού Προστασίας Δεδομένων σε ένα ολοκληρωμένο σύστημα διαχείρισης και διασφάλισης, σε βάθος χρόνου, της συμμόρφωσης. Η εφαρμογή ενός συστήματος διευρυμένης εταιρικής διακυβέρνησης συντελεί στην τυποποίηση των διαδικασιών και στη βελτιστοποίηση του έργου της «διαρκούς συμμόρφωσης». Βασικό πυλώνα της διαδικασίας συμμόρφωσης αποτελεί ο σχεδιασμός και η υλοποίηση ενός προγράμματος περιοδικών ελέγχων και επιθεωρήσεων. Ένας εσωτερικός ή εξωτερικός έλεγχος για ιδιωτικότητα και συμμόρφωση με το Γενικό Κανονισμό Προστασίας Δεδομένων μπορεί να γίνει είτε αυτοτελώς (stand alone audit)είτε να εκτελεστεί ως μέρος ενός γενικότερου προγράμματος εσωτερικών ελέγχων (combined audit)ιδιωτικότητας, ασφάλειας και ποιότητας. Ο εσωτερικός έλεγχος (first party – internal audit) δύναται να υλοποιηθεί από τον Υπεύθυνο Προστασίας Δεδομένων, από ομάδα εσωτερικού ελέγχου είτε από εξωτερικό σύμβουλο. Ο εξωτερικός έλεγχος δύναται να πραγματοποιηθεί είτε από πελάτη ή άλλο ενδιαφερόμενο (second part audit), είτε από την εποπτική Αρχή (third party audit), είτε από φορέα πιστοποίησης (Έλεγχος πιστοποίησης συμμόρφωσης γενικού Κανονισμού Προστασίας Δικαιωμάτων). Ένας έλεγχος (εσωτερικός ή εξωτερικός) μπορεί να υλοποιηθεί οριζόντια, δηλαδή αναφορικά με τις συνολικές διεργασίες ενός Οργανισμού (παροχή υπηρεσιών,

[262]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.34.
Στο άρθρο 39 παράγραφος 1 του Γενικού Κανονισμού Προστασίας ΔεδομένωνΕ.Ε. 679/2016απαριθμούνται τα καθήκοντα του υπευθύνου προστασίας δεδομένων και αναφέρεται συγκεκριμένα ότι ο υπεύθυνος προστασίας δεδομένων έχει «τουλάχιστον» τα ακόλουθα καθήκοντα. Συνεπώς, ο υπεύθυνος επεξεργασίας μπορεί κάλλιστα να αναθέτει στον υπεύθυνο προστασίας δεδομένων και άλλα καθήκοντα πέραν αυτών που αναφέρονται ρητώς στο άρθρο 39 παράγραφος 1, ή να τα εξειδικεύει περαιτέρω.
[263]Άρθρο 39 παρ 1 στοιχ. α'του Γενικού Κανονισμού Προστασίας ΔεδομένωνΕ.Ε. 679/2016
[264]Άρθρο 39 παρ 1 στοιχ. β'του Γενικού Κανονισμού Προστασίας ΔεδομένωνΕ.Ε. 679/2016
[265]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ. 26

εξυπηρέτηση πελατών, marketing). Εναλλακτικά, μπορεί να υλοποιηθεί κάθετα ή εξειδικευμένα, δηλαδή με έμφαση σε διεργασίες ή επεξεργασίες, όπου έχει εντοπιστεί ο μεγαλύτερος κίνδυνος, σύμφωνα με την εκτίμηση αντικτύπου που έχει προηγηθεί. Για την επιτυχία του Εγχειρήματος είναι καίρια η συγκρότηση μιας μικτής Ομάδας Ελέγχου, που θα αποτελείται από στελέχη με εμπειρία σε θέματα ιδιωτικότητας (νομικούς, μηχανικούς, πληροφορικούς) αλλά και από εμπειρογνώμονες με εμπειρία στη διεξαγωγή και στις τεχνικές ελέγχων.[266]

