ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

ΚΩΔΙΚΑΣ ΔΕΟΝΤΟΛΟΓΙΑΣ
ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
ΣΤΟ ΤΡΑΠΕΖΙΚΟ ΣΥΣΤΗΜΑ

(ΣΧΕΔΙΟ 16.1.2019)

Περιεχόμενα

Κεφάλαιο Α'

Εισαγωγή – Προοίμιο

Ο παρών Κώδικας Δεοντολογίας (στο εξής «ο Κώδικας») εκπονήθηκε από την Ελληνική Ένωση Τραπεζών (εφεξής ΕΕΤ), κατόπιν συνεργασίας των τραπεζών-μελών της, στο πλαίσιο εφαρμογής του άρθρου 40 του Γενικού Κανονισμού (ΕΕ) 2016/679 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών» (εφεξής «Κανονισμός»).

Λαμβάνοντας υπόψη την ως άνω ρητή πρόβλεψη στον Κανονισμό, σύμφωνα με την οποία παρέχεται η δυνατότητα σε ενώσεις ομοειδών επιχειρήσεων κατάρτισης Κωδίκων Δεοντολογίας προκειμένου να διευκολύνεται η ουσιαστική εφαρμογή του, θεσπίζεται ο παρών Κώδικας Δεοντολογίας που έχει διαμορφωθεί, έτσι ώστε να ανταποκρίνεται πλήρως στις νέες απαιτήσεις για την προστασία των προσωπικών δεδομένων και την ελεύθερη κυκλοφορία αυτών, αλλά και στα ιδιαίτερα χαρακτηριστικά της λειτουργίας των χρηματοπιστωτικών επιχειρήσεων. Έτσι ο Κώδικας αποτελεί επιπρόσθετο εχέγγυο διαφάνειας και προστασίας της προσωπικότητας των πελατών των πιστωτικών ιδρυμάτων και των συνεργαζόμενων με αυτά τρίτων.

Ο Κώδικας Δεοντολογίας θέτει με σαφήνεια τις βασικές αρχές της διαφάνειας, συνέπειας, υπευθυνότητας και λογοδοσίας, που διέπουν την επεξεργασία των προσωπικών δεδομένων και συμβάλλει στην ισχυροποίηση της ασφάλειας δικαίου στις σχέσεις των πιστωτικών ιδρυμάτων με τους πολίτες.

Ο παρών Κώδικας υλοποιεί τον Κανονισμό και με την έννοια αυτή τα πιστωτικά ιδρύματα στις συμβάσεις τους προβλέπουν πάντα επίπεδο προστασίας προσωπικών δεδομένων τουλάχιστον ίδιο με αυτό που ρυθμίζεται από τον παρόντα Κώδικα. Τυχόν πρόσθετες συμβατικές υποχρεώσεις των πιστωτικών ιδρυμάτων, που διασφαλίζουν υψηλότερο επίπεδο προστασίας στους πελάτες τους σε σχέση με τον παρόντα Κώδικα, παραμένουν ισχυρές. Εάν σύμβαση πιστωτικού ιδρύματος εμφανίζει κενό ρύθμισης ως προς τα προσωπικά δεδομένα, αυτό θα καλύπτεται από τις διατάξεις του παρόντος κώδικα, ακόμη και εάν η σύμβαση δεν περιλαμβάνει ρητή αναφορά σε αυτόν.

Άρθρο 1

Πεδίο εφαρμογής

1.1. Στον παρόντα Κώδικα υπάγονται τα πιστωτικά ιδρύματα μέλη της ΕΕΤ.

1.2. Στον Κώδικα αυτόν μπορούν να υπαχθούν πιστωτικά ιδρύματα που λειτουργούν νόμιμα στην Ελλάδα μη μέλη της ΕΕΤ, είτε έχουν την έδρα τους στην Ελλάδα, συμπεριλαμβανομένων των συνεταιριστικών τραπεζών, είτε πρόκειται για υποκαταστήματα αλλοδαπών πιστωτικών ιδρυμάτων που

ασκούν δραστηριότητα στην Ελλάδα, καθώς και το Ταμείο Παρακαταθηκών και Δανείων, εφόσον αποστείλουν σχετική γραπτή δήλωση προσχώρησης στον παρόντα Κώδικα Δεοντολογίας. Για τα μέλη που υπάγονται στον κώδικα θα αναρτηθεί και θα επικαιροποιείται σχετική κατάσταση στην ιστοσελίδα της ΕΕΤ.

1.3. Στον Κώδικα αυτόν μπορούν επίσης να υπαχθούν, με έγγραφη δήλωσή τους, χρηματοδοτικά ιδρύματα, καθώς θυγατρικές πιστωτικών ιδρυμάτων που έχουν ήδη υπαχθεί σε αυτόν.

1.4. Ο Κώδικας εφαρμόζεται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, καθώς και στη μη αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο, ως μέρος των επιχειρηματικών δραστηριοτήτων των πιστωτικών ιδρυμάτων.

1.5. Στον παρόντα Κώδικα δεν υπάγονται τα προσωπικά δεδομένα των φυσικών προσώπων εκπροσώπων νομικών προσώπων ή αντικλήτων φυσικών ή νομικών προσώπων, εφόσον τηρούνται αποκλειστικά για σκοπούς είτε εκπροσώπησης, είτε για τις ανάγκες των άρθρων 142 επομ. ΚΠολΔ, δεδομένου ότι αυτά δεν ενεργούν για ίδιο λογαριασμό και οι πράξεις ή παραλείψεις τους αφορούν αποκλειστικά και μόνο τα νομικά πρόσωπα, τα οποία δεν εμπίπτουν στο υποκειμενικό πεδίο εφαρμογής του νομικού πλαισίου προστασίας δεδομένων προσωπικού χαρακτήρα.

1.6. Επεξεργασία προσωπικών δεδομένων από τα πιστωτικά ιδρύματα υπό την ιδιότητα αυτών ως εργοδοτών δεν εμπίπτει στον παρόντα κώδικα.

Άρθρο 2

Σκοπός

2.1. Ο παρών Κώδικας έχει ως βασικό σκοπό να αποσαφηνίσει τις γενικές αρχές που διέπουν την επεξεργασία των δεδομένων των υποκειμένων από τα πιστωτικά ιδρύματα και να παράσχει την απαιτούμενη πληροφόρηση προς αυτά, προκειμένου να ενισχύσει την εμπιστοσύνη τους όσον αφορά τη διασφάλιση των προσωπικών δεδομένων τους, καθ' όλη τη διάρκεια της συναλλακτικής σχέσης τους με τα πιστωτικά ιδρύματα.

2.2. Λαμβάνοντας υπόψη τις ιδιαίτερες νομοθετικές και κανονιστικές απαιτήσεις που διέπουν τη λειτουργία των πιστωτικών ιδρυμάτων, ο εν λόγω Κώδικας στοχεύει στην ισχυροποίηση της διαφάνειας των κανόνων που εφαρμόζουν τα πιστωτικά ιδρύματα αναφορικά με την επεξεργασία των προσωπικών δεδομένων, διευκολύνοντας με αυτό τον τρόπο την απρόσκοπτη άσκηση, εκ μέρους των υποκειμένων των δεδομένων, των σχετικών δικαιωμάτων τους.

2.3. Επιπρόσθετα, ο Κώδικας παρέχει τη δυνατότητα επέκτασης του πεδίου εφαρμογής του και σε υπεύθυνους επεξεργασίας ή εκτελούντες την επεξεργασία που διατηρούν οιουδήποτε τύπου συνεργασία με τα πιστωτικά ιδρύματα, διευκολύνοντας τη μεταξύ τους διαβίβαση δεδομένων προσωπικού χαρακτήρα με την τήρηση των κατάλληλων εγγυήσεων.

2.4. Παράλληλα, ο Κώδικας περιέχει ρυθμίσεις και προβλέψεις που καθιστούν εφικτή την υποχρεωτική παρακολούθηση της συμμόρφωσης, ιδίως όσον αφορά τον προσδιορισμό των κινδύνων που συνδέονται με την επεξεργασία, την εκτίμησή τους από άποψη προέλευσης, φύσης, πιθανότητας και σοβαρότητας και την αποτύπωση των βέλτιστων πρακτικών για τον περιορισμό των κινδύνων.

Κεφάλαιο Β'

Ενότητα 1

Θεσμικό πλαίσιο

Άρθρο 3

Αρχές επεξεργασίας

3.1. 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 Κανονισμού. 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.

3.2. Ειδικότερα, κάθε πιστωτικό ίδρυμα διασφαλίζει με κατάλληλες πολιτικές διαδικασίες και οργανωτικά και τεχνικά μέσα ότι τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται:

α) Συλλέγονται για προκαθορισμένους, ρητούς και νόμιμους σκοπούς, όπως αυτοί ορίζονται στο άρθρο 4 του Κώδικα και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς,

β) Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων,

γ) Είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο μέτρο για την επίτευξη των σκοπών για τους οποίους υποβάλλονται σε επεξεργασία,

δ) Είναι ακριβή και, όταν είναι εφικτό, επικαιροποιούνται, ενώ πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση των δεδομένων προσωπικού χαρακτήρα που είναι αποδεδειγμένα ανακριβή,

ε) Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της

επεξεργασίας, αλλά και την άσκηση δικαιωμάτων ή την υπεράσπιση εννόμων συμφερόντων, σύμφωνα με τις κάθε φορά ισχύουσες διατάξεις των νόμων.

στ) Υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια τους, περιλαμβανομένης τόσο της προστασίας τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, όσο και της ασφαλούς καταστροφής ή ανωνυμοποίησής τους, μετά τη λήξη του χρόνου τήρησης, με τη χρησιμοποίηση καταλλήλων τεχνικών ή οργανωτικών μέτρων.

Ενότητα 2

Ο ρόλος των πιστωτικών ιδρυμάτων

Άρθρο 4

Σκοποί επεξεργασίας

4.1.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.

Τα πιστωτικά ιδρύματα 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.

4.2. Παροχή τραπεζικών υπηρεσιών

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 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.

Σε κάθε περίπτωση συναλλαγής ή κατάρτισης σύμβασης με πιστωτικά ιδρύματα, αυτά συλλέγουν και επεξεργάζονται προσωπικά δεδομένα που ταυτοποιούν με πληρότητα και ακρίβεια το αντισυμβαλλόμενο φυσικό πρόσωπο και προσδιορίζουν τον τόπο κατοικίας του και τα στοιχεία επικοινωνίας μαζί του, όπως επιβάλλεται κατ΄ αρχήν από τις γενικές αρχές του δικαίου.

Πέραν αυτών, ειδικότερα ανά κατηγορία προϊόντων και υπηρεσιών, τα πιστωτικά ιδρύματα επεξεργάζονται προσωπικά δεδομένα πελατών τους για τους ακόλουθους σκοπούς:

α) Καταθετικά προϊόντα και πράξεις 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.

β) Χορηγητικά προϊόντα.

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.

γ) Επενδυτικά προϊόντα και υπηρεσίες φύλαξης και διοικητικής διαχειρίσεως τίτλων.

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.

δ) Προϊόντα μικτών χαρακτηριστικών.

Στην περίπτωση των προϊόντων μικτών χαρακτηριστικών η επεξεργασία των σχετικών προσωπικών δεδομένων εξυπηρετεί τους αντίστοιχους των χαρακτηριστικών τους σκοπούς, κατά τα προαναφερθέντα.

4.3. Προώθηση τραπεζικών προϊόντων και υπηρεσιών

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.

α) 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 Κανονισμό, όταν γίνεται επεξεργασία προσωπικών δεδομένων για σκοπούς εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται σε κάθε περίπτωση να αντιταχθεί (άρθρο 21, παρ. 2 του Κανονισμού). 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 (άρθρο 22, παρ. 1 και 2 του Κανονισμού).

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 διαχωρισθεί 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.

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 (βλ. άρθρο 10 του παρόντος κώδικα), προς τα οποία θα γίνει η προώθηση. Περαιτέρω σημειώνεται ότι λόγω της φύσης των 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 (βλ. επομ. άρθρο 5), 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 ουδένα κίνδυνο συνεπάγονται για τα υποκείμενα των δεδομένων-πελάτες. Παρά ταύτα στις περιπτώσεις αυτές πρέπει να παρέχεται στο υποκείμενο το δικαίωμα εναντίωσης.

β) Έρευνα Ικανοποίησης Πελατών

Με τις έρευνες αυτές τα πιστωτικά ιδρύματα επιδιώκουν αφενός να διαπιστώσουν το βαθμό ικανοποίησης των πελατών τους από τα προϊόντα ή/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 (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.
Κατ' ακολουθία, οι κατά τα παραπάνω 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.

γ) 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 μη, εφόσον αυτή είναι αναγκαία για την δημόσια προβολή της εικόνας και της δραστηριότητας του πιστωτικού ιδρύματος (π.χ. επεξεργασία δεδομένων κειμένων εκπροσώπων ΜΜΕ, επεξεργασία δεδομένων υποκείμενων που ευεργετούνται από χορηγίες ή παροχές αριστείας ή άλλες παροχές κοινωνικού ή φιλανθρωπικού χαρακτήρα), ή αφορούν σε 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.

4.4. 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:

α) συστημάτων καταγραφής εικόνας στους χώρους συναλλαγών εντός των καταστημάτων του πιστωτικού ιδρύματος ή εκτός αυτών στις θέσεις των ATMs,

β) 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,

γ) 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.

4.5. 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.

4.6 Μετοχολόγιο

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.

4.7 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 κλπ.ή/και απευθύνεται σε

αρμόδιους κατά περίπτωση φορείς, αρχές ή υπηρεσίες, προς τους οποίους ή/και οποίες διαβιβάζει τα προσωπικά δεδομένα των εκάστοτε εμπλεκομένων φυσικών προσώπων (αντιδίκων, ομόδικων, αντικλήτων, κλπ.).

Η νομική βάση για την εν λόγω επεξεργασία-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 (δικηγόροι / δικηγορικές εταιρίες, δικαστικοί επιμελητές κλπ.).
Τα ανωτέρω ισχύουν και για τη διαβίβαση προσωπικών δεδομένων πελατών σε εταιρίες ενημέρωσης οφειλετών (Ν. 3758/2009, όπως εκάστοτε ισχύει) και εταιρίες διαχείρισης απαιτήσεων (Ν. 4354/2015, 4469/2017, όπως εκάστοτε ισχύει).

4.8 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.

4.9 Διαβίβαση σε αρχές.