Στην πράξη κατά τη διεξαγωγή των εσωτερικών επιθεωρήσεων είναι προαπαιτούμενη η συνεργασία του Υπευθύνου Προστασίας Δεδομένων με τα υπόλοιπα τμήματα του Οργανισμού και εκτελούνται συνδυασμένοι (risk based) έλεγχοι, με χρήση καταλόγων ελέγχων (checklists), τεχνικών IT audit, συνεργασία με εκπαιδευμένους ελεγκτές και την κατάρτιση αναλυτικών εκθέσεων, με παράλληλη ενημέρωση της Διοίκησης και μέριμνα για τη σωστή διαχείριση των ευρημάτων. Εκτός από τις εσωτερικές επιθεωρήσεις απαιτείται να γίνεται συνεχής παρακολούθηση της συμμόρφωσης και των επεξεργασιών των δεδομένων (continuous monitoring).Με την επιλογή και την εφαρμογή οργανωτικών και τεχνικών μέτρων παρακολούθησης, παράλληλα με την εφαρμογή τεχνικών εργαλείων παρακολούθησης της πρόσβασης χρήσης, παρακολούθησης της ακεραιότητας των κρίσιμων δεδομένων και εργαλείων με δυνατότητα άμεσης ειδοποίησης. Επίσης προτείνεται η χρήση δεικτών, όπως για παράδειγμα ο χρόνος ικανοποίησης των αιτημάτων των υποκειμένων των δικαιωμάτων, το πλήθος των μη εξουσιοδοτημένων προσβάσεων σε δεδομένα. Τέλος, ο προγραμματισμός διεξαγωγής περιοδικών τεχνικών ελέγχων σε συστήματα και εφαρμογές, με σάρωση για τεχνικές αδυναμίες (vulnerability scans),διεξαγωγής τεχνικών ελέγχων παρείσδυσης (penetration tests)σε υπολογιστές, δίκτυα και εφαρμογές εξυπηρέτησης πελατείας είναι κάποιες προτεινόμενες ενέργειες που εάν υλοποιηθούν από έμπειρους τεχνικούς, απαραιτήτως με τη χρήση νόμιμων εργαλείων (με νόμιμες άδειες χρήσης) μπορούν να δώσουν ευρήματα προς έγκαιρη και σωστή αξιοποίηση, που θα οδηγήσουν σε αποκατάσταση πιθανών προβλημάτων.[267]

Καθήκον παροχής συμβουλών για την εκτίμηση αντικτύπου.(άρθρο 39, παρ1γ')

Η συμμετοχή του υπευθύνου προστασίας δεδομένων, ή της ομάδας του, σε όλα τα ζητήματα που σχετίζονται με την προστασία των δεδομένων, όσο το δυνατόν νωρίτερα, είναι καίριας σημασίας. Όσον αφορά τις εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων, ο Γενικός Κανονισμός Προστασίας Δικαιωμάτων προβλέπει ρητώς την έγκαιρη συμμετοχή του υπευθύνου προστασίας δεδομένων και προσδιορίζει ότι ο υπεύθυνος

[266]Κανέλος Λεωνίδας.: «TheGDPRhandbook. Για DPOs, Επιχειρήσεις & Οργανισμούς», εκδόσεις Νομική Βιβλιοθήκη,2020, σελ.83-84
[267]Κανέλος Λεωνίδας.: «TheGDPRhandbook. Για DPOs, Επιχειρήσεις & Οργανισμούς», εκδόσεις Νομική Βιβλιοθήκη,2020, σελ.86

επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων κατά τη διενέργεια εκτιμήσεων αντικτύπου σχετικά με την προστασία των δεδομένων.[268]

Η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων είναι μια διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητα της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων , που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους.[269]Αποτελεί σημαντικό εργαλείο για την πλήρωση της υποχρέωσης λογοδοσίας, καθώς παρέχει συνδρομή στους υπεύθυνους επεξεργασίας προκειμένου να συμμορφώνονται με τις προδιαγραφές του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016, αλλά και να αποδεικνύουν ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για τη διασφάλιση της συμμόρφωσης προς τον Κανονισμό. Είναι μια διαδικασία εμπέδωσης και απόδειξης της συμμόρφωσης.[270]

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα κατήρτισε, βάσει του άρθρου 35 παρ.4 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016, σχέδιο καταλόγου με τα είδη των πράξεων επεξεργασίας που υπόκεινται απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων. Ρητά στην κατηγορία της συστηματικής αξιολόγησης βαθμολόγησης, πρόβλεψης, πρόγνωσης και κατάρτισης προφίλ, αναφέρεται[271] ως ενδεικτικό παράδειγμα η περίπτωση, κατά την οποία χρηματοπιστωτικό ίδρυμα ελέγχει τους πελάτες του με βάσει δεδομένα πιστοληπτικής ικανότητας ή δεδομένα για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας ή δεδομένα για εγκλήματα απάτης. Ο Υπεύθυνος Προστασίας Δεδομένων οφείλει να ενημερώσει για την ύπαρξη του εν λόγω καταλόγου.

Όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων για ζητήματα όπως, ενδεικτικά, τα ακόλουθα:

Εάν θα πρέπει ή όχι να διενεργήσει εκτίμηση αντικτύπου σχετικά με την

[268]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.18

[269]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (WP248 rev01 4.4.2017), 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.

[270]Σωτηρόπουλος Β, «Υπεύθυνος Προστασίας Δεδομένων Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», Εκδόσεις Σάκκουλα, 2019, σελ.221

[271] Απόφαση 65/2018 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

προστασία των δεδομένων.

Ποια μεθοδολογία πρέπει να ακολουθήσει κατά τη διενέργεια της εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων.

Εάν πρέπει να διενεργήσει την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων εσωτερικά ή να την αναθέσει σε εξωτερικό συνεργάτη.

Τι εγγυήσεις (περιλαμβανομένων των τεχνικών και οργανωτικών μέτρων) πρέπει να εφαρμόσει προκειμένου να μετριαστούν οι κίνδυνοι για τα δικαιώματα και τα συμφέροντα των υποκειμένων των δεδομένων.

Εάν διενεργήθηκε σωστά ή όχι η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και εάν τα συμπεράσματά της (σχετικά με το εάν θα δοθεί ή όχι συνέχεια στην επεξεργασία και τι εγγυήσεις θα εφαρμοστούν) είναι σύμφωνα με τις απαιτήσεις περί προστασίας των δεδομένων.[272]

Σε κάθε περίπτωση, εάν ο Υπεύθυνος Επεξεργασίας διαφωνήσει με την παρεχόμενη συμβουλή του Υπευθύνου προστασίας Δεδομένων, στο έγγραφο της εκτίμησης αντικτύπου θα πρέπει να δικαιολογηθεί εγγράφως για ποιο λόγο δεν έχει ακολουθηθεί η συμβουλή.

Η εκτίμηση αντικτύπου ή μελέτη κινδύνων ιδιωτικότητας διεξάγεται συνήθως είτε για κρίσιμες επεξεργασίες υψηλού κινδύνου, είτε για νέες επεξεργασίες από τον Οργανισμό ή την εφαρμογή νέων Συστημάτων. Ιδιαίτερα, όταν για την επεξεργασία χρησιμοποιούνται νέες τεχνολογίες, πρέπει να συνεκτιμηθεί η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας και το ενδεχόμενο η επεξεργασία να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων με τη διενέργεια εκτίμησης αντικτύπου. Σε μια εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας, οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.[273] Κρίσιμα ζητήματα είναι η ενημέρωση της Διοίκησης και η λήψη έγκρισης, καθώς και η σωστή και έγκαιρη διαχείρισης των κινδύνων με την επιλογή κατάλληλων προτύπων και μεθοδολογίας.[274]

Καθήκον για συνεργασία και διαβούλευση με την εποπτική Αρχή.

Σύμφωνα με το άρθρο 39 παρ.1 στοιχ. δ’ και ε’, ο υπεύθυνος προστασίας δεδομένων θα πρέπει να «συνεργάζεται με την εποπτική αρχή» και να «ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί

[272]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.33

[273]Σωτηρόπουλος Β, «Υπεύθυνος Προστασίας Δεδομένων Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», Εκδόσεις Σάκκουλα, 2019, σελ.364

[274]Κανέλος Λεωνίδας.: «The GDPR handbook. Για DPOs, Επιχειρήσεις & Οργανισμούς», εκδόσεις Νομική Βιβλιοθήκη,2020, σελ.85

διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα».[275] Τα εν λόγω καθήκοντα αναφέρονται ουσιαστικά στον «μεσολαβητικό» ρόλο του υπευθύνου προστασίας δεδομένων που αναφέρεται στην εισαγωγή των παρουσών κατευθυντήριων γραμμών. Ο Υπεύθυνος προστασίας Δεδομένων ενεργεί ως σημείο επικοινωνίας, προκειμένου να διευκολύνει την πρόσβαση της εποπτικής αρχής στα έγγραφα και τις πληροφορίες που σχετίζονται με την επιτέλεση των καθηκόντων της, όπως προβλέπονται στο άρθρο 57 του Γενικού Κανονισμού Προστασίας Δεδομένων, καθώς και με την άσκηση των εξουσιών έρευνας και των διορθωτικών, αδειοδοτικών και συμβουλευτικών εξουσιών, όπως προβλέπονται στο άρθρο 58 του Γενικού Κανονισμού Προστασίας Δεδομένων.

Όπως προαναφέρθηκε, ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους [276], όμως η υποχρέωση τήρησης του απορρήτου ή της εμπιστευτικότητας δεν σημαίνει ότι ο υπεύθυνος προστασίας δεδομένων απαγορεύεται να επικοινωνήσει με την εποπτική αρχή και να της ζητήσει συμβουλές. Σύμφωνα με το άρθρο 39 παρ. 1 στοιχ. ε’ του Κανονισμού Προστασίας Δεδομένων, ο Υπεύθυνος Προστασίας Δεδομένων μπορεί να πραγματοποιεί διαβουλεύσεις με την εποπτική αρχή, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

Ωστόσο είναι σημαντικό ο Υπεύθυνος Προστασίας Δεδομένων να νοείται ως μέρος του πιστωτικού Οργανισμού που υπηρετεί και όχι ως «πράκτορας» της εποπτικής Αρχής. Για να διασφαλιστεί η συμμόρφωση εντός του οργανισμού είναι κρίσιμης σημασίας η υποστήριξη και η καλή συνεργασία με ην εποπτική αρχή.[277]