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 πχ. φοροδιαφυγή, απάτη κλπ.), είτε διεθνών υποχρεώσεων της χώρας (όπως πχ. στην περίπτωση της FATCA).
Στις περιπτώσεις αυτές η διαβίβαση αποτελεί υποχρέωση εκ του νόμου, για την εκπλήρωση της οποίας δεν απαιτείται συγκατάθεση των υποκειμένων των διαβιβαζόμενων δεδομένων και κατά κανόνα ούτε ειδική ενημέρωση αυτών.
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.

4.10 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 ή/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 κλπ.

Άρθρο 5

Η συγκατάθεση των πελατών-υποκειμένων

5.1 Η συγκατάθεση 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. 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.

5.2 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.

5.3 Η προσέγγιση του υποκειμένου για τη χορήγηση (ή άρνηση) συγκατάθεσης δεν υπόκειται σε προϋποθέσεις ή περιορισμούς, εκτός από αυτούς που υπαγορεύονται από την καλή πίστη.

Τυχόν προγενέστερη δήλωση του υποκειμένου ότι δεν επιθυμεί την προσέγγισή του για την προώθηση προϊόντων ή/και υπηρεσιών προς το πιστωτικό ίδρυμα ή τρίτο (πχ. πάροχο υπηρεσιών κινητής τηλεφωνίας) δεν επηρεάζει την επικοινωνία μαζί του για την παροχή (ή μη) συγκατάθεσης, εφόσον δεν πρόκειται για προώθηση.

5.4 Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει την παρασχεθείσα συγκατάθεσή του ανά πάσα στιγμή. 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.

5.5 Τα πιστωτικά ιδρύματα 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.

5.6 Συγκατάθεση που είχε χορηγηθεί σύμφωνα με τις διατάξεις του Ν.2472/97 παραμένει ισχυρή και υπό τον Γενικό Κανονισμό, υπό την προϋπόθεση ότι πληρούνται οι κατά τα ανωτέρω ειδικές προϋποθέσεις αυτού.

Άρθρο 6

Συλλογή και είδος δεδομένων

6.1.Με εξαίρεση τα δεδομένα υπό (α) και (β) κατωτέρω, που είναι απολύτως απαραίτητα για κάθε συναλλακτική ή συμβατική σχέση με το πιστωτικό ίδρυμα, το είδος και το πλήθος των λοιπών δεδομένων που συλλέγονται και τίθενται σε επεξεργασία, εξαρτάται σε κάθε περίπτωση από το είδος της σύμβασης που είτε θα συναφθεί, είτε υφίσταται με το πιστωτικό ίδρυμα και το προσφερόμενο ή παρεχόμενο προϊόν ή υπηρεσία.

Τα δεδομένα αυτά είναι ενδεικτικά τα εξής:

α) Δεδομένα ταυτοποίησης, όπως ονοματεπώνυμο, πατρώνυμο, μητρώνυμο, ΑΔΤ, ΑΦΜ, ΑΜΚΑ, φύλο, υπηκοότητα, ημερομηνία και τόπο γέννησης, κλπ.

Τα δεδομένα αυτά συλλέγονται απευθείας από τα υποκείμενα ή/και από δημόσια προσβάσιμες πηγές ή/και από δημόσια προσβάσιμα κοινωνικά δίκτυα (π.χ. faceboook, twitter).

β) Δεδομένα επικοινωνίας: ταχυδρομική και ηλεκτρονική διεύθυνση, τηλέφωνο σταθερό και κινητό κλπ.

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.

γ) Δεδομένα μελών της διοίκησης πελατών-νομικών προσώπων ή ενώσεων προσώπων ή επιχειρήσεων, όπως και των κυριότερων φορέων αυτών, όπως αυτά προκύπτουν από σχετικές δημόσια προσβάσιμες πηγές (πχ ΓΕΜΗ) ή από σχετικά έγγραφα αυτών.

δ) Δεδομένα οικονομικής και περιουσιακής κατάστασης, επάγγελμα, αποδοχές, εξαρτώμενα μέλη, έντυπα Ε1 και Ε9, εκκαθαριστικά σημειώματα κλπ.

Τα εν λόγω δεδομένα συλλέγονται είτε απευθείας από τα υποκείμενα, είτε από δημόσια προσβάσιμες πηγές, όπως υποθηκοφυλακεία, κτηματολογικά γραφεία κλπ.

ε) Δεδομένα υγείας του υποκειμένου ή των εξαρτώμενων μελών της οικογένειας του που συλλέγονται αποκλειστικά από αυτό και μόνο, με δική του πρωτοβουλία .

στ) Δεδομένα αθέτησης των οικονομικών υποχρεώσεων, όπως ενδεικτικά ακάλυπτες επιταγές, καταγγελίες συμβάσεων δανείων και πιστώσεων, διαταγές πληρωμής, κατασχέσεις και επιταγές προς πληρωμή, αιτήσεις και αποφάσεις εξυγίανσης ή πτώχευσης κλπ.

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.” (www.tiresias.gr) 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.

ζ) Δεδομένα που αφορούν στην πιστοληπτική ικανότητα των υποκειμένων: οφειλές σε πιστωτικά ή και χρηματοδοτικά ιδρύματα από δάνεια ή πιστώσεις.

Τα δεδομένα αυτά συλλέγονται είτε από το πιστωτικό ίδρυμα στο πλαίσιο συμβατικών σχέσεων των πελατών τους με αυτό, είτε από άλλα πιστωτικά ιδρύματα, όταν αυτό επιτρέπεται, είτε από αρχεία δεδομένων οικονομικής συμπεριφοράς και κυρίως την ΤΕΙΡΕΣΙΑΣ Α.Ε (www.tiresias.gr) ή οποιαδήποτε εταιρεία επεξεργασίας δεδομένων οικονομικής συμπεριφοράς στην Ελλάδα ή σε άλλο κράτος μέλος της Ευρωπαϊκής Ένωσης.

η) Δεδομένα που αφορούν στη συναλλακτική συμπεριφορά του πελάτη, που προκύπτουν και συλλέγονται από τη λειτουργία της σύμβασης (-εων) με το πιστωτικό ίδρυμα, όπως και από τη χρήση των προϊόντων και υπηρεσιών του πιστωτικού ιδρύματος (π.χ. των πιστωτικών ή χρεωστικών καρτών), όπως και από δημόσια προσβάσιμα κοινωνικά δίκτυα.

θ) Δεδομένα πιστωτικής βαθμολόγησης (credit scoring-credit profiling).

Τα δεδομένα αυτά είτε παράγονται από το πιστωτικό ίδρυμα από τον αυτοματοποιημένο συνδυασμό δεδομένων υπό (γ), (ε), (στ) και (ζ) ανωτέρω, είτε συλλέγονται από την ΤΕΙΡΕΣΙΑΣ Α.Ε. (www.tiresias.gr) ή οποιαδήποτε εταιρεία επεξεργασίας δεδομένων οικονομικής συμπεριφοράς στην Ελλάδα ή σε άλλο κράτος μέλος της Ευρωπαϊκής Ένωσης.

ι) Δεδομένα αναγνωριστικά της ηλεκτρονικής ταυτότητας του Πελάτη, όπως η διεύθυνση διαδικτυακού πρωτοκόλλου (IP Address).

ια)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 λειτουργεία των συστημάτων του πιστωτικού ιδρύματος (πχ. βασικά cookies).

ιβ) Δεδομένα τηλεφωνικών ή και διαδικτυακών επικοινωνιών του Πελάτη με το πιστωτικό ίδρυμα που καταγράφονται σύμφωνα με το κατά περίπτωση θεσμικό πλαίσιο.

ιγ) Δεδομένα διενέργειας πράξεων πληρωμών και παροχής υπηρεσιών πληρωμών, τα οποία συλλέγονται από τον πελάτη ή τον πάροχο υπηρεσιών πληρωμών που έχει αυτός επιλέξει.

ιδ) 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)-www.tiresias.gr, από αστυνομικές αρχές, όπως και από αρμόδιους φορείς του εξωτερικού που είναι επιφορτισμένοι με την πρόληψη και καταστολή των προαναφερθέντων εγκλημάτων.

ιε) 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.

ιστ) Δεδομένα εικόνας από τα συστήματα βιντεοσκόπησης των χώρων του πιστωτικού ιδρύματος, στους οποίους υπάρχουν οι σχετικές κατά νόμο σημάνσεις.

6.2 Στην έννοια της συλλογής των δεδομένων από τους πελάτες κατά τα ανωτέρω, περιλαμβάνεται και η συλλογή τους από τρίτα πρόσωπα κατ΄ εντολή των πελατών.

Άρθρο 7

Ειδικές κατηγορίες προσωπικών δεδομένων

7.1 Με την επιφύλαξη των διατάξεων των επόμενων παραγράφων του άρθρου αυτού και των σχετικών διατάξεων του Κανονισμού, απαγορεύεται από τα πιστωτικά ιδρύματα η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, τις καταδίκες και ποινικές διώξεις, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

7.2 Τα πιστωτικά ιδρύματα επιτρέπεται να επεξεργάζονται προσωπικά δεδομένα ειδικών κατηγοριών στις ακόλουθες εναλλακτικά περιπτώσεις:

α) Όταν το υποκείμενο των δεδομένων είτε έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων στο πλαίσιο της συνεργασίας του με το πιστωτικό ίδρυμα, είτε η συγκατάθεσή του αυτή εμπεριέχεται στο αίτημά του με το οποίο υπέβαλε στο πιστωτικό ίδρυμα τα ειδικής κατηγορίας δεδομένα του (βλ. και αρ. 5 ανωτέρω), όπως π.χ. μετά από πρωτοβουλία του υποκειμένου για την επίτευξη καλύτερων όρων ρύθμισης υφιστάμενης σύμβασης πίστωσης ή εξαίρεσης από τους περιορισμούς στην ανάληψη

μετρητών και κίνηση κεφαλαίων (capital controls) ή πραγματοποίηση συναλλαγών με ειδικούς τρόπους λόγω προβλημάτων όρασης, ακοής κλπ.

β) Η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων (πχ μέσω των κοινωνικών δικτύων).

γ) Η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

7.3 Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα που σχετίζονται με την υγεία, λόγω επίκλησής τους από το υποκείμενο, κατά τα αναφερόμενα στην προηγούμενη παρ. 2, απαγορεύεται να επεκταθεί κατά οποιονδήποτε τρόπο για την εξυπηρέτηση άλλων σκοπών από το πιστωτικό ίδρυμα ή από τρίτους. Η εν λόγω επεξεργασία θα υπόκειται σε κατάλληλα και ειδικά μέτρα ασφάλειας και περιορισμού της πρόσβασης, για την προστασία των δικαιωμάτων και ελευθεριών των φυσικών προσώπων, σύμφωνα με τους όρους των σχετικών αδειών τήρησης αρχείου ευαίσθητων δεδομένων που έχουν χορηγηθεί από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στα πιστωτικά ιδρύματα και τις διατάξεις του Κανονισμού.

7.4 Η επεξεργασία δεδομένων προσωπικού χαρακτήρα που σχετίζονται με καταδίκες και ποινικές διώξεις υποκειμένων, δύναται να πραγματοποιείται από το πιστωτικό ίδρυμα τόσο στο πλαίσιο των έννομων υποχρεώσεών του για την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, καθώς και σε περίπτωση που αυτό είναι απαραίτητο για την εκτέλεση σύμβασης ή έχει άμεσο έννομο συμφέρον, όπως για την επιλεξιμότητα σε συγκεκριμένη θέση εργασίας (πχ. σε θέση διαχείρισης χρημάτων) ή για τη θεμελίωση, υποστήριξη ή άσκηση νομικών αξιώσεων. Το πιστωτικό ίδρυμα σε αυτή την περίπτωση διασφαλίζει την ασφαλή επεξεργασία των συγκεκριμένων δεδομένων, τη χρονική διάρκεια τήρησής τους, καθώς και τη διαδικασία διαγραφής τους.

Άρθρο 8

Αποδέκτες

1. Αποδέκτες των προσωπικών δεδομένων των πελατών των πιστωτικών ιδρυμάτων είναι κυρίως:
   α) Οι υπάλληλοι και τα στελέχη τους που είναι αρμόδια για την ολοκλήρωση της κατά περίπτωση συναλλαγής ή την κατάρτιση, διαχείριση και παρακολούθηση της εκάστοτε σύμβασης με τον πελάτη,
   β) Στελέχη θυγατρικών εταιριών του πιστωτικού ιδρύματος, που ανήκουν στον χρηματοπιστωτικό τομέα για την εκτίμηση του αναλαμβανόμενου κινδύνου σε ομιλικό επίπεδο, την εκπλήρωση των σχετικών εποπτικών υποχρεώσεων και την κατά ενιαίο τρόπο αντιμετώπιση των πελατών.
   γ) Άλλα πιστωτικά ή χρηματοδοτικά ιδρύματα ή φορείς του εσωτερικού ή του εξωτερικού περιλαμβανομένων των εταιριών ή φορέων ειδικού σκοπού κατά την έννοια του Ν.3156/2003, όπως εκάστοτε ισχύει, εφόσον, αυτό είναι αναγκαίο για την ολοκλήρωση μιας συναλλαγής, όπως πχ. στην περίπτωση της μεταφοράς κεφαλαίων εντός Ελλάδος ή Ευρωπαϊκής Ένωσης ή και σε

τρίτες χώρες, οπότε ισχύουν τα αναφερόμενα στο άρθρο 12 του παρόντος, ή της τιτλοποίησης απαιτήσεων ή της χρήσης πιστωτικής ή χρεωστικής κάρτας σε άλλο πιστωτικό ίδρυμα ή σε δίκτυο που δεν ανήκει στο πιστωτικό ίδρυμα που εξέδωσε την κάρτα.

δ) Φορείς στους οποίους το πιστωτικό ίδρυμα αναθέτει τη διεκπεραίωση εργασιών ή την εκτέλεση έργων για λογαριασμό του, όπως πχ. πραγματογνώμονες, εταιρίες παροχής υπηρεσιών πληροφορικής, τηλεφωνικής εξυπηρέτησης, αναλύσεων δεδομένων, αρχειοθέτησης κλπ.

ε) Φορείς συγχρηματοδότησης ή παροχής εγγυήσεων του εσωτερικού ή του εξωτερικού, όπως το Ελληνικό Δημόσιο, το ΕΤΕΑΝ, η Ευρωπαϊκή Τράπεζα Επενδύσεων, το Ταμείο Εγγύησης Καταθέσεων και Επενδύσεων (ΤΕΚΕ) κλπ.

στ) Εταιρίες ενημέρωσης οφειλετών (Ν.3758/2009, όπως ισχύει), εταιρίες διαχείρισης απαιτήσεων (Ν.4354/2015, όπως ισχύει), δικηγόροι, δικηγορικές εταιρίες, δικαστικοί επιμελητές, συμβολαιογράφοι κλπ.

ζ) Εταιρίες ή φορείς που λειτουργούν νόμιμα και είναι εξειδικευμένοι στην επικαιροποίηση στοιχείων ταυτοποίησης και επικοινωνίας, φυσικών και νομικών προσώπων, κυρίως στις περιπτώσεις που οι πελάτες παραλείπουν να επικαιροποιήσουν τα ως άνω στοιχεία τους στο πιστωτικό ίδρυμα με το οποίο συναλλάσσονται, κατά παράβαση της σχετικής υποχρέωσης (βλ. παρ. 8.2).

η) Εταιρίες ή φορείς του εσωτερικού ή του εξωτερικού που αποκτούν απαιτήσεις του πιστωτικού ιδρύματος κατά πελατών του, όπως πχ. επενδυτικές εταιρίες.

θ) Άλλα τραπεζικά και χρηματοδοτικά ιδρύματα που έχουν χρηματοδοτήσει τον ίδιο πελάτη-οφειλέτη ή στα οποία αυτός τηρεί καταθετικούς λογαριασμούς, εφόσον αυτός υποβάλει αίτηση υπαγωγής στο Ν.4469/2015, για τον εξωδικαστικό μηχανισμό διευθέτησης οφειλών, ή στο Ν.3869/2010, για την πτώχευση των ιδιωτών, σύμφωνα με τις διατάξεις αυτών, όπως ισχύουν.

ι) Εποπτικές των πιστωτικών ιδρυμάτων αρχές, όπως η Τράπεζα της Ελλάδος, η Ευρωπαϊκή Κεντρική Τράπεζα, ο Ενιαίος Εποπτικός Μηχανισμός κλπ., Δικαστικές και Εισαγγελικές αρχές ή φορείς του Δημοσίου στο πλαίσιο των καθηκόντων τους, όπως φορολογικές αρχές.

ια) Η διατραπεζικού χαρακτήρα εταιρία με την επωνυμία ΤΡΑΠΕΖΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΑΕ (ΤΕΙΡΕΣΙΑΣ ΑΕ) για δεδομένα που αφορούν σε ακάλυπτες επιταγές, απλήρωτες συναλλαγματικές και γραμμάτια σε διαταγή, καταγγελίες συμβάσεων χορήγησης δανείων ή πιστώσεων και την εξέλιξη τέτοιων συμβάσεων, για την εξασφάλιση της πληρότητας και ακρίβειας των αρχείων της ως άνω εταιρίας και τη λειτουργία του αρχείου της ‘’Τειρεσίας Σύστημα Ελέγχου Κινδύνου” (ΤΣΕΚ), όπως και για δεδομένα που αφορούν σε καταγγελίες συμβάσεων μεταξύ πιστωτικών ιδρυμάτων και εμπορικών επιχειρήσεων για την αποδοχή από τις τελευταίες πιστωτικών ή/και χρηματοδοτικών καρτών (acquiring), όπως αναλυτικά αναφέρεται στη σχετική ενημέρωση που είναι αναρτημένη στην ιστοσελίδα της ΤΕΙΡΕΣΙΑΣ ΑΕ (www.teiresias.gr).

ιβ) Εταιρίες προβολής και προώθησης προϊόντων ή/και υπηρεσιών όπως και πραγματοποίησης ερευνών αγοράς και ικανοποίησης πελατών .
ιγ) Για τα δεδομένα του μετοχολογίου, αποδέκτες είναι επίσης οι λοιποί μέτοχοι του πιστωτικού ιδρύματος, το Κεντρικό Αποθετήριο Αθηνών ΑΕ, η Επιτροπή Κεφαλαιαγοράς και λοιποί φορείς με αρμοδιότητα στους μετοχικούς τίτλους, τις επ΄αυτών συναλλαγές κλπ.

2. Έχοντας υπόψη ότι η ενημέρωση των υποκειμένων για τις κατηγορίες αποδεκτών είναι διαχρονικά αποδεκτή από το σχετικό θεσμικό πλαίσιο (Οδηγία 95/46/ΕΕ, άρθρα 10 και 11 και Κανονισμός ΕΕ/2016/679, άρθρα 13, παρ.1,ε και 14, παρ.1,ε), τα πιστωτικά ιδρύματα ενημερώνουν τους πελάτες τους για τους κατά τα ανωτέρω αποδέκτες των δεδομένων τους προσδιορίζοντας αυτούς κατά κατηγορία, εφόσον είναι αντικειμενικά αδύνατος ο εξατομικευμένος προσδιορισμός των αποδεκτών για κάθε πελάτη κατά τη διάρκεια της συμβατικής του σχέσης με το πιστωτικό ίδρυμα.

Άρθρο 9

Ακρίβεια δεδομένων προσωπικού χαρακτήρα

9.1. Τα πιστωτικά ιδρύματα, ως υπεύθυνοι επεξεργασίας, λαμβάνουν όλα τα απαραίτητα μέτρα προκειμένου τα δεδομένα προσωπικού χαρακτήρα των υποκειμένων – πελατών τους να είναι ακριβή και να επικαιροποιούνται, ενώ προνοούν ώστε όσα δεδομένα αποδεδειγμένα δεν είναι ακριβή, να μη διαβιβάζονται σε οποιονδήποτε τρίτο και να μην υφίστανται οποιαδήποτε επεξεργασία, εκτός της αποθήκευσης, μέχρι τη διόρθωσή τους, άλλως, να διαγράφονται.

9.2. Έχοντας υπόψη ότι πολλά προσωπικά δεδομένα συλλέγονται από τους πελάτες των πιστωτικών ιδρυμάτων (βλ. ανωτέρω άρθρο 6), αυτοί οφείλουν να ενημερώνουν το πιστωτικό ίδρυμα για κάθε μεταβολή των δεδομένων προσωπικού χαρακτήρα που τους αφορούν, χωρίς καθυστέρηση, καθώς επίσης και να ανταποκρίνονται σε εύλογο χρονικό διάστημα σε κάθε αίτημα του πιστωτικού ιδρύματος που αφορά την επικαιροποίηση των εν λόγω δεδομένων. Σε περίπτωση που ο πελάτης δεν έχει ανταποκριθεί στην ως άνω υποχρέωσή του, το πιστωτικό ίδρυμα δικαιούται, με βάση τα προσωπικά δεδομένα ταυτοποίησης και επικοινωνίας που ήδη έχει, να αναζητήσει τα ισχύοντα δεδομένα με κάθε νόμιμο τρόπο.

9.3. Τα πιστωτικά ιδρύματα υιοθετούν διαδικασίες ελέγχου της πληρότητας και ακρίβειας των δεδομένων που τηρούν, όπως και της επικαιροποίησης αυτών και λαμβάνουν υπόψη την κατά την προηγούμενη παράγραφο ανταπόκριση των πελατών τους για την αξιολόγηση τους.

Άρθρο 10

Χρόνος τήρησης δεδομένων

10.1 Τα προσωπικά δεδομένα τηρούνται για το χρόνο που είναι απαραίτητος για την εκπλήρωση του σκοπού που εξυπηρετεί η επεξεργασία τους, άλλως για τον ελάχιστο χρόνο που απαιτεί η εκάστοτε ισχύουσα νομοθεσία που διέπει τη λειτουργία των πιστωτικών ιδρυμάτων και σε κάθε περίπτωση για χρόνο όχι μεγαλύτερο των (20) είκοσι ετών από τη λήξη της σύμβασης ή της συναλλαγής, που είναι ο χρόνος της κατ' άρθρο 249 ΑΚ γενικής παραγραφής των αξιώσεων. Εάν μέχρι τη λήξη της ως άνω προθεσμίας βρίσκονται σε εξέλιξη δικαστικές ενέργειες με το πιστωτικό ίδρυμα που αφορούν άμεσα ή έμμεσα το υποκείμενο των δεδομένων, ο εν λόγω χρόνος τήρησης των προσωπικών δεδομένων παρατείνεται μέχρι την έκδοση αμετάκλητης δικαστικής απόφασης.,

10.2. Ειδικότερα και ενδεικτικά :

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 (5) 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 (5) ετών ή για πρόσθετη περίοδο δύο (2) ετών μετά από απόφαση της Επιτροπής Κεφαλαιαγοράς όταν διενεργεί έρευνα για κατάχρηση της αγοράς (άρθρο 43 του ν. 4443/2016).

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 (45) 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 (άρθρο 16 της υπ' αριθ. 1/2011 Οδηγία της Αρχής).

ε) Οι τηλεφωνικές επικοινωνίες με πελάτες στο πλαίσιο των διατάξεων του Ν. 3758/2009 διατηρούνται υποχρεωτικά για ένα (1) 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 (άρθρο 8 παρ. 2 Ν. 3758/2009).

στ) Αρχεία με δεδομένα υποκειμένων που δημιουργούνται από την εφαρμογή του Κώδικα Δεοντολογίας του Ν. 4224 /2013 στο πλαίσιο της διαδικασίας επίλυσης καθυστερήσεων, διατηρούνται για ελάχιστη περίοδο έξι (6) 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 (Κεφάλαιο 7ο της υπ' αριθ. 195/2016 Απόφασης της Επιτροπής Πιστωτικών και Ασφαλιστικών Θεμάτων της Τράπεζας της Ελλάδος).

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 (1) 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 (5) 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 συνίστανται :

(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.

Άρθρο 11

Κατάρτιση "profile"

11.1 Τα πιστωτικά ιδρύματα διενεργούν σε αυτοματοποιημένες επεξεργασίες προσωπικών δεδομένων πελατών τους ή/και σε κατάρτιση "profile" με τον αυτοματοποιημένο συνδυασμό περισσότερων του ενός χαρακτηριστικών. Αυτού του είδους οι επεξεργασίες αξιοποιούν τις συνεχώς αυξανόμενες δυνατότητες της πληροφορικής και των μαθηματικών μοντέλων, αυξάνοντας αντίστοιχα την ακρίβεια των εντεύθεν αποτελεσμάτων και κατ' ακολουθία τις πιθανότητες επίτευξης του επιδιωκόμενου αποτελέσματος.

11.2. Τα πιστωτικά ιδρύματα προκειμένου να προβαίνουν σε αυτοματοποιημένη επεξεργασία δεδομένων, συμπεριλαμβανομένης της κατάρτισης "profile", πρέπει σε κάθε περίπτωση να τηρούν τις αρχές της θεμιτής επεξεργασίας, δηλαδή διαφάνεια της επεξεργασίας, σχετική ενημέρωση των υποκειμένων, συμβατότητα με τον αρχικό σκοπό, ελαχιστοποίηση των δεδομένων, ακρίβεια, διαδικασίες επαλήθευσης και επικαιροποίησης και συγκεκριμένο χρόνο τήρησης ανάλογα με τους εκάστοτε επιδιωκόμενους σκοπούς. Ειδικότερα, τα πιστωτικά ιδρύματα πρέπει να μπορούν να εξηγούν και να δικαιολογούν την ανάγκη της χρήσης προσωπικών δεδομένων για την κατάρτιση "profile" για την επίτευξη του εκάστοτε επιδιωκόμενου σκοπού επεξεργασίας, άλλως οφείλουν να χρησιμοποιούν ανωνυμοποιημένα ή ψευδοανωνυμοποιημένα δεδομένα.

11.3.1 Τα πιστωτικά ιδρύματα υποχρεούνται να αξιολογούν με τη μεγαλύτερη δυνατή ακρίβεια τον πιστωτικό κίνδυνο που καλούνται να αναλάβουν ή έχουν αναλάβει, με σκοπό τη μείωση του κινδύνου αφερεγγυότητας των πελατών τους ως προς την αποπληρωμή των οικονομικών υποχρεώσεων που έχουν αναλάβει. Πρόκειται για επεξεργασία που στηρίζεται τόσο σε νομική υποχρέωση, όσο και στα έννομα συμφέροντα των πιστωτικών ιδρυμάτων.

Στο πλαίσιο αυτό, τα πιστωτικά ιδρύματα συλλέγουν όλα τα διαθέσιμα σχετικά δεδομένα (όπως περιουσιακής κατάστασης, συναλλακτικής συμπεριφοράς και συνέπειας, δυσμενών οικονομικών στοιχείων κλπ.) τόσο από τον πελάτη, όσο και από αρχεία δεδομένων οικονομικής συμπεριφοράς που λειτουργούν στη χώρα (πχ. ΤΕΙΡΕΣΙΑΣ ΑΕ) ή σε άλλα κράτη-μέλη της Ευρωπαϊκής Ένωσης, εφόσον συντρέχει περίπτωση, και αξιοποιούν αυτά με τον εκάστοτε προσφορότερο τρόπο, περιλαμβανομένης της χρήσης εξειδικευμένων μοντέλων αξιολόγησης για την κατάρτιση πιστωτικού "profile"και της συνακόλουθης βαθμολόγησης της πιστοληπτικής ικανότητας των πελατών τους, υφιστάμενων ή υποψήφιων.

11.3.2 Τα πιστωτικά ιδρύματα μπορούν να αναθέτουν την ως άνω πιστωτική βαθμολόγηση σε φορείς που έχουν ως δραστηριότητα την επεξεργασία δεδομένων οικονομικής συμπεριφοράς ή/και να αντλούν τέτοια δεδομένα από τέτοιου αντικειμένου δραστηριότητας φορείς που δραστηριοποιούνται στην Ελλάδα ή σε κράτη-μέλη της ΕΕ και λειτουργούν νόμιμα.

11.3.3 Για την κατά τα ανωτέρω επεξεργασία, είναι σε κάθε περίπτωση αναγκαία η πλήρης ενημέρωση του υποκειμένου από το πιστωτικό ίδρυμα και, εάν συντρέχει περίπτωση επεξεργασίας από τρίτο ή άντλησης δεδομένων από τρίτο, η ενημέρωση των υποκειμένων και από τον τρίτο.

11.3.4 Εάν με βάση το κατά τα ανωτέρω "profile" λαμβάνεται πλήρως αυτοματοποιημένη απόφαση, δεν απαιτείται η προηγούμενη συγκατάθεση του πελάτη – υποκειμένου, εφόσον αυτό είναι απολύτως απαραίτητο για την κατάρτιση ή εκτέλεση της σύμβασης. Ωστόσο το υποκείμενο έχει το δικαίωμα να εκφράσει άποψη επί της απόφασης και να την αμφισβητήσει, καθώς και να εξασφαλίσει από το πιστωτικό ίδρυμα την επανεξέταση της υπόθεσης με ανθρώπινη παρέμβαση.