Ιεράρχηση δραστηριοτήτων των Υπευθύνων Προστασίας Δεδομένων

Σύμφωνα με το άρθρο 39 παρ.2 του Γενικού Κανονισμού Προστασίας Δεδομένων, ο υπεύθυνος προστασίας δεδομένων «λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας». Το εν λόγω άρθρο υπενθυμίζει ουσιαστικά μια γενική αρχή της κοινής λογικής, η οποία σχετίζεται ενδεχομένως με πολλές πτυχές των καθημερινών εργασιών που επιτελεί ο υπεύθυνος προστασίας δεδομένων. Απαιτεί από τους υπεύθυνους προστασίας δεδομένων να ιεραρχούν τις δραστηριότητές τους κατά σειρά προτεραιότητας και να επικεντρώνονται στα ζητήματα που εγκυμονούν σοβαρότερους κινδύνους για την προστασία των δεδομένων. Αυτό δεν σημαίνει μεν ότι θα πρέπει να παραμελούν την παρακολούθηση της

[275] Άρθρο 39 παρ.1 στοιχ. δ’ και ε’ του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[276] Άρθρο 38 παρ.5 του Γενικού Κανονισμού Προστασίας Δεδομένων Ε.Ε. 679/2016
[277] Σωτηρόπουλος Β, «Υπεύθυνος Προστασίας Δεδομένων Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», Εκδόσεις Σάκκουλα, 2019, σελ.435

συμμόρφωσης των πράξεων επεξεργασίας δεδομένων που παρουσιάζουν συγκριτικά χαμηλότερο επίπεδο κινδύνου, υποδεικνύει όμως ότι θα πρέπει να εστιάζουν πρώτιστα στους τομείς υψηλού κινδύνου. Αυτή η επιλεκτική και ρεαλιστική προσέγγιση θα βοηθήσει λογικά τους υπεύθυνους προστασίας δεδομένων να συμβουλεύουν τον υπεύθυνο επεξεργασίας ποια μεθοδολογία να χρησιμοποιήσει κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, σε ποιους τομείς θα πρέπει να διενεργηθεί εσωτερικός ή εξωτερικός έλεγχος για την προστασία των δεδομένων, ποιες δραστηριότητες εσωτερικής κατάρτισης θα πρέπει να παρασχεθούν στο προσωπικό ή στα διοικητικά στελέχη που είναι υπεύθυνα για δραστηριότητες επεξεργασίας δεδομένων, και σε ποιες πράξεις επεξεργασίας θα πρέπει να διαθέσει περισσότερο χρόνο και πόρους.[278]

Ο υπεύθυνος προστασίας δεδομένων που ορίζεται από εκτελούντα την επεξεργασία επιβλέπει επιπλέον τις δραστηριότητες που αναπτύσσει ο οργανισμός του εκτελούντος την επεξεργασία όταν ενεργεί αυτοδικαίως ως υπεύθυνος επεξεργασίας (π.χ., ανθρώπινο δυναμικό, πληροφορική, εφοδιαστική).[279]

4. Επίλογος

Στις περισσότερες περιπτώσεις, οι τράπεζες που επιδιώκουν τη συμμόρφωση προς την ισχύουσα νομοθεσία προστασίας δεδομένων προσωπικού χαρακτήρα αξιοποιούν τους υπάρχοντες μηχανισμούς προστασίας δεδομένων και τα προϋπάρχοντα πληροφοριακά συστήματα ασφάλειας,αναπροσαρμόζοντάς τα, αντί να επιλέξουν τη λύση του ριζικού μετασχηματισμού. Τείνουν γενικά να συμμορφώνονται μετά από την επιβολή συστάσεων και προειδοποιήσεων, παρά να εφαρμόσουν εκ των προτέρων μία πρωτοβουλία επανασχεδιασμού των διαδικασιών σε κάθε τμήμα του ευρέως φάσματος των τραπεζικών εργασιών με κριτήριο την αποτελεσματική προστασία των δικαιωμάτων προσωπικού χαρακτήρα των συναλλασσομένων.

Κατά την εκπόνηση της παρούσας εργασίας, διαπιστώθηκε από τις πρόσφατες αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ότι ενώ έγιναν προσπάθειες από μέρους των τραπεζών για συμμόρφωση προς τον Γενικό Κανονισμό Προστασίας Δικαιωμάτων κατά τον σχεδιασμό των νέων προϊόντων και των νέων υπηρεσιών δεν λαμβάνεται πάντα η μέριμνα για την ορθή εφαρμογή του ισχύοντος νομοθετικού πλαισίου ή ότι έστω δεν επιδιώκεται να εξασφαλιστεί μέσω επίσημης γνωμοδότησης η ορθή ερμηνεία του, ώστε να προβλεφθούν παραλείψεις και λάθος ερμηνείες.

[278]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ. 25

[279]Ομάδα Προστασίας των Προσώπων έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα του Άρθρου 29 (6/EL WP 243 rev.01 – Απρίλιος 2017), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ.13

«Κάλλιον το προλαμβάνειν ή το θεραπεύειν», σύμφωνα με τη ρήση του Ιπποκράτη, αλλά στην πραγματικότητα οι Τράπεζες τείνουν να λαμβάνουν δράση μετά από την διαπίστωση παραβάσεων.
Παρατίθεται ως χαρακτηριστικό παράδειγμα η Απόφαση 48/2018 της Αρχής Προστασίας Προσωπικών Δεδομένων σχετικά με τη δυνατότητα ανέπαφων συναλλαγών των τραπεζικών καρτών. Προτού οι Τράπεζες λανσάρουν την καινοτόμα αυτή λειτουργικότητα, δεν προέβησαν στις απαραίτητες ενέργειες για να διασφαλίσουν ότι η επεξεργασία των δεδομένων θα είναι νόμιμη. Προέβησαν σε έκδοση καρτών όπου το εν λόγω χαρακτηριστικό ήταν ενεργοποιημένο από προεπιλογή, χωρίς ο πελάτης να το έχει αιτηθεί ή να έχει παράσχει τη συγκατάθεσή του και χωρίς να του δίνεται η δυνατότητα να διακόψει την επεξεργασία αυτή. Χρειάστηκε να μεσολαβήσει ικανό χρονικό διάστημα, μετά την έκδοση της εν λόγω απόφασης, προκειμένου να καταστεί δυνατόν συστημικά ο πελάτης να απενεργοποιεί το συγκεκριμένο χαρακτηριστικό αυτοβούλως. Να σημειωθεί ότι η καινοτομία αυτή προωθήθηκε λίγο πριν την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων, και ενώ είχε ήδη δημοσιευτεί το κείμενο του Κανονισμού, σε χρονική περίοδο που γινόταν εκτενής συζήτηση για τα ζητήματα που προέκυπταν από την ερμηνεία του.

4.1 Σύνοψη και Συμπεράσματα

Συνοψίζοντας, διαπιστώθηκε από τη μελέτη των αποφάσεων της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ότι στο πεδίο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τις Τράπεζες τα παρακάτω σημεία χρήζουν ιδιαίτερης μνείας και προσοχής.
Αρχικά, σχετικά με την υποχρέωση ενημέρωσης του υποκειμένου των δικαιωμάτων, διαπιστώθηκαν κατά διαστήματα πολλές παραλείψεις και επενέβη η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Επιγραμματικά αναφέρονται η υποχρέωση προσήκουσας ενημέρωσης οφειλετών για την τιτλοποίηση απαιτήσεων (Απόφαση 33/2018 της Α.Π.Δ.Π.Χ), την υποχρέωση ενημέρωσης του υποκειμένου των δικαιωμάτων στην περίπτωση που γίνεται επεξεργασία χωρίς τη συγκατάθεσή του για τη διαπίστωση της πιστοληπτικής ικανότητας (Απόφαση 50/2000 της Α.Π.Δ.Π.Χ), την υποχρέωση ενημέρωσης κατόχου κάρτας με λειτουργικότητα ανέπαφων συναλλαγών ως προς την ειδική επεξεργασία (Απόφαση 48/2018 της Α.Π.Δ.Π.Χ), την υποχρέωση ενημέρωσης του υποκειμένου των δικαιωμάτων σχετικά με την καταγραφή των τηλεφωνικών συνομιλιών, το σκοπό επεξεργασίας και το χρονικό διάστημα τήρησης των δεδομένων (Απόφαση 72/2013 της Α.Π.Δ.Π.Χ.) και την υποχρέωση ενημέρωσης των υποκειμένων των δικαιωμάτων δια του τύπου σχετικά με τη διαβίβαση δεδομένων λόγω συγχώνευσης Τραπεζών (Αποφάσεις 38/2013 και 127/2013 της Α.Π.Δ.Π.Χ.).
Επίσης, χρειάστηκε να δοθούν διευκρινήσεις σχετικά με τη λήψης συγκατάθεσης του υποκειμένου των δικαιωμάτων πριν την επεξεργασία από