11.4. Το πιστωτικό ίδρυμα οφείλει επίσης, στο πλαίσιο νόμιμης υποχρέωσής του, να συλλέγει πληροφορίες για κάθε πελάτη για την αξιολόγηση της συνολικής του εικόνας (customer profile) για τον σκοπό πρόληψης του ξεπλύματος χρήματος και της χρηματοδότησης της τρομοκρατίας. Προς τούτο τα πιστωτικά ιδρύματα χρησιμοποιούν εξειδικευμένα μοντέλα ανάλυσης των εκάστοτε σχετικών δεδομένων.

11.5 Το πιστωτικό ίδρυμα έχει νόμιμη υποχρέωση να συλλέγει πληροφορίες για κάθε πελάτη επενδυτικών προϊόντων ή πελάτη που λαμβάνει επενδυτικού χαρακτήρα υπηρεσίες με σκοπό την αξιολόγηση των γνώσεων και των εμπειριών του στη διενέργεια των συγκεκριμένων συναλλαγών και την κατάρτιση του επενδυτικού του "profile".

11.6. Επιπροσθέτως, τα πιστωτικά ιδρύματα είναι δυνατόν να καταρτίζουν το συναλλακτικό ή/και το πιστοληπτικό "profile" των πελατών τους, είτε για την προώθηση σε αυτούς νέων προϊόντων ή υπηρεσιών, είτε για την επιδίωξη της αύξησης της χρήσης ήδη χορηγηθέντων.

Στις περιπτώσεις αυτές η νομική βάση της επεξεργασίας συνίσταται καταρχάς στο έννομο συμφέρον των πιστωτικών ιδρυμάτων να αυξήσουν τον κύκλο εργασιών τους χάριν των μετόχων, των εργαζομένων και της πελατείας τους, αλλά και των ίδιων των πελατών, διότι παρέχεται σε αυτούς η δυνατότητα αφενός να ενημερώνονται για τις εξελίξεις στην τραπεζική αγορά και αφετέρου να λαμβάνουν τραπεζικά προϊόντα και υπηρεσίες σύμφωνα με τις εξατομικευμένες ανάγκες τους.

Όμως λόγω της ιδιαιτερότητας των παρεχόμενων προϊόντων ή/και υπηρεσιών και της αποφυγής σύγχυσης της πελατείας των πιστωτικών ιδρυμάτων, η προηγούμενη σχετική συγκατάθεση των πελατών προκρίνεται ως ασφαλέστερη νομική βάση, τουλάχιστον για τα προϊόντα που συνεπάγονται κίνδυνο για τον πελάτη, κατά τα αναφερόμενα στην παρ. 4.3 ανωτέρω.

11.7 Όταν το πιστωτικό ίδρυμα προβαίνει σε συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών φυσικών προσώπων, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης "profile", στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως το επηρεάζουν σημαντικά το πιστωτικό ίδρυμα οφείλει να προβεί σε εκπόνηση εκτίμησης αντικτύπου όσον αφορά την επεξεργασία και τις παραμέτρους της, τις εντεύθεν επιπτώσεις της και τους κινδύνους που συνεπάγεται.

Άρθρο 12

Διαβίβαση προσωπικών δεδομένων σε άλλες χώρες

12.1.1 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 (ΕΟΧ).

12.1.2 Η κατά τα λοιπά διαβίβαση προσωπικών δεδομένων εντός της Ευρωπαϊκής Ένωσης είναι ελεύθερη, εάν πληρούνται οι όροι και οι προϋποθέσεις του Κανονισμού.

12.2.1 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.

12.2.2 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.

12.2.3 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.

12.2.4 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 Κανονισμού.

12.2.5 Σε εξαιρετικές περιπτώσεις, διαβιβάσεις από το πιστωτικό ίδρυμα σε τρίτες χώρες χωρίς απόφαση επάρκειας (παρ. 12.2.2 ανωτέρω) και χωρίς την ύπαρξη κατάλληλων εγγυήσεων (παρ. 12.2.3 ανωτέρω) μπορεί να λαμβάνουν χώρα, εφόσον συντρέχει κάποια από τις παρεκκλίσεις του άρθρου 49 του Κανονισμού. Τέτοιες παρεκκλίσεις περιλαμβάνουν τη λήψη ρητής συγκατάθεσης του υποκειμένου, αφού προηγουμένως το πιστωτικό ίδρυμα ενημερώσει το υποκείμενο για τους κινδύνους που εγκυμονεί η προτεινόμενη διαβίβαση/εις, την εκτέλεση σύμβασης μεταξύ του υποκειμένου και του πιστωτικού ιδρύματος ή για την εφαρμογή προσυμβατικών μέτρων κατόπιν αιτήματος του υποκειμένου ή για τη σύναψη ή εκτέλεση σύμβασης η οποία συνήφθη προς όφελος του υποκειμένου μεταξύ του πιστωτικού ιδρύματος και άλλου προσώπου.

Η συνηθέστερη ίσως τέτοια περίπτωση στην τραπεζική πρακτική είναι όταν η διαβίβαση είναι αναγκαία για την εκτέλεση σύμβασης μεταξύ του πιστωτικού ιδρύματος και του υποκειμένου, όπως η εντολή μεταβίβασης κεφαλαίων σε τρίτες χώρες, εφόσον η διαβίβαση αυτή είναι περιστασιακή και δεν πραγματοποιείται στο πλαίσιο σταθερής συνεργασίας μεταξύ των τραπεζών του εντολέα και του δικαιούχου. Στις περιπτώσεις αυτές το πιστωτικό ίδρυμα οφείλει να ενημερώνει τους πελάτες του ότι για την εκτέλεση της εντολής τα δεδομένά τους θα διαβιβαστούν σε τρίτες χώρες και εφόσον, κατόπιν αυτού η εντολή δοθεί από τον πελάτη, σε αυτήν εμπεριέχεται και η σχετική για τη διαβίβαση συγκατάθεση.

12.2.6 Το πιστωτικό ίδρυμα μπορεί επίσης να διαβιβάσει σε τρίτη χώρα προσωπικά δεδομένα, όταν η διαβίβαση είναι αναγκαία για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, περιλαμβανομένων των προδικαστικών ενεργειών, καθώς και σε οποιαδήποτε περίπτωση επιβάλλεται από νόμο της Ευρωπαϊκής Ένωσης, διεθνείς συνθήκες και δικαστικές αποφάσεις των ελληνικών ή/και των δικαστηρίων των κρατών – μελών της Ευρωπαϊκής Ένωσης. Στην περίπτωση της διαβίβασης για προάσπιση δικαιωμάτων ή εννόμων συμφερόντων δεν απαιτείται η προηγούμενη ενημέρωση του υποκειμένου, εφόσον αυτή περιορίζει τα δικαιώματα του πιστωτικού ιδρύματος ή εφόσον η υποχρέωση ενημέρωσης είναι πιθανόν να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της διαβίβασης.

12.2.7. Ειδικά για διαβίβαση προσωπικών δεδομένων σε τρίτη χώρα βάσει απόφασης δικαστηρίου ή διοικητικής αρχής της τρίτης χώρας που υποχρεώνει το πιστωτικό ίδρυμα σε διαβίβαση δεδομένων, πρέπει να ελέγχεται εάν η απόφαση βασίζεται σε διεθνή συμφωνία μεταξύ της Ελλάδας ή της ΕΕ με την τρίτη χώρα, με την επιφύλαξη άλλων τυχόν λόγων διαβίβασης. Σε περίπτωση διεθνούς συμφωνίας, όπως πχ. της Σύμβασης Αμοιβαίας Δικαστικής Συνδρομής (ΣΑΔΣ), τα πιστωτικά ιδρύματα πρέπει καταρχάς να απορρίπτουν αιτήματα απευθείας διαβίβασης και να παραπέμπουν την αιτούσα αρχή της τρίτης χώρας στην κατά τη συμφωνία αρμόδια εθνική αρχή.

12.2.8. Ελλείψει απόφασης επάρκειας ή κατάλληλων εγγυήσεων ή δεσμευτικών εταιρικών κανόνων και εφόσον δεν ισχύουν οι παραπάνω παρεκκλίσεις, εάν η διαβίβαση είναι απαραίτητη για τους σκοπούς επιτακτικών εννόμων συμφερόντων του, το πιστωτικό ίδρυμα μπορεί να

διαβιβάσει προσωπικά δεδομένα σε τρίτη χώρα ή σε διεθνή οργανισμό, θα πρέπει όμως να έχει εκτιμήσει όλες τις περιστάσεις που σχετίζονται με τη συγκεκριμένη διαβίβαση, η οποία θα πρέπει να είναι μη επαναλαμβανόμενη, να αφορά μικρό αριθμό υποκειμένων και να περιλαμβάνει τις δέουσες εγγυήσεις για την προστασία των δεδομένων του υποκειμένου. Το πιστωτικό ίδρυμα ενημερώνει αφενός το υποκείμενο σχετικά με τη διαβίβαση για τα επιτακτικά έννομα συμφέροντα που επιδιώκει και αφετέρου την εποπτική αρχή για τη διαβίβαση βάσει της συγκεκριμένης παρέκκλισης.

Άρθρο 13

Εκτίμηση Αντικτύπου σχετικά με την προστασία των Προσωπικών Δεδομένων

13.1 Η εκτίμηση αντικτύπου αποτελεί σημαντικό εργαλείο για την εκπλήρωση της υποχρέωσης λογοδοσίας, καθώς παρέχει συνδρομή στα πιστωτικά ιδρύματα, που λειτουργούν ως υπεύθυνοι επεξεργασίας, όχι μόνον να συμμορφώνονται με τις προδιαγραφές του Κανονισμού, αλλά και για να αποδεικνύουν ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για τη διασφάλιση της συμμόρφωσής τους προς τον Κανονισμό. Στο πλαίσιο αυτό, τα πιστωτικά ιδρύματα παρέχουν εκπαίδευση στο προσωπικό τους προκειμένου αυτό να κατανοήσει την ανάγκη να εξετάζει το ενδεχόμενο εκπόνησης εκτίμησης αντικτύπου από το πρώτο στάδιο οποιουδήποτε έργου περιλαμβάνει επεξεργασία προσωπικών δεδομένων και τον τρόπο εκπόνησης αυτής και έχουν καταγεγραμμένη σχετική διαδικασία.

13.2 Τα πιστωτικά ιδρύματα διενεργούν υποχρεωτικά εκτίμηση αντικτύπου, σύμφωνα με τις διατάξεις του άρθρου 35 του Κανονισμού, στο πλαίσιο της γενικής υποχρέωσής τους να εφαρμόζουν μέτρα για την ενδεδειγμένη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων όποτε διενεργούν πράξεις επεξεργασίας που ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, όπως μεταξύ άλλων η λήψη απόφασης αποκλεισμού από προϊόντα ή υπηρεσίες των πιστωτικών ιδρυμάτων.

13.3 Τα πιστωτικά ιδρύματα δύνανται να εκπονούν πρότυπες κλαδικές εξειδικευμένες εκτιμήσεις αντικτύπου, έτσι ώστε να εξετάζονται τα ζητήματα που ανακύπτουν στον χρηματοπιστωτικό τομέα, λόγω εκτέλεσης συγκεκριμένου είδους πράξεων επεξεργασίας κατά το δυνατόν ομοιόμορφα.

13.4 Η εκτίμηση αντικτύπου διενεργείται πριν από την επεξεργασία, επανεξετάζεται διαρκώς και επαναξιολογείται τακτικά. Τα πιστωτικά ιδρύματα αξιολογούν συνεχώς τους κινδύνους που απορρέουν από τις δραστηριότητες επεξεργασίας προσωπικών δεδομένων προκειμένου να εξακριβώνουν πότε μία επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

13.5 Κατ’ ελάχιστο περιεχόμενο οι εκτιμήσεις αντικτύπου που διενεργούν τα πιστωτικά ιδρύματα περιλαμβάνουν. (σύμφωνα με το άρθρο 35 παρ. 7 και τις αιτιολογικές σκέψεις 84 και 90 του Κανονισμού), τα εξής: α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της

επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας, β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους επιδιωκόμενους με αυτή σκοπούς, γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς τον Κανονισμό και τον παρόντα Κώδικα, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων.

13.6 Δεν απαιτείται η εκπόνηση εκτιμήσεων αντικτύπου για επεξεργασίες που αφορούν υφιστάμενα, κατά την έναρξη ισχύος του Κανονισμού, προϊόντα ή και υπηρεσίες, εκτός εάν μετά από το χρονικό σημείο αυτό, συμβεί κάποια αλλαγή στις πράξεις επεξεργασίας (πχ. νέα τεχνολογία), με αποτέλεσμα τα δικαιώματα και οι ελευθερίες των υποκειμένων στα οποία οι επεξεργασίες αφορούν να περιορισθούν ή να αυξηθεί σημαντικά ο αριθμός των υποκειμένων που επηρεάζονται.

13.7 Τα πιστωτικά ιδρύματα φροντίζουν ώστε ο/οι εκτελών/εκτελούντες την επεξεργασία για λογαριασμό τους να συνδράμουν στην κατανόηση και τεκμηρίωση των σχεδιαζόμενων πράξεων επεξεργασίας και στον προσδιορισμό των τυχόν κινδύνων.

13.8 Όταν η εκτίμηση αντικτύπου αποκαλύπτει υψηλούς υπολειπόμενους κινδύνους, για τα δικαιώματα και τις ελευθερίες των υποκειμένων, για τον μετριασμό των οποίων δεν έχουν προβλεφθεί ή ληφθεί μέτρα, το πιστωτικό ίδρυμα ζητά τη γνώμη της Αρχής.

13.9 Τα πιστωτικά ιδρύματα, ως υπεύθυνοι επεξεργασίας, είναι αρμόδια για τη διασφάλιση της διενέργειας και υλοποίησης των εκτιμήσεων αντικτύπου, για τις οποίες υποχρεούνται να ζητούν τη γνώμη των Υπευθύνων Προστασίας Δεδομένων (DPOs) τους, οι οποίοι παρακολουθούν την υλοποίηση των ως άνω εκτιμήσεων.