τις Τράπεζες και τις εξαιρέσεις από την υποχρέωση αυτή. Ο όρος για προαπαιτούμενη συγκατάθεση πελάτη της Τράπεζας για επεξεργασία δεδομένων του για διαφημιστικούς σκοπούς, προκειμένου να του χορηγηθεί χρεωστική κάρτα κρίθηκε παράνομος από την Αρχή, διότι η επεξεργασία γίνεται για σκοπούς διαφορετικούς από την εκτέλεση της σύμβασης και η συγκατάθεση δεν θεωρείται ειδική και ελεύθερη (Απόφαση 18/2007 της Α.Π.Δ.Π.Χ.). Η επεξεργασία επιτρέπεται χωρίς τη συγκατάθεση του υποκειμένου όταν είναι απαραίτητη για την εκτέλεση σύμβασης, στην οποία το συμβαλλόμενο μέρος είναι υποκείμενο των δεδομένων. Εάν μία επεξεργασία δεν μπορεί να εκληφθεί ως απολύτως απαραίτητη στο πλαίσιο των συμβατικών σχέσεων, απαιτείται συγκατάθεση του υποκειμένου, αφού έχει προηγηθεί επαρκής και σαφής ενημέρωση για την επεξεργασία. (Απόφαση 39/2015 της Α.Π.Δ.Π.Χ.). Στην περίπτωση συλλογής δεδομένων για το σκοπό διαπίστωσης πιστοληπτικής ικανότητας δεν απαιτούνταν συγκατάθεση του υποκειμένου, βάσει της εξαίρεσης του αρθ.5 του Ν.2472/97 (Απόφαση 50/2000 τα Α.Π.Δ.Π.Χ.). Για τη διαβίβαση δεδομένων από τράπεζα σε εταιρία ενημέρωσης οφειλετών δεν απαιτούνταν συγκατάθεση του υποκειμένου των δικαιωμάτων, εφόσον προηγήθηκε σαφής ενημέρωση του οφειλέτη για τις κατηγορίες των αποδεκτών των δεδομένων του, εφόσον θεωρείται επεξεργασία αναγκαία για την εκτέλεση σύμβασης (Έγγραφο Γ/ΕΞ/73-1/28-01-2013 της Α.Π.Δ.Π.Χ.)

Ακόμη, σχετικά με την επεξεργασία ευαίσθητων δεδομένων από τις τράπεζες διευκρινίστηκε ότι επιτρέπεται κατ’ εξαίρεση, κατόπιν λήψης γραπτής συγκατάθεσης του υποκειμένου, αφού προηγηθεί ενημέρωση του υποκειμένου για το σκοπό της επεξεργασίας, τα δεδομένα και τους αποδέκτες τους και τον υπεύθυνο επεξεργασίας και αφού η τράπεζα λάβει ειδική άδεια από την Αρχή προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Σε δύο περιπτώσεις η Αρχή χορήγησε στις τράπεζες τη σχετική άδεια. Για την εκπλήρωση του σκοπού της υπαγωγής των υποκειμένων των δικαιωμάτων στις εξαιρέσεις από τις απαγορεύσεις και τους περιορισμούς που τέθηκαν στην ανάληψη μετρητών και μεταφορά κεφαλαίων (Capital Controls, από 18-07-2015 Πράξη Νομοθετικού περιεχομένου και Ν.4350/2015). Για την εκπλήρωση του σκοπού της υπαγωγής των δανειοληπτών στη διαδικασία επίλυσης καθυστερήσεων κατ’ εφαρμογή του Ν.4224/2013.

Ιδιαίτερη μέριμνα θα πρέπει να γίνει από τις τράπεζες για τη βελτίωση των τεχνικών και οργανωτικών μέτρων ασφαλείας, ώστε να προστατευτούν από τη διαρροή των δεδομένων, την αθέμιτη ή παράνομη επεξεργασία τους ή την μη εξουσιοδοτημένη πρόσβαση υπαλλήλων ή τρίτων, καθώς σε αρκετές περιπτώσεις διαπιστώθηκαν παραβιάσεις.

Σχετικά με την ανταπόκριση των τραπεζών σε αιτήματα των συναλλασσομένων τους για ικανοποίηση του δικαιώματος πρόσβασης στα δεδομένα τους, διαπιστώθηκε σε πολλές περιπτώσεις ότι δεν ικανοποιήθηκε το δικαίωμα ή ότι δεν τηρήθηκαν τα προβλεπόμενα χρονικά διαστήματα. Η

Αρχή απεφάνθη ότι δεν απαιτείται η επίκληση έννομου συμφέροντος από το υποκείμενο των δικαιωμάτων, προκειμένου να λάβει γνώση των πληροφοριών που το αφορούν και που τηρεί η τράπεζα ως υπεύθυνος επεξεργασίας (Απόφαση 143/2017 της Α.Π.Δ.Π.Χ.). Επίσης ιδιαίτερη προσοχή θα πρέπει να δοθεί στην έγκαιρη γνωστοποίηση περιστατικών παραβίασης από τις τράπεζες στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθώς διαπιστώθηκαν παρατυπίες. Ακόμη, σχετικά με τη νομιμότητα της επεξεργασίας των δεδομένων από τις τράπεζες, τα μέτρα δέουσας επιμέλειας, που δύναται να λάβουν οι τράπεζες ως προς τα ιδρύματα πληρωμών, θα πρέπει να επιτάσσονται από εθνικό νόμο ή έστω από τις πράξεις της αρμόδιας εποπτικής Αρχής. Ούτε το ίδιο το ίδρυμα πληρωμών , που υπόκειται σε εποπτεία δεν μπορεί να διενεργήσει πλήρη έλεγχο για τους δικούς του πελάτες , εάν δεν προβλέπεται ρητά από το νόμο (Γ/ΕΞ/4417-1/31-7-2014).