13.10 Όταν σχεδιαζόμενη επεξεργασία ενδέχεται να έχει σοβαρή επίπτωση στα υποκείμενα των δεδομένων, τα πιστωτικά ιδρύματα ζητούν την γνώμη αυτών με τον κατά περίπτωση πρόσφορο τρόπο, που, λαμβανομένου υπόψη του μεγάλου αριθμού των πελατών τους, μπορεί να είναι δειγματοληπτική ή/και μέσω οργανώσεων καταναλωτών. Εάν η τελική απόφαση του πιστωτικού ιδρύματος διαφέρει από την κατά τα προαναφερθέντα γνώμη των υποκειμένων των δεδομένων, τότε το πιστωτικό ίδρυμα τεκμηριώνει τους λόγους για τους οποίους αποφάσισε να συνεχίσει. Ο υπεύθυνος επεξεργασίας μπορεί να παραλείψει την αναζήτηση της γνώμης πελατών-υποκειμένων όταν αυτή μπορεί να βλάψει τα έννομα συμφέροντά του σε βαθμό δυσανάλογο από τον ενδεχόμενο περιορισμό των δικαιωμάτων αυτών, όπως ιδίως όταν με τη διαδικασία αυτή θα διαρρεύσουν επιχειρηματικά σχέδια και θα πληγεί η ανταγωνιστική θέση του πιστωτικού ιδρύματος.

13.11 Κατά την εκτίμηση του αντικτύπου μιας πράξης επεξεργασίας δεδομένων από διάφορα εμπλεκόμενα μέρη λαμβάνεται υπόψη η

συμμόρφωσή τους με εγκεκριμένο Κώδικα Δεοντολογίας, καθώς και με σχετικές πιστοποιήσεις και άλλες κατάλληλες εγγυήσεις.

Άρθρο 14

Ανάθεση σε εκτελούντες την επεξεργασία

14.1 Τα πιστωτικά ιδρύματα, όπως και κάθε υπεύθυνος επεξεργασίας, δικαιούνται να αναθέτουν την επεξεργασία προσωπικών δεδομένων σε τρίτους, στο πλαίσιο και υπό τις προϋποθέσεις που εκάστοτε υπαγορεύονται από το κανονιστικό και εποπτικό τους πλαίσιο και τον Κανονισμό.
14.2 Το πιστωτικό ίδρυμα διασφαλίζει ότι οι αποδέκτες των δεδομένων, στους οποίους αναθέτει την επεξεργασία τους, παρέχουν επαρκείς διαβεβαιώσεις , ιδίως από πλευράς εμπειρογνωμοσύνης, αξιοπιστίας και πόρων, τεχνικών μέσων και οργανωτικών δομών που θα ανταποκρίνονται στην προς ανάθεση επεξεργασία και τις απαιτήσεις του εφαρμοστέου δικαίου, συμπεριλαμβανομένης της ασφάλειας της επεξεργασίας. Στις περιπτώσεις αυτές μεταξύ του πιστωτικού ιδρύματος-υπεύθυνου επεξεργασίας και του τρίτου-εκτελούντος την επεξεργασία για λογαριασμό του πιστωτικού ιδρύματος συνάπτεται μία σύμβαση. Στη συγκεκριμένη σύμβαση περιγράφεται το αντικείμενο της επεξεργασίας που ανατίθεται, ο σκοπός της, το είδος και οι κατηγορίες των δεδομένων που θα τεθούν υπό επεξεργασία από τον εκτελούντα αυτή, οι σχετικές εντολές του πιστωτικού ιδρύματος προς τον εκτελούντα ή τον τρόπο που αυτές θα δίδονται κατά τη διάρκεια της επεξεργασίας από τον τρίτο, τα οργανωτικά και τεχνικά μέτρα που πρέπει να έχει και να διατηρεί καθόλη τη διάρκεια της σύμβασης ο εκτελών την επεξεργασία και οι αναγκαίες διαβεβαιώσεις και εξασφαλίσεις ότι ο εκτελών θα τηρεί τους όρους του Κανονισμού και της ως άνω σύμβασης. Θα πρέπει, επίσης να προσδιορίζονται οι όροι υπό τους οποίους ο εκτελών θα συνδράμει τον υπεύθυνο και η διάρκεια αυτής της επεξεργασίας.

14.3 Οι εκτελούντες την επεξεργασία οφείλουν να είναι σε θέση να αποδείξουν τη συμμόρφωσή τους ως προς τις υποχρεώσεις τους από τον Κανονισμό και τις συμβάσεις της προηγούμενης παραγράφου στα πιστωτικά ιδρύματα - υπευθύνους επεξεργασίας και στα εποπτικά όργανα αυτών, με τα οποία οφείλουν να συνεργάζονται.

14.4 Κατ΄ ακολουθία των αναφερόμενων στην παρ. 14.1 ανωτέρω, το πιστωτικό ίδρυμα έχει τη δυνατότητα να αναθέτει σε εκτελούντες την επεξεργασία, επεξεργασίες που το ίδιο θα μπορούσε να πραγματοποιήσει. Τέτοιες επεξεργασίες μπορεί να είναι η συλλογή δεδομένων, η κατηγοριοποίησή τους, η έκδοση μηνιαίων λογαριασμών πιστωτικών καρτών κλπ. Δεν πρόκειται, ωστόσο για ανάθεση επεξεργασίας, εάν αφορά σε εργασίες τις οποίες το ίδιο δεν μπορεί αντικειμενικά να εκτελέσει, επειδή λ.χ. αυτές μπορεί να εκτελεσθούν μόνο από δικαστικούς επιμελητές, συμβολαιογράφους, ορκωτούς ελεγκτές κλπ. Στις περιπτώσεις αυτές, ανάλογα με τα πραγματικά περιστατικά, πρόκειται για συμβάσεις εντολής έργου κλπ. μεταξύ δύο ανεξάρτητων μεταξύ τους υπεύθυνων επεξεργασίας ή μεταξύ συνυπεύθυνων επεξεργασίας.

14.5 Οι εκτελούντες την επεξεργασία απαγορεύεται να χρησιμοποιούν τα δεδομένα που τους παρέδωσε ο υπεύθυνος επεξεργασίας -πιστωτικό ίδρυμα- για σκοπούς διαφορετικούς από τους περιγραφόμενους στη σύμβαση ανάθεσης ή να διαθέτουν άμεσα ή έμμεσα, ολικά ή μερικά, τα ως άνω δεδομένα σε τρίτους, στην έννοια των οποίων περιλαμβάνεται και το προσωπικό τους που δεν ασχολείται στη συγκεκριμένη επεξεργασία. Σε οποιαδήποτε τέτοια περίπτωση ο εκτελών την επεξεργασία, πέραν των δικών του ευθυνών, υποχρεούται να καλύψει κάθε ζημιά του πιστωτικού ιδρύματος που ανέθεσε την επεξεργασία, λόγω προστίμων, αποζημιώσεων, δαπανών κάθε μορφής κλπ, περιλαμβανομένης και της αποθετικής ζημιάς λόγω του εντεύθεν πλήγματος της φήμης του.

14.6 Ο εκτελών την επεξεργασία υποχρεούται να ενημερώνει τον υπεύθυνο επεξεργασίας για κάθε παραβίαση των προσωπικών δεδομένων που επεξεργάζεται, αμέσως μόλις περιέλθει σε γνώση του, με κάθε πρόσφορο τρόπο, την αιτία και την έκτασή της, όπως και να συνδράμει έγκαιρα και με κάθε τρόπο τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της προσβολής και την εκπλήρωση των εκ του Κανονισμού σχετικών υποχρεώσεων.

14.7 Το πιστωτικό ίδρυμα, μετά τη λήξη της επεξεργασίας μπορεί κατ΄επιλογή να απαιτήσει από τον εκτελούντα: α) να του επιστρέψει το σύνολο των δεδομένων προσωπικού χαρακτήρα μέσω ασφαλούς αρχείου, ο μορφότυπος του οποίου έχει προσυμφωνηθεί ή/και β) να διαγράψει και να αποδείξει τη διαγραφή όλων των αντιγράφων των δεδομένων προσωπικού χαρακτήρα του πιστωτικού ιδρύματος που επεξεργαζόταν ο εκτελών την επεξεργασία, εκτός εάν το δίκαιο της Ένωσης ή το ελληνικό δίκαιο απαιτεί την αποθήκευση των δεδομένων προσωπικών χαρακτήρα.

14.8 Το πιστωτικό ίδρυμα, επιβλέπει καθ΄όλη τη διάρκεια της επεξεργασίας τη συμμόρφωση των εκτελούντων προς τις υποχρεώσεις που υπέχουν οι τελευταίοι από τις διατάξεις του Κανονισμού και τις σχετικές συμβάσεις ανάθεσης και διενεργεί το ίδιο ή με εξουσιοδοτημένα από αυτό πρόσωπα, ελέγχους και επιθεωρήσεις. Ο εκτελών την επεξεργασία υποχρεούται να διευκολύνει αυτούς τους ελέγχους.

14.9 Ο εκτελών την επεξεργασία για λογαριασμό πιστωτικού ιδρύματος απαγορεύεται να αναθέσει περαιτέρω την επεξεργασία, ολικά ή μερικά, σε τρίτο εάν προηγουμένως ο υπεύθυνος επεξεργασίας δεν έχει εγκρίνει την περαιτέρω ανάθεση. Ο εκτελών την επεξεργασία επιβάλει στον υπεργολάβο του τουλάχιστον τις ίδιες υποχρεώσεις που έχει έναντι του υπευθύνου μέσω μεταξύ τους σύμβασης που βρίσκεται σε κάθε περίπτωση στη διάθεση του υπευθύνου. Ο εκτελών την επεξεργασία παραμένει πλήρως υπόλογος έναντι του υπευθύνου για τις πράξεις ή παραλείψεις του υπεργολάβου του αναφορικά με την επεξεργασία που του ανατέθηκε και τα σχετικά προσωπικά δεδομένα.

Άρθρο 15

15.1 Το πιστωτικό ίδρυμα είναι δυνατόν να λειτουργεί ως υπεύθυνος επεξεργασίας προσωπικών δεδομένων πελατών του για την εξυπηρέτηση

ενός συγκεκριμένου σκοπού επεξεργασίας παράλληλα με άλλο φορέα ο οποίος επεξεργάζεται τα ίδια, ολικά ή μερικά, προσωπικά δεδομένα για την εξυπηρέτηση άλλου διακριτού σκοπού.

Στις περιπτώσεις αυτές δεν τίθεται θέμα συνυπευθυνότητας των δύο φορέων, αλλά για δύο ανεξάρτητους υπευθύνους επεξεργασίας.

Σε αυτή την κατηγορία, όπως προαναφέρθηκε (παρ. 14.4 ανωτέρω), ανήκουν οι περιπτώσεις ανάθεσης εργασιών σε δικαστικούς επιμελητές, συμβολαιογράφους κλπ. Επίσης τέτοια περίπτωση συντρέχει όταν το πιστωτικό ίδρυμα εκδίδει "co-branded" κάρτες σε συνεργασία με εμπορική επιχείρηση (βλ. παρ. 16.2 κατωτέρω).

15.2 Το πιστωτικό ίδρυμα μπορεί να είναι από κοινού υπεύθυνο επεξεργασίας με άλλο φορέα, όπως πχ. συμβαίνει στην περίπτωση χορήγησης κοινοπρακτικών δανείων από περισσότερες της μίας τράπεζες. Στις περιπτώσεις αυτές τα εμπλεκόμενα συνυπεύθυνα επεξεργασίας πιστωτικά ιδρύματα μεριμνούν για τον σαφή καθορισμό των ορίων ευθύνης καθενός αναφορικά με την επεξεργασία των προσωπικών δεδομένων των ενεχόμενων φυσικών προσώπων και ιδίως ως προς την ενημέρωση αυτών και την ανταπόκριση στην άσκηση των κατά τον Κανονισμό δικαιωμάτων τους.

Άρθρο 16

Τα πιστωτικά ιδρύματα

ως Εκτελούντα την Επεξεργασία

16.1 Τα πιστωτικά ιδρύματα στο πλαίσιο της λειτουργίας τους, ενδέχεται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για τρίτους – υπευθύνους επεξεργασίας. Οι υποχρεώσεις του πιστωτικού ιδρύματος ως εκτελούντος την επεξεργασία διέπονται από το παρόν άρθρο και από το άρθρο 14 του παρόντος Κώδικα, οι διατάξεις του οποίου εφαρμόζονται ανάλογα και στην περίπτωση αυτή.

16.2 Κατ΄ ακολουθία των προαναφερόμενων, συνήθης περίπτωση πιστωτικού ιδρύματος-εκτελούντος την επεξεργασία είναι η, μετά την εκχώρηση απαιτήσεων του πιστωτικού ιδρύματος σε τρίτο, ανάθεση από τον εκδοχέα της διαχείρισης των μεταβιβασθεισών απαιτήσεων υπό τις συγκεκριμένες οδηγίες του.
Αντίθετα, δεν συντρέχει περίπτωση εκτέλεσης επεξεργασίας από το πιστωτικό ίδρυμα ενδεικτικά όταν ανατίθεται σε αυτό η πίστωση των αποδοχών εργαζομένων από τον εργοδότη τους (γιατί στην περίπτωση αυτή το πιστωτικό ίδρυμα είναι εντολοδόχος για την διενέργεια πράξεων πληρωμών, τις οποίες ο εργοδότης-εντολέας δεν μπορεί να εκτελέσει, ώστε το πιστωτικό ίδρυμα είναι υπεύθυνος επεξεργασίας για τον σκοπό της εκπλήρωσης της εντολής και ο εργοδότης είναι υπεύθυνος επεξεργασίας για τον σκοπό της εκπλήρωσης της υποχρέωσης καταβολής των αποδοχών του προσωπικού του), όταν το πιστωτικό ίδρυμα εκδίδει σε συνεργασία με επιχείρηση-πελάτη του κάρτες "co-branded", (γιατί το πιστωτικό ίδρυμα είναι

υπεύθυνο για την έκδοση και διαχείριση των καρτών που μόνο αυτό μπορεί να εκδώσει και η επιχείρηση είναι υπεύθυνη επεξεργασίας για την εξόφληση του τμήματος των προϊόντων ή/και υπηρεσιών που πωλεί με τη χρήση των καρτών) ή όταν το πιστωτικό ίδρυμα εκτελεί πληρωμές κατ' εντολή πελατών τους.

16.3 Σε κάθε περίπτωση τα πιστωτικά ιδρύματα μεριμνούν ώστε οι συμβάσεις τους με τρίτους που αφορούν (και) στην επεξεργασία προσωπικών δεδομένων να καταρτίζονται με την απαιτούμενη ακρίβεια όσον αφορά στο αντικείμενο και στις υποχρεώσεις, τις ευθύνες και τα δικαιώματα κάθε συμβαλλομένου, ώστε να καθίσταται σαφές πότε συντρέχει περίπτωση εκτέλεσης της επεξεργασίας ή συνεργασίας δύο ανεξάρτητων υπεύθυνων επεξεργασίας ή συνυπεύθυνων.