Εξαιρετικά σημαντικό είναι να λαμβάνουν οι τράπεζες όλα τα απαιτούμενα μέτρα ώστε τα δεδομένα που επεξεργάζονται να είναι επικαιροποιημένα, να μην διατηρούνται για χρονικό διάστημα πέραν του αναγκαίου και προβλεπόμενου και να καταστρέφονται με τον προσήκοντα τρόπο, όταν παρέλθει το διάστημα τήρησής τους. Οι συμβάσεις που χρησιμοποιούν οι τράπεζες θα πρέπει να επικαιροποιούνται τακτικά ώστε να συμπεριλαμβάνουν τυχόν εξελίξεις επί της ερμηνείας των νομοθετικών διατάξεων.

Εν κατακλείδι, επισημαίνεται ο καθοριστικός και καίριος ρόλος του Υπευθύνου προστασίας Δεδομένων της εκάστοτε τράπεζας, ιδίως κατά την εκπλήρωση των καθηκόντων του προς ενημέρωση και παροχή συμβουλών, προς παρακολούθηση της συμμόρφωσης και προς παροχής συμβουλών για τη διενέργεια εκτίμησης αντικτύπου, κάθε φορά που κρίνεται αναγκαίο. Ο Υπεύθυνος Προστασίας Δεδομένων της τράπεζας θα εμφυσήσει στην κουλτούρα της τράπεζας τις Βασικές Αρχές επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, ώστε η λειτουργία της τράπεζας σε όλο το φάσμα των τραπεζικών εργασιών που εκτελεί να εναρμονίζεται προς αυτές.

Επιδίωξη της Τράπεζας οφείλει να είναι η νόμιμη επεξεργασία των δεδομένων, μόνο για τους προβλεπόμενους σκοπούς και νόμιμους λόγους, με ιδιαίτερη μέριμνα για την προσήκουσα ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων και την εκπλήρωση των υποχρεώσεων της ως υπεύθυνος επεξεργασίας. Με την εφαρμογή δέσμης πολιτικών θα πρέπει να διασφαλίζεται η ασφάλεια των δεδομένων. Ενίσχυση της ασφάλειας της επεξεργασίας με κρυπτογράφηση και νέες τεχνολογίες, παρακολούθηση των απειλών, διενέργεια αξιολογήσεων κινδύνου, εφαρμογή διαδικασιών ιχνηλασίας και περιορισμού των προσβάσεων, χρήση πολλαπλών επιπέδων άμυνας και τακτικές ενημερώσεις στην πολιτική ασφαλείας λόγω των ραγδαίων τεχνολογικών εξελίξεων είναι ενδεικτικά μέτρα, στα οποία θα πρέπει να προβεί μια τράπεζα προς ελαχιστοποίηση του κινδύνου παραβίασης

των δεδομένων προσωπικού χαρακτήρα που τηρούν.
Ακόμη και εάν οι τράπεζες δεν είναι διατεθειμένες να επενδύσουν σε έναν εκ βάθρων μετασχηματισμό τους υπό το πρίσμα της προστασίας των δεδομένων των συναλλασσομένων της με διαλειτουργικότητα σε όλο το εύρος των υπηρεσιών και των λειτουργιών τους, οφείλουν να επενδύσουν στην κατάρτιση μιας ενιαίας και συνεκτικής πολιτικής που θα ενσωματώνει αποτελεσματικά τη νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα σε όλο το φάσμα των τραπεζικών εργασιών και των υποστηρικτικών υπηρεσιών της.

Παράρτημα Α - Βιβλιογραφία

Β.1 Βιβλιογραφία

Β.1.1 Βιβλία

Αλεξανδροπούλου – Αιγυπτιάδου Ε., «Ηλεκτρονική επεξεργασία προσωπικών δεδομένων στο πεδίο της Τραπεζικής Δραστηριότητας (Νομικό Πλαίσιο) Αρμ. ΝΗ' (2004)1337–1395.
Αλεξανδροπούλου – Αιγυπτιάδου Ε., «Η προστασία των προσωπικών δεδομένων πριν και μετά τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 Ε.Ε», 9ο Πανελλήνιο Συνέδριο Ε.Ε.Ν.e-Θέμις, 2018.
Αλεξανδροπούλου – Αιγυπτιάδου Ε. – Μυλώση Μ., «Προσωπικά δεδομένα οικονομικής συμπεριφοράς και ηλεκτρονική επεξεργασία τους από την ΤΕΙΡΕΣΙΑΣ Α.Ε.», ΔΙΜΕΕ, 2015.
Ιγγλεζάκης Ι., «Προστασία Προσωπικών Δεδομένων στο σύστημα πληροφοριών "ΤΕΙΡΕΣΙΑΣ"», εκδόσεις Σάκκουλα, 2006
Κανέλος Λ., «The GDPR handbook. Για DPOs, Επιχειρήσεις & Οργανισμούς», εκδόσεις Νομική Βιβλιοθήκη,2020
Μήτρου Λ., «Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα», εκδόσεις Σάκκουλα, 2017.
Σωτηρόπουλος Β., «Υπεύθυνος προστασίας δεδομένων. Εγχειρίδιο για τον ιδιωτικό και δημόσιο τομέα», εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2019