Κεφάλαιο Γ'

Δικαιώματα των υποκειμένων και διασφάλιση της άσκησής τους

Ενότητα 1

Δικαιώματα

Άρθρο 17

Διαφανής ενημέρωση

17.1 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.

17.2 Τα πιστωτικά ιδρύματα στο πλαίσιο των αρχών για τη θεμιτή και με διαφάνεια επεξεργασία των δεδομένων προσωπικού χαρακτήρα, οφείλουν, να ενημερώνουν το υποκείμενο των δεδομένων για την ταυτότητά τους 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 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.

17.3 Όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από τον πελάτη- υποκείμενο των δεδομένων, το πιστωτικό ίδρυμα, παρέχει στο υποκείμενο των δεδομένων τις κατά την προηγούμενη παράγραφο πληροφορίες κατά τη λήψη αυτών. 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. 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.

17.4 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: α) η παροχή πληροφοριών στο υποκείμενο αποδεικνύεται αδύνατη ή θα απαιτούσε δυσανάλογη προσπάθεια (π.χ. ανύπαρκτα ή ελλιπή στοιχεία επικοινωνίας με τους πελάτες-υποκείμενα) ή είναι πιθανόν να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της επεξεργασίας (π.χ. παροχή στοιχείων που αποδυναμώνουν την άσκηση νόμιμου δικαιώματος), ή β) η απόκτηση ή η κοινολόγηση των δεδομένων προβλέπεται ρητώς σε νόμο που παρέχει τα κατάλληλα μέτρα για την προστασία των εννόμων συμφερόντων των υποκειμένων (π.χ. ΓΕΜΗ, φορολογική αρχή κλπ), ή γ) η πληροφορία υπόκειται σε επαγγελματικό απόρρητο.

17.5 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 είναι αποτελεσματικός.

17.6 Η κατά τα παραπάνω ενημέρωση που παρέχεται πρέπει να είναι συνοπτική, διαφανής, κατανοητή, με απλή διατύπωση και σε εύκολα προσβάσιμη μορφή ιδίως όταν πρόκειται για ενημέρωση απευθυνόμενη σε ανηλίκους. Οι ενημερώσεις παρέχονται γραπτώς ή με άλλα πρόσφορα κατά περίπτωση μέσα, όπως ηλεκτρονικά. Όταν ζητείται από το υποκείμενο των δεδομένων, η ενημέρωση μπορεί να δίνεται προφορικά, υπό την προϋπόθεση ότι το υποκείμενο των δεδομένων έχει αποδεδειγμένα ταυτοποιηθεί.

17.7 Όταν το πιστωτικό ίδρυμα προτίθεται να επεξεργαστεί περαιτέρω τα δεδομένα προσωπικού χαρακτήρα για άλλο σκοπό από εκείνον για τον οποίο συλλέχθηκαν, το πιστωτικό ίδρυμα παρέχει στους πελάτες-υποκείμενα των δεδομένων, πριν την έναρξη της επεξεργασίας αυτής, κάθε πληροφορία που είναι αναγκαία για τη διασφάλιση θεμιτής και με διαφάνεια επεξεργασίας ανεξάρτητα εάν τα δεδομένα είχαν συλλεγεί από το υποκείμενο ή από άλλες πηγές.

Άρθρο 18

18.1 Το πιστωτικό ίδρυμα διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων που προβλέπονται στον Κανονισμό (άρθρα 15 έως 22) και στον παρόντα Κώδικα και παρέχει τα μέσα για ηλεκτρονική υποβολή των αιτημάτων, ιδίως όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία με ηλεκτρονικά μέσα.

18.2 Το πιστωτικό ίδρυμα περιγράφει τον τρόπο εξακρίβωσης της ταυτότητας του υποκειμένου κατά την άσκηση των δικαιωμάτων του και τα στοιχεία που ζητά για την επιβεβαίωση της ταυτότητας. Στις περιπτώσεις που το πιστωτικό ίδρυμα μπορεί να αποδείξει ότι δεν είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου των δεδομένων, δεν ανταποκρίνεται στα σχετικά αιτήματα, μέχρις ότου το υποκείμενο των δεδομένων να παράσχει συμπληρωματικές πληροφορίες που επιτρέπουν την αναμφίβολη εξακρίβωση της ταυτότητάς του.

18.3 Οι πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων και κάθε ανακοίνωση για την άσκηση των κατά τα ανωτέρω δικαιωμάτων, περιλαμβανομένης της ανακοίνωσης παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, παρέχονται δωρεάν.

Εάν όμως το αίτημα του υποκειμένου των δεδομένων είναι προδήλως αβάσιμο ή υπερβολικό, ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα τους, είτε το υποκείμενο υποχρεούται να καλύψει πλήρως το κόστος της αιτούμενης ενέργειας, είτε το πιστωτικό ίδρυμα δικαιούται να αρνηθεί να δώσει συνέχεια στο αίτημα, κατά τη κρίση του, ενημερώνοντας σχετικά το υποκείμενο πριν από την ανταπόκρισή του σε αυτά.

Άρθρο 19

Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

19.1 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:

- τις κατηγορίες των υπό επεξεργασία δεδομένων (πχ. δεδομένα ταυτοπροσωπίας, επικοινωνίας, εισοδηματικής κατάστασης κλπ.),
- 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),
- την προέλευσή τους (πχ. από τον οφειλέτη, από την εταιρεία ΤΕΙΡΕΣΙΑΣ ΑΕ ή άλλα αρχεία δεδομένων οικονομικής συμπεριφοράς, από υποθηκοφυλακεία κλπ.),
- τα της άσκησης των κατά τον Κανονισμό δικαιωμάτων του, περιλαμβανομένου του δικαιώματος καταγγελίας στην Αρχή,
- εάν στην επεξεργασία περιλαμβάνεται αυτοματοποιημένη λήψη απόφασης ή κατάρτιση προφίλ.

19.2 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 παράγονται, ανά προϊόν ή υπηρεσία, από τα συστήματα πληροφορικής που διαθέτει. Αναπαραγωγή και αποστολή δεδομένων που έχουν ήδη διατεθεί στον πελάτη μπορεί να γίνει μόνο με την επιβάρυνση του πελάτη με το σχετικό κόστος, (βλ. και άρθρο 18, παρ. 3 ανωτέρω), ενώ αναπαραγωγή με διαφορετικό τρόπο μπορεί να γίνει μόνο εάν είναι ευχερώς συστημικά εφικτό και πάλι με την αντίστοιχη επιβάρυνση του αιτούντος πελάτη.

19.3 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, π.χ. αρχεία αποβιωσάντων στα οποία περιέχονται στοιχεία κληρονόμων.

19.4 Εάν προσωπικά δεδομένα που αναφέρονται σε τρίτα φυσικά πρόσωπα περιέχονται στο αρχείο πελάτη που ασκεί το δικαίωμα πρόσβασης (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.

19.5 Στην περίπτωση αυτοματοποιημένης επεξεργασίας ή κατάρτισης profile, 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.

19.6 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.

19.7 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.

19.8 Τα πιστωτικά ιδρύματα ως υπεύθυνοι επεξεργασίας διασφαλίζουν, την ικανοποίηση του κατά τις προηγούμενες παρ. 6 και 7 δικαιώματος πρόσβασης των υποκειμένων στα σχετικά δεδομένα, χωρίς να απαιτείται επίκληση ειδικότερων λόγων για την άσκηση του δικαιώματος αυτού και χωρίς την προηγούμενη κρίση από την πλευρά του πιστωτικού ιδρύματος ως προς το αν δικαιολογείται η άσκηση του δικαιώματος αυτού ή όχι.

Άρθρο 20

Δικαίωμα διόρθωσης

20.1 Το υποκείμενο των δεδομένων έχει την υποχρέωση και το δικαίωμα να απαιτήσει από το πιστωτικό ίδρυμα την, χωρίς αδικαιολόγητη καθυστέρηση, διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν.

20.2 Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα που το αφορούν.

20.3 Το πιστωτικό ίδρυμα προβαίνει στην διόρθωση ή συμπλήρωση στους προβλεπόμενους από τον Κανονισμό χρόνους ανταπόκρισης (άρθρο 12 παρ. 3), υπό την προϋπόθεση ότι το υποκείμενο των δεδομένων θα υποβάλει σε αυτό την απαιτούμενη κατά περίπτωση πλήρη σχετική τεκμηρίωση.

Άρθρο 21

Δικαίωμα διαγραφής (δικαίωμα στη λήθη)

21.1 Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητεί τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εάν η διατήρηση των εν λόγω δεδομένων παραβιάζει τον Κανονισμό ή τον παρόντα Κώδικα ή το ελληνικό δίκαιο.

21.2 Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητεί τη διαγραφή και την παύση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν, ιδίως εάν τα δεδομένα αυτά δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβάλλονταν κατ' άλλο τρόπο σε επεξεργασία, είτε εάν το υποκείμενο των δεδομένων ανακαλέσει τη συγκατάθεσή του επί της οποίας βασίζεται η επεξεργασία ή εάν αντιτάσσεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν και δεν υπάρχει άλλη νομική βάση για τη συνέχιση αυτής είτε εάν η επεξεργασία δεν ήταν σύμφωνη με το νόμο ή υπάρχει νομική υποχρέωση για τη διαγραφή.

21.3 Το πιστωτικό ίδρυμα προβαίνει στη διαγραφή των σχετικών δεδομένων από το φυσικό και από το ηλεκτρονικό αρχείο στους προβλεπόμενους από τον Κανονισμό (άρθρο 12, παρ. 3) και τον παρόντα Κώδικα (άρθρο 27) 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, κατά το άρθρο 9 ανωτέρω, χρόνου τήρησης αυτών, εκτός εάν πρόκειται για επουσιώδη δεδομένα που ουδεμία επιρροή ασκούν στα δικαιώματα και τα έννομα συμφέροντα του πιστωτικού ιδρύματος.

Άρθρο 22

Δικαίωμα περιορισμού της επεξεργασίας

22.1 Το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από το πιστωτικό ίδρυμα τον περιορισμό της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα:

α) 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,

β) η επεξεργασία έχει κριθεί παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,

γ) 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,

δ) 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.

22.2 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.

22.3 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.

Άρθρο 23

Υποχρέωση γνωστοποίησης προς τρίτους

23.1 Το πιστωτικό ίδρυμα ανακοινώνει κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των

δεδομένων που διενεργείται σύμφωνα με τις διατάξεις του Κανονισμού και του παρόντος Κώδικα σε κάθε αποδέκτη στον οποίο γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα πριν από τη διόρθωση ή τη διαγραφή, εκτός εάν αυτό αποδεικνύεται ανέφικτο ή εάν συνεπάγεται δυσανάλογη προσπάθεια.

23.2 Το πιστωτικό ίδρυμα ενημερώνει το υποκείμενο των δεδομένων σχετικά με τους εν λόγω αποδέκτες, εφόσον αυτό ζητηθεί από αυτό.

Άρθρο 24

Δικαίωμα στη φορητότητα των δεδομένων

24.1 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.

24.2 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.

24.3 Το δικαίωμα στη φορητότητα ικανοποιείται με την επιφύλαξη των διατάξεων που αφορούν στο δημόσιο συμφέρον ή σε εκπλήρωση νομικής υποχρέωσης του πιστωτικού ιδρύματος - υπεύθυνου επεξεργασίας, όπως π.χ. στην περίπτωση νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Επίσης, το δικαίωμα στη φορητότητα δεν ικανοποιείται και σε περίπτωση που αφορά σε δεδομένα τρίτων, τα οποία δεν μπορούν να διαχωριστούν όπως π.χ. κοινοί λογαριασμοί, συνυπόχρεοι δανείων κλπ.

24.4 Το δικαίωμα στη φορητότητα δεν συνεπάγεται την διαγραφή των δεδομένων στα οποία αφορά η φορητότητα, για την οποία ισχύουν τα αναφερόμενα στο σχετικό άρθρο 21, παρ.3 παραπάνω.

24.5 Δεν περιλαμβάνονται στο πεδίο εφαρμογής του δικαιώματος στη φορητότητα τα προσωπικά δεδομένα που παράγονται ή συνάγονται από την επεξεργασία, όπως π.χ. η κατάρτιση πιστοληπτικού profile, διότι δεν

πρόκειται για δεδομένα που παρέχονται από το υποκείμενο, αλλά από την ανάλυση δεδομένων που δεν αφορούν μόνο στην τυχόν χορηγητική σύμβαση μεταξύ πιστωτικού ιδρύματος και υποκειμένου.

Άρθρο 25

Δικαίωμα εναντίωσης

25.1 Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η οποία βασίζεται στην αναγκαιότητα εκπλήρωσης καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, περιλαμβανομένης της κατάρτισης profile. 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, κατά το άρθρο 10 ανωτέρω, χρόνου τήρησης αυτών.

25.2 Εάν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης profile, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση. Όταν το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονται πλέον σε επεξεργασία για τους σκοπούς αυτούς. 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, ηλ. μηνυμάτων, sms κλπ.

25.3 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 επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με τον Κανονισμό, εκτός εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που ασκείται για λόγους δημόσιου συμφέροντος.

25.4 Το αργότερο κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων, το πιστωτικό ίδρυμα επισημαίνει το δικαίωμα του υποκειμένου για εναντίωση, το οποίο περιγράφεται με σαφήνεια και χωριστά από οποιαδήποτε άλλη πληροφορία.

Επιπροσθέτως, το πιστωτικό ίδρυμα 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.

Άρθρο 26

Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

26.1 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.

26.2 Η λήψη απόφασης που λαμβάνεται βάσει αποκλειστικά αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, επιτρέπεται: (α) 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, (β) 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, (γ) όταν το υποκείμενο των δεδομένων παρέσχε τη ρητή προς τούτο συγκατάθεσή του.

26.3 Στις περιπτώσεις (α) και (γ) της προηγούμενης παρ. 26.2, 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. Τα δικαιώματα αυτά μπορούν να ασκηθούν εντός αποκλειστικής προθεσμίας τριάντα (30) ημερών από τη γνώση της απόφασης.

Ενότητα 2

Χρόνοι ανταπόκρισης των πιστωτικών ιδρυμάτων

Άρθρο 27

27.1 Το πιστωτικό ίδρυμα υποχρεούται να απαντά στα κατά τα προαναφερθέντα αιτήματα των πελατών του-υποκειμένων των δεδομένων χωρίς καθυστέρηση και σε κάθε περίπτωση εντός μηνός από την παραλαβή του αιτήματος. Η εν λόγω προθεσμία μπορεί να παραταθεί κατά δύο ακόμη μήνες, εφόσον απαιτείται λόγω πολυπλοκότητας του αιτήματος ή/και του αριθμού των αιτημάτων, μετά από σχετική ενημέρωση του αιτούντος-υποκείμενου των δεδομένων για την εν λόγω παράταση, καθώς και για τους

λόγους της καθυστέρησης εντός της παραπάνω αρχικής μηνιαίας προθεσμίας. Εάν το υποκείμενο των δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα, η ενημέρωση παρέχεται, εάν είναι δυνατόν, με ηλεκτρονικά μέσα, εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό. Το πιστωτικό ίδρυμα διαμορφώνει και παρέχει ηλεκτρονικά μέσα για την υποβολή των αιτημάτων, ιδίως όταν τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία με ηλεκτρονικά μέσα.

27.2 Εάν το πιστωτικό ίδρυμα δεν ενεργήσει επί του αιτήματος του υποκειμένου των δεδομένων, το πιστωτικό ίδρυμα ενημερώνει το υποκείμενο των δεδομένων, χωρίς καθυστέρηση και το αργότερο εντός μηνός από την παραλαβή του αιτήματος, για τους λόγους για τους οποίους δεν ενήργησε και για τη δυνατότητα υποβολής καταγγελίας στην Αρχή και άσκησης δικαστικής προσφυγής.

Ενότητα 3

Προστασία των ανηλίκων

Άρθρο 28

Προστασία ανηλίκων

28.1 Έχοντας υπόψη ότι, σύμφωνα με το άρθρο 136 ΑΚ, ανήλικος που συμπλήρωσε το 15ο έτος της ηλικίας του είναι ικανός να συνάπτει συμβάσεις εργασίας ως μισθωτός, εφόσον συναινούν οι ασκούντες την επιμέλειά του, κατ΄ακολουθία, υπό τις ίδιες προϋποθέσεις, αυτός μπορεί να ανοίξει σε πιστωτικό ίδρυμα καταθετικό λογαριασμό μισθοδοσίας, οπότε το πιστωτικό ίδρυμα επεξεργάζεται τα προσωπικά του δεδομένα αποκλειστικά και μόνο για την λειτουργία της συγκεκριμένης σύμβασης και τις εντεύθεν νομικές κανονιστικές ή εποπτικές υποχρεώσεις του πιστωτικού ιδρύματος, αποκλειομένης οποιασδήποτε άλλης επεξεργασίας, περιλαμβανομένης αυτής για σκοπούς προώθησης προϊόντων ή υπηρεσιών.

28.2 Έχοντας υπόψη ότι οι ανήλικοι κατά τεκμήριο έχουν μικρότερη επίγνωση των κινδύνων και των συνεπειών από την επεξεργασία των προσωπικών τους δεδομένων, όπως και των δικαιωμάτων που μπορούν να ασκήσουν για την προστασία τους, τα πιστωτικά ιδρύματα λαμβάνουν σε κάθε περίπτωση ειδική μέριμνα για την προστασία των προσωπικών δεδομένων αυτών και δεν επεξεργάζονται αυτά για σκοπούς προώθησης προϊόντων ή υπηρεσιών των ίδιων ή τρίτων ούτε για την λήψη αυτοματοποιημένων αποφάσεων περιλαμβανομένης της κατάρτισης "profile".

Κεφάλαιο Δ΄

Η εσωτερική οργάνωση των πιστωτικών ιδρυμάτων

Άρθρο 29

Υπεύθυνος Προστασίας Δεδομένων

(Data Protection Officer “DPO”)

29.1 Κάθε πιστωτικό ίδρυμα, ορίζει Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ), και εξασφαλίζει την ανεξαρτησία του στην εκτέλεση των κατά τον Κανονισμό και την επόμενη παράγραφο του άρθρου αυτού καθηκόντων του, όπως και ότι τα ως άνω καθήκοντά του δεν έρχονται σε σύγκρουση με τυχόν άλλα καθήκοντα που του έχουν ανατεθεί. Ο ΥΠΔ κάθε πιστωτικού ιδρύματος αναφέρεται απευθείας στην Διευθύνοντα Σύμβουλο του πιστωτικού ιδρύματος ή σε αναπληρωτή του.

29.2 Ο ΥΠΔ πρέπει να έχει άριστη γνώση του Κανονισμού, να διαθέτει ουσιαστική γνώση και εμπειρία στο δίκαιο και τις πρακτικές για την προστασία των προσωπικών δεδομένων και καλή γνώση της λειτουργίας των πιστωτικών ιδρυμάτων, των πράξεων επεξεργασίας που αυτά διενεργούν, καθώς και των συστημάτων πληροφορικής και των ειδικών αναγκών ασφαλείας, με επαγγελματική και προσωπική ακεραιότητα και υψηλό αίσθημα επαγγελματικής δεοντολογίας και ικανότητα εκπλήρωσης των προβλεπόμενων στον Κανονισμό καθηκόντων του, θωρακίζεται δε θεσμικά αναλόγως 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.

29.3 Ο ΥΠΔ έχει τα καθήκοντα που αναφέρονται στο άρθρο 39 του Κανονισμού, ιδίως δε τα κάτωθι:

(α) ενημερώνει και συμβουλεύει το πιστωτικό ίδρυμα και τους υπαλλήλους οι αρμοδιότητες των οποίων άπτονται της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, για την εφαρμογή και συμμόρφωσή τους με τον Κανονισμό, τη σχετική νομοθεσία και τον παρόντα Κώδικα,

(β)παρακολουθεί τη συμμόρφωση με τον Κανονισμό, ~~και~~ τη σχετική νομοθεσία και τον παρόντα Κώδικα,

(γ) συμμετέχει στην εκτίμηση αντικτύπου και την προηγούμενη διαβούλευση με την αρχή, στην κατάρτιση και τήρηση του αρχείου δραστηριοτήτων επεξεργασίας, στη διαδικασία γνωστοποίησης παραβίασης δεδομένων προς την εποπτική αρχή και της ανακοίνωσης στα υποκείμενα όπου απαιτείται, συνδράμει στην εκτίμηση του ενδεδειγμένου επιπέδου ασφαλείας με βάση την προσέγγιση του κινδύνου στις πράξεις επεξεργασίας και ενημερώνει για τους μηχανισμούς που απαιτούνται για τη διασυνοριακή διαβίβαση δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς,

(δ) αποτελεί το σημείο επικοινωνίας με τα υποκείμενα των υπό επεξεργασία από το πιστωτικό ίδρυμα προσωπικών δεδομένων, τα οποία μπορούν να επικοινωνούν μαζί του για κάθε θέμα σχετικό με την εν λόγω επεξεργασία και την άσκηση των δικαιωμάτων τους,

(ε) ενεργεί ως σημείο επικοινωνίας με την ΑΠΔΠΧ, με την οποία συνεργάζεται και αφενός τη διευκολύνει στην άσκηση των αρμοδιοτήτων της, ιδίως στην πρόσβασή της στα αναγκαία έγγραφα και πληροφορίες που αφορούν στις δραστηριότητες επεξεργασίας, τηρουμένου του καθήκοντος απορρήτου ή εμπιστευτικότητας και αφετέρου ζητά τη γνώμη της σε περιπτώσεις υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων.

29.4 Ο ΥΠΔ δεν καθορίζει τους σκοπούς και τα μέσα κάθε επεξεργασίας του πιστωτικού ιδρύματος, ούτε εκπροσωπεί το πιστωτικό ίδρυμα ενώπιον Δικαστηρίων ή της ΑΠΔΠΧ.

29.5 Τα στοιχεία επικοινωνίας του ΥΠΔ, αλλά όχι απαραίτητα και το ονοματεπώνυμό του καθίστανται γνωστά στους ενδιαφερόμενους, ώστε να διασφαλίζεται η ακώλυτη και απευθείας πρόσβαση και επικοινωνία τους μαζί του. Προς τούτο τα ως άνω στοιχεία επικοινωνίας δημοσιοποιούνται, μεταξύ άλλων, στην ιστοσελίδα κάθε πιστωτικού ιδρύματος, περιλαμβάνονται στους γενικούς όρους συναλλαγών, όπως και στην ιστοσελίδα του, όπου καταχωρούνται τα κείμενα ενημέρωσης των υποκειμένων για την επεξεργασία των προσωπικών τους δεδομένων.

29.6 Το πιστωτικό ίδρυμα γνωστοποιεί στην ΑΠΔΠΧ τα πλήρη στοιχεία του ΥΠΔ.

29.7 Σε περίπτωση ομίλου επιχειρήσεων το πιστωτικό ίδρυμα μπορεί να ορίσει ένα μόνο ΥΠΔ, υπό την προϋπόθεση ότι αυτός είναι εύκολα προσβάσιμος σε κάθε εγκατάσταση για τα υποκείμενα των δεδομένων, την εποπτική αρχή και τους υπαλλήλους και ότι διασφαλίζεται ότι αυτός, συνεπικουρούμενος από ομάδα, εφόσον απαιτείται, επιτελεί αποτελεσματικά το σύνολο των καθηκόντων του έναντι όλων των εταιρειών του ομίλου.

Κεφάλαιο Ε’

Ασφάλεια και καταστροφή προσωπικών δεδομένων

Άρθρο 30

Ασφάλεια δεδομένων προσωπικού χαρακτήρα

30.1 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.

30.2 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: i) τις τεχνολογικές λύσεις που χρησιμοποιούν, ii) τις υπηρεσίες που αναθέτουν σε εξωτερικούς παρόχους και iii) το τεχνικό περιβάλλον των πελατών. Εξετάζουν τους κινδύνους που συνδέονται με τις επιλεγμένες τεχνολογικές πλατφόρμες, με την 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.

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.

30.3 Τα πιστωτικά ιδρύματα 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.

30.4 Τα πιστωτικά ιδρύματα εφαρμόζουν μέτρα ασφάλειας τα οποία ενσωματώνουν πολλαπλά επίπεδα ασφάλειας, στο πλαίσιο των οποίων η αποτυχία μίας γραμμής άμυνας αντιμετωπίζεται από την επόμενη γραμμή άμυνας.

30.5 Τα πιστωτικά ιδρύματα 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.

30.6 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.

30.7 Κατά τον σχεδιασμό, την ανάπτυξη και τη συντήρηση ψηφιακών υπηρεσιών , 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/ή η αρχειοθέτηση, καθώς και η απεικόνιση δεδομένων προσωπικού χαρακτήρα διατηρούνται στα απολύτως αναγκαία επίπεδα.

30.8 Τα πιστωτικά ιδρύματα 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.

30.9.Τα πιστωτικά ιδρύματα εφαρμόζουν κατάλληλες διαδικασίες παρακολούθησης, ιχνηλασίας 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.

30.10 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.

Άρθρο 31

Παραβίαση προσωπικών δεδομένων

31.1 Παραβίαση δεδομένων συνιστά κάθε περιστατικό παραβίασης της ασφάλειας της επεξεργασίας που συνεπάγεται αλλοίωση, μεταβολή, άκαιρη διαγραφή ή διαβίβαση προσωπικών δεδομένων σε μη νόμιμο αποδέκτη αυτών, όπως και πρόσβαση σε προσωπικά δεδομένα από μη νόμιμους αποδέκτες αυτών, ανεξάρτητα εάν αυτό είναι αποτέλεσμα ανθρώπινης ενέργειας ή παράλειψης ή τυχαίο, απρόβλεπτο, περιστατικό.

31.2 Τα πιστωτικά ιδρύματα εφαρμόζουν διαδικασίες εντοπισμού περιστατικών παραβίασης, περιλαμβανομένης της άμεσης διερεύνησης σχετικών καταγγελιών πελατών ή αναφορών απασχολούμενων σε αυτά, προκειμένου να διαπιστώσουν εάν πράγματι υπήρξε παραβίαση και την έκταση αυτής.

31.3 Το προσωπικό των πιστωτικών ιδρυμάτων υποχρεούται να προωθεί άμεσα στην αρμόδια υπηρεσία οποιαδήποτε, έστω και υπόνοια, παραβίασης, όπως και κάθε καταγγελία παραβίασης ή σχετικό παράπονο πελάτη. Τα πιστωτικά ιδρύματα μεριμνούν ώστε οι κάθε μορφής συνεργάτες, οι εκτελούντες για λογαριασμό τους επεξεργασίες, όπως και οι συνυπεύθυνοι με αυτά, να αναλαμβάνουν ρητά αντίστοιχες υποχρεώσεις και να συνεργάζονται με αυτά για την άμεση αντιμετώπιση τέτοιων περιστατικών και τον περιορισμό των επιπτώσεών τους.

31.4 Τα πιστωτικά ιδρύματα αμέσως μόλις εντοπισθεί περιστατικό παραβίασης λαμβάνουν κάθε πρόσφορο τεχνικό ή/και οργανωτικό μέτρο για την αντιμετώπισή του, τον περιορισμό των επιπτώσεών του στους πελάτες

- υποκείμενα των δεδομένων και την αποτροπή επανεμφάνισής του στο μέλλον.
31.5 Τα πιστωτικά ιδρύματα γνωστοποιούν στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα κάθε περιστατικό παραβίασης, που μετά από αξιολόγηση του κινδύνου διαπιστώνεται ότι μπορεί να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων.
31.6.1 Η κατά την προηγούμενη παρ.31.5 γνωστοποίηση πρέπει να γίνει εντός των πρώτων 72 ωρών από τη γνώση του περιστατικού. Σε αυτή τη γνωστοποίηση περιλαμβάνεται η περιγραφή του, οι ενδεχόμενες συνέπειες και τα ληφθέντα ή προτεινόμενα μέτρα για την αντιμετώπισή του. Η γνωστοποίηση που αφορά στην έκταση των επιπτώσεων ή/και στα μέτρα για την αντιμετώπιση του περιστατικού παραβίασης μπορεί να γίνει διαδοχικά, εφόσον αυτό εύλογα δικαιολογείται από τα χαρακτηριστικά του περιστατικού, οπότε η Αρχή ενημερώνεται σχετικά με την πρώτη γνωστοποίηση.
31.6.2 Σε περίπτωση που η κατά τα ανωτέρω γνωστοποίηση δεν μπορεί να πραγματοποιηθεί εντός της προθεσμίας των 72 πρώτων ωρών από τη γνώση του περιστατικού, το πιστωτικό ίδρυμα πρέπει, με τη γνωστοποίηση, να αιτιολογήσει την καθυστέρηση.
31.7 Σε περίπτωση που η παραβίαση είναι ενδεχόμενο να θέσει σε σοβαρό κίνδυνο τα δικαιώματα των υποκειμένων, στα προσωπικά δεδομένα των οποίων η παραβίαση αφορά, το πιστωτικό ίδρυμα ενημερώνει και αυτά.
31.8 Τα πιστωτικά ιδρύματα τηρούν αρχείο στο οποίο καταχωρούνται τα περιστατικά παραβίασης, οι επιπτώσεις τους οι αντίστοιχες ενέργειες του πιστωτικού ιδρύματος και η σχετική κατά περίπτωση τεκμηρίωση.
31.9 Τα πιστωτικά ιδρύματα απευθύνονται στις αρμόδιες κατά περίπτωση αρχές για την αντιμετώπιση περιστατικών παραβίασης που είτε μπορεί να έχουν ευρύτερες επιπτώσεις, είτε ενδέχεται να είναι αποτέλεσμα αξιόποινων πράξεων και συνεργάζονται με αυτές.
31.10 Στις περιπτώσεις κατά τις οποίες πιστωτικά ιδρύματα είναι από κοινού υπεύθυνοι επεξεργασίας με άλλα πιστωτικά ιδρύματα ή τρίτους, μεταξύ τους συμβάσεις περιέχουν όρους που να καθορίζουν ποιος υπεύθυνος θα έχει την πρωτοβουλία για την εξέταση των περιστατικών παραβίασης και την ευθύνη για την ενημέρωση της Αρχής και των υποκειμένων.