Β.1.2 Άρθρα

Khiar I., Trautwein K., Huber A. and Stamm J. (2018), The EU General Data Protection Regulation (GDPR) in the banking industry https://www.pwc.ch/en/publications/2017/gdpr_banking_industry_report_en.pdf (23/2/2020)
Baxter M. (2018), Open banking and GDPR, is there a clash? https://gdpr.report/news/2018/01/18/open-banking-gdpr-clash (2/12/2019)

Β.1.2 Ανέκδοτες Πηγές (Εργασίες /Διατριβές)

Κατσή Ε., «Ο υπεύθυνος προστασίας δεδομένων στον γενικό κανονισμό προστασίας δεδομένων (ΕΚ) 679/2016», Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών Δίκαιο και Πληροφορική, Πανεπιστήμιο Μακεδονίας, 2019 http://dspace.lib.uom.gr/handle/2159/23421
Μοστράτου Ζ., «GDPR. Η εφαρμογή του νόμου περί προστασίας των προσωπικών δεδομένων στην Εθνική τράπεζα της Ελλάδος», Ελληνικό Ανοικτό Πανεπιστήμιο,2019 https://apothesis.eap.gr/handle/repo/41321
Μπρούζου Α., «Ο Υπεύθυνος Προστασίας Δεδομένων στο Γ.Κ.Π.Δ.»,

Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών Δίκαιο και Πληροφορική, Πανεπιστήμιο Μακεδονίας,2018 http://dspace.lib.uom.gr/handle/2159/23453
Πανάγου Ε., «Επεξεργασία δεδομένων οικονομικής συμπεριφοράς στον τραπεζικό χώρο», Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών Δίκαιο και Πληροφορική, Πανεπιστήμιο Μακεδονίας,2019 http://dspace.lib.uom.gr/handle/2159/22742

Β.2 Ιστοσελίδες

Α.Π.Δ.Π.Χ. www.dpa.gr

Γενικός Κανονισμός 2016/679/ΕΕ http://www.dataprotection.gov.cy/dataprotection/

Ελληνική Ένωση Τραπεζών. https://www.hba.gr/info/gdpr

Ενημερωτικό δελτίο (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Τεύχος 12 / Ιούλιος 2015 https://www.dpa.gr/el/enimerwtiko/e-newsletter/12o-teyhos

Ετήσια έκθεση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2018 https://www.dpa.gr/el/enimerwtiko/etisies-ektheseis/etisia-ekthesi-2018

Ετήσια έκθεση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2017 https://www.dpa.gr/el/enimerwtiko/ektheseis/etisia-ekthesi-2017

Ετήσια έκθεση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2014 https://www.dpa.gr/el/enimerwtiko/etisies-ektheseis/etisia-ekthesi-2014

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της 25ης Νοεμβρίου 2015, Οδηγία 2015/2366/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου της 25ης Νοεμβρίου 2015 (ΕΕ L 271) https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=LEGISSUM:2404020302_1&from=EL

Κείμενο αιτιολογικής έκθεσης ΓΚΠΔ, πηγή: http://www.europarl.europa.eu/sides/

Οδηγία https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=LEGISSUM:l24120

Ομάδα εργασίας άρθρου 29 Guidelines on Data Protection Officers ('DPOs') ,16/EL WP 243 rev. 0 file:///C:/Users/user/Contacts/Downloads/wp243_rev01_enpdf.pdf

Ομάδα εργασίας του άρθρου 29 (2011), Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, WP 187, 13 Ιουλίου 2011 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf

Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του

«εκτελούντος την επεξεργασία», (00264/10/EL WP 169), 16 Φεβρουαρίου 2010 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων, Γνώμη 10/2006 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από την Παγκόσμια Εταιρεία Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (SWIFT), (01935/06/EL WP128), 22 Νοεμβρίου 2006. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_el.pdf

Ομάδα εργασίας του άρθρου 29 (2014), Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ, WP 217, 4 Απριλίου 2014 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf

Ομάδα εργασίας του άρθρου 29 (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 17/EL WP 248 αναθ. 01 ,2016/679. https://www.dpa.gr/sites/default/files/2019-12/wp248_rev.01_el.pdf

Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, «Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων», Έκδοση 2018

https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

Συμβούλιο της Ευρώπης, Επιτροπή της Σύμβασης 108, Γνώμη για τις επιπτώσεις της επεξεργασίας των ονομαστικών καταστάσεων επιβατών στην προστασία δεδομένων (Opinion on the Data protection implications of the processing of Passenger Name Records), T-PD(2016)18rev, 19 Αυγούστου 2016 https://rm.coe.int/16806b051e

ΤΕΙΡΕΣΙΑΣ Α.Ε http://www.tiresias.gr/company.html

EUR Lex https://eur-lex.europa.eu

European Union https://ec.europa.eu

Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR. Version 2.0, December 2020 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

-