Άρθρο 32

Καταστροφή προσωπικών δεδομένων

32.1 Όταν ο σκοπός επεξεργασίας των προσωπικών δεδομένων επιτευχθεί και εξαντληθεί ο κατά το άρθρο 9 ανωτέρω χρόνος τήρησης αυτών, τα πιστωτικά ιδρύματα υποχρεούνται, με την επιφύλαξη της διάταξης της επόμενης παραγράφου, να καταστρέψουν ή να ανωνυμοποιήσουν τα προσωπικά δεδομένα κατά τρόπο που να μην είναι δυνατή η ταυτοποίηση των φυσικών προσώπων στα οποία αυτά αφορούν.

32.2 Η καταστροφή των προσωπικών δεδομένων συνεπάγεται την πλήρη διαγραφή αυτών από τα λειτουργικά συστήματα του πιστωτικού ιδρύματος, που χρησιμοποιούνται για τη διεξαγωγή των εργασιών του, όχι όμως κατ΄ανάγκη και από τα ιστορικά αρχεία αυτού που δεν συνδέονται με τα ως άνω λειτουργικά συστήματα, δεν είναι προσβάσιμα από τους λειτουργούς του, εκτός από τους υπεύθυνους φύλαξης των συγκεκριμένων αρχείων, μετά από ειδικό προς τούτο αίτημα και δεν χρησιμοποιούνται για την λήψη αποφάσεων.

32.3 Κάθε πιστωτικό ίδρυμα εντάσσει στην πολιτική επεξεργασία των προσωπικών δεδομένων ειδικές διατάξεις για την κατά τα ανωτέρω καταστροφή ή/και ανωνυμοποίηση των προσωπικών δεδομένων και εκπονεί και εφαρμόζει ειδικές προς τούτο διαδικασίες.

Κεφάλαιο Στ΄
΄Ελεγχος συμμόρφωσης και επίλυσης διαφορών

Ενότητα 1
΄Ελεγχος συμμόρφωσης με τις διατάξεις του Κώδικα

Άρθρο 33

33.1 Ο Κώδικας δεσμεύει τα ιδρύματα που συμμετέχουν ή μεταγενέστερα προσχωρούν σε αυτόν, κατά το άρθρο 39 κατωτέρω. Οι διατάξεις του Κώδικα δεν υπερισχύουν του σχετικού νομικού και κανονιστικού πλαισίου περιλαμβανομένου του Κανονισμού, σε περίπτωση δε αμφισβήτησης στην ερμηνεία τους υπερισχύουν οι θεσμικές διατάξεις.

33.2 Μόνη η προσχώρηση στον Κώδικα δεν συνιστά συμμόρφωση με τις ισχύουσες διατάξεις και οι προσχωρούντες σε αυτόν οφείλουν να διεξάγουν τις δικές τους αξιολογήσεις ως προς τη συμμόρφωση με το ισχύον θεσμικό πλαίσιο.

Άρθρο 34

34.1. Έχοντας υπόψη τις διατάξεις του άρθρου 41 του Κανονισμού, τα συμμετέχοντα στον παρόντα Κώδικα πιστωτικά και χρηματοδοτικά ιδρύματα συστήνουν με τον παρόντα Κώδικα Ομάδα Έργου, σκοπός της οποίας είναι η παρακολούθηση της συμμόρφωσης με τον Κώδικα των εκάστοτε συμμετεχόντων σε αυτόν ιδρυμάτων (εφεξής “Ομάδα Έργου του Κώδικα”).
34.2 Στην ως άνω Ομάδα Έργου του Κώδικα συμμετέχουν:

α) Οι Υπεύθυνοι Προστασίας Δεδομένων των πιστωτικών και χρηματοδοτικών ιδρυμάτων που εκάστοτε συμμετέχουν στον Κώδικα ή οι αντικαταστάτες τους στην Ελλάδα, στις περιπτώσεις πιστωτικών ιδρυμάτων με έδρα σε άλλο κράτος-μέλος, τα οποία έχουν ορίσει Υπεύθυνο Προστασίας στην έδρα τους, σε επίπεδο ομίλου.

β) Ένας νομικός εξειδικευμένος στην προστασία των προσωπικών δεδομένων.
γ) Ένα στέλεχος εξειδικευμένο στην ασφάλεια συστημάτων, κατά προτίμηση με σχετική εμπειρία στο χώρο των πιστωτικών ιδρυμάτων.

34.3. Τα υπό α της προηγούμενης παρ. 34.2 μέλη της Ομάδας Έργου του Κώδικα εκλέγουν με πλειοψηφία 3/5 του συνόλου αυτών, κάθε δύο (2) έτη, τον νομικό και το εξειδικευμένο στην ασφάλεια συστημάτων στέλεχος, των εδαφίων γ και δ της προηγούμενης παραγράφου, για διετή θητεία. Η ως άνω εκλογή ολοκληρώνεται τουλάχιστον έναν πλήρη μήνα πριν από τη λήξη της θητείας των αποχωρούντων ως άνω μελών, κατά τη διάρκεια του οποίου οι αποχωρούντες υποχρεούνται να ενημερώσουν πλήρως τους νεοεκλεγέντες για τα πεπραγμένα της θητείας τους και τις τυχόν εκκρεμότητες.

34.4 Τα κατά την προηγούμενη παρ. 34.3 μέλη της Ομάδας Έργου του Κώδικα είναι επανεκλέξιμα για μία ακόμη θητεία.

34.5 Η ετήσια αποζημίωση των μελών της Ομάδας Έργου καθορίζεται με απόφαση των μελών της που λαμβάνεται με πλειοψηφία 4/5 του συνόλου αυτών.

34.6 Όλα μέλη της Ομάδας Έργου του Κώδικα είναι απολύτως ανεξάρτητα κατά την άσκηση των καθηκόντων τους.

Άρθρο 35

Σκοπός της Ομάδας Έργου του Κώδικα είναι η παρακολούθηση της τήρησης του παρόντος Κώδικα από τα εκάστοτε μετέχοντα σε αυτόν ιδρύματα. Προς τούτο η Ομάδα Έργου του Κώδικα υποχρεούται να καταρτίσει διαδικασίες αφενός σχετικών ελέγχων, κυρίως αναφορικά με την ύπαρξη πολιτικών και διαδικασιών προστασιών των προσωπικών δεδομένων των πελατών των πιστωτικών και χρηματοδοτικών ιδρυμάτων και των συναλλασσόμενων με αυτά, και αφετέρου διαδικασίες για την ανταπόκριση στην άσκηση των δικαιωμάτων των υποκειμένων και υποδοχή, διερεύνηση και αντιμετώπιση τυχόν σχετικών καταγγελιών.

Άρθρο 36

36.1 Η Ομάδα Έργου του Κώδικα συγκροτείται σε σώμα με την εκλογή του Προέδρου της και δύο (2) Αντιπροέδρων. Πρόεδρος εκλέγεται ένας από τους Υπευθύνους Προστασίας Προσωπικών Δεδομένων των συστημικών Τραπεζών, για θητεία τριών (3) ετών.

36.2 Ο Πρόεδρος, και σε περίπτωση κωλύματος αυτού ο πρώτος ή ο δεύτερος Αντιπρόεδρος, συγκαλεί την Ομάδα Έργου του Κώδικα σε συνεδριάσεις και συντονίζει τις συζητήσεις και το έργο αυτής.

36.3 Η Ομάδα Έργου του Κώδικα συνεδριάζει τακτικά τουλάχιστον ανά δίμηνο και έκτακτα όποτε παρίσταται ανάγκη.

36.4 Η Ομάδα Έργου του Κώδικα βρίσκεται σε απαρτία εάν παρίστανται σε αυτή τουλάχιστον τα 2/3 του συνόλου των μελών της, στα οποία περιλαμβάνονται οι Υπεύθυνοι Προσωπικών Δεδομένων των συστημικών τραπεζών και λαμβάνει αποφάσεις με τις ψήφους των 2/3 των παρισταμένων μελών.

Κάθε μέλος της Ομάδας Έργου του Κώδικα έχει μία ψήφο.

36.5 Όταν στην Ομάδα Έργου του Κώδικα συζητείται θέμα που αφορά στην εφαρμογή του Κανονισμού ή/και του Κώδικα σε συμμετέχον στον παρόντα ίδρυμα, το μέλος της Ομάδας Έργου του Κώδικα που προέρχεται από αυτό μπορεί να εκθέσει τις απόψεις του στην Ομάδα, δεν μετέχει όμως στην ψηφοφορία και η κατά την προηγούμενη παρ. 36.4 απαρτία και πλειοψηφία υπολογίζονται χωρίς αυτό.

36.6 Η Ομάδα Έργου του Κώδικα μπορεί να διορίσει Εκτελεστική Επιτροπή από τα μέλη της και να καθορίσει τον τρόπο λειτουργίας και τα καθήκοντά της, όπως ιδίως η διερεύνηση καταγγελιών και η υποβολή σχετικών εισηγήσεων στην ολομέλεια.

Άρθρο 37

37.1 Η Ομάδα Έργου του Κώδικα καταρτίζει ετήσιο προϋπολογισμό των δαπανών της, ο οποίος εγκρίνεται από την Εκτελεστική Επιτροπή της Ελληνικής Ένωσης Τραπεζών και ο οποίος καλύπτεται από τα συμμετέχοντα στον Κώδικα πιστωτικά και χρηματοδοτικά ιδρύματα ανάλογα με τον συνολικό αριθμό των κάθε μορφής πελατών τους.

37.2 Η Ελληνική Ένωση Τραπεζών συνδράμει τη λειτουργία της Ομάδας Έργου του Κώδικα από την άποψη των υποδομών, της γραμματειακής υποστήριξης κα της λογιστικής παρακολούθησης.

Ενότητα 2

Διαδικασία επίλυσης διαφορών

Άρθρο 38

38.1 Τα πιστωτικά και χρηματοδοτικά ιδρύματα που εκάστοτε εντάσσονται στον παρόντα Κώδικα διαθέτουν πολιτικές και διαδικασίες για την εφαρμογή του Κανονισμού και του Κώδικα και την εντός των προθεσμιών του Κανονισμού, αντιμετώπισης των αιτημάτων των υποκειμένων των δεδομένων.

38.2 Σε κάθε περίπτωση υποκείμενα των δεδομένων-πελατών των πιστωτικών και χρηματοδοτικών ιδρυμάτων που εκάστοτε μετέχουν στον Κώδικα μπορούν να απευθυνθούν στον Μεσολαβητή Τραπεζικών και Επενδυτικών Υπηρεσιών για τη μεσολάβησή του για την επίλυση διαφοράς, που αφορά στην προστασία των προσωπικών δεδομένων και την ελεύθερη κυκλοφορία αυτών, σύμφωνα με τον Κανονισμό και τον Κώδικα, μετά ως άνω ιδρύματα.

Κεφάλαιο Ζ΄

Διαδικασία ένταξης στον Κώδικα

Άρθρο 39

39.1 Κάθε πιστωτικό ή χρηματοδοτικό ίδρυμα ή υποκατάστημα τέτοιου ιδρύματος του εξωτερικού που λειτουργεί νόμιμα την Ελλάδα μπορεί να υποβάλει αίτηση στην Ομάδα Έργου του Κώδικα για την υπαγωγή του σε αυτόν. Η υποβολή τέτοιας αίτησης συνεπάγεται αυτοδίκαια την ανεπιφύλακτη αποδοχή του παρόντος, όπως αυτός ισχύει κατά την υποβολή της αίτησης, και όλων των αποφάσεων της Ομάδας Έργου του Κώδικα.

39.2 Η Ομάδα Έργου του Κώδικα εγκρίνει την αίτηση εφόσον ελεγχθεί ότι συντρέχουν οι τυπικές προϋποθέσεις του πρώτου εδαφίου της προηγούμενης παρ. 36.1.

39.3 Με την κατά τα παραπάνω έγκριση της αίτησης υπαγωγής, ο Υπεύθυνος Προσωπικών Δεδομένων του αιτούντος ιδρύματος μετέχει στην Ομάδα Έργου του Κώδικα (άρθρα 33 επομ. ανωτέρω), η οποία αναπροσαρμόζει την κάλυψη του προϋπολογισμού αυτής για το υπόλοιπο του έτους στο οποίο αυτός αφορά, κατά τα αναφερόμενα στο άρθρο 37 ανωτέρω.

Κεφάλαιο Η΄

Διαδικασία αναθεώρησης του Κώδικα

Άρθρο 40

40.1 Η Ομάδα Έργου του Κώδικα (άρθρα 33 επομ. του παρόντος) διασφαλίζει τη συνεχή προσαρμογή του Κώδικα προς το νομικό και κανονιστικό πλαίσιο, τις αποφάσεις του Συμβουλίου των άρθρων 64 επομ. του Κανονισμού, της εθνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της νομολογίας των ανωτάτων Δικαστηρίων της χώρας και των Δικαστηρίων της Ευρωπαϊκής Ένωσης.

40.2 Ο παρών τούτος Κώδικας αναθεωρείται τουλάχιστον ανά διετία, με την απαρτία και πλειοψηφία της παρ. 36.4 ανωτέρω.
