ΣΥΣΤΑΣΕΙΣ ΕΠΙΤΡΟΠΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΠΡΟΣ ΟΛΕΣ ΤΙΣ ΑΣΦΑΛΙΣΤΙΚΕΣ ΕΤΑΙΡΕΙΕΣ ΠΟΥ ΠΑΡΕΧΟΥΝ ΥΠΗΡΕΣΙΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΩΝ ΚΛΑΔΟΥ ΖΩΗΣ ΚΑΙ ΚΛΑΔΟΥ ΓΕΝΙΚΗΣ ΦΥΣΕΩΣ

Αναφορικά με το θέμα της συλλογής και γενικά της επεξεργασίας προσωπικών δεδομένων των πελατών/ασφαλιζόμενων των ασφαλιστικών εταιρειών που παρέχουν υπηρεσίες διαχείρισης ασφαλειών κλάδου ζωής και κλάδου γενικής φύσεως, με βάση τις αρμοδιότητες που μου παρέχονται από το άρθρο 23 (γ) του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001 (Νόμος 138 (Ι) / 2001), όπως τροποποιήθηκε (στο εξής «ο Νόμος»), επιθυμώ να επισύρω την προσοχή σας στο νομοθετικό πλαίσιο που αναφέρεται στο Μέρος Α και να απευθύνω τις συστάσεις που αναφέρονται στο Μέρος Β:

ΜΕΡΟΣ Α- ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

1. ΔΙΑΤΑΞΕΙΣ ΤΟΥ ΝΟΜΟΥ

1.1. Σύμφωνα με τις διατάξεις του άρθρου 2 του Νόμου:
«*υπεύθυνος επεξεργασίας*» σημαίνει «οποιοδήποτε πρόσωπο που καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα».

«*προσωπικά δεδομένα*» είναι «κάθε πληροφορία, που αναφέρεται στο υποκείμενο των δεδομένων, δηλαδή στο φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί αμέσως ή εμμέσως.».

Για παράδειγμα προσωπικά δεδομένα είναι: το ονοματεπώνυμο, η ημερομηνία γέννησης, το φύλο, ο αριθμός τηλεφώνου, η ηλεκτρονική διεύθυνση, ο αριθμός δελτίου ταυτότητας, ο αριθμός κοινωνικών ασφαλίσεων, η οικογενειακή και οικονομική κατάσταση κ.λ.π.

Το ίδιο άρθρο ορίζει την έννοια των «*ευαίσθητων δεδομένων*» ως «τα δεδομένα που αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, την υγεία, την ερωτική ζωή και ερωτικό προσανατολισμό, καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες».

Επίσης, στο ίδιο άρθρο ορίζεται ως «*συγκατάθεση*» «κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή και εν πλήρη επίγνωση, και με την οποία το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν».

Σύμφωνα επίσης με το άρθρο 2, ως «*Αρχείο δεδομένων προσωπικού χαρακτήρα*» ή «*αρχείο*» νοείται «το διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία αποτελούν ή δύνανται να αποτελέσουν αντικείμενο επεξεργασίας, και τα οποία είναι προσιτά με βάση συγκεκριμένα κριτήρια».

Το άρθρο 3(1) του Νόμου προβλέπει ότι, οι διατάξεις του Νόμου εφαρμόζονται στην αυτοματοποιημένη εν όλω ή εν μέρει επεξεργασία, καθώς και στη μη αυτοματοποιημένη

επεξεργασία προσωπικών δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.

1.2. Οι διατάξεις του άρθρου 4(1) του Νόμου ορίζουν ρητά ότι, ο υπεύθυνος επεξεργασίας, στην προκειμένη περίπτωση, οι ασφαλιστικές εταιρείες, διασφαλίζουν ότι τα προσωπικά δεδομένα:

(α) υφίστανται θεμιτή και νόμιμη επεξεργασία,

(β) συλλέγονται για προσδιορισμένους, σαφείς και νόμιμους σκοπούς και δεν υφίστανται μεταγενέστερη επεξεργασία ασυμβίβαστη με τους σκοπούς αυτούς (αρχή του σκοπού),

(γ) είναι συναφή, πρόσφορα και όχι περισσότερα από ότι κάθε φορά απαιτείται ενόψει των σκοπών της επεξεργασίας (αρχή της αναλογικότητας),

(δ) είναι ακριβή και, εφόσον χρειάζεται, υποβάλλονται σε ενημέρωση,

(ε) διατηρούνται μόνο για όσο χρονικό διάστημα είναι απαραίτητο για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους.

Συνεπώς, κάθε επεξεργασία προσωπικών δεδομένων που γίνεται πέραν του επιδιωκόμενου σκοπού ή η οποία δεν είναι πρόσφορη και αναγκαία για την επίτευξή του, δεν είναι νόμιμη.

1.3. Η συλλογή και κάθε περαιτέρω επεξεργασία απλών και ευαίσθητων προσωπικών δεδομένων που αφορούν στους πελάτες/ασφαλιζόμενους επιτρέπεται, καταρχήν, εφόσον ο υπεύθυνος επεξεργασίας έχει εκ των προτέρων εξασφαλίσει τη συγκατάθεσή τους. Κατ' εξαίρεση, η συλλογή και κάθε περαιτέρω επεξεργασία τόσο των απλών όσο και των ευαίσθητων προσωπικών δεδομένων επιτρέπεται και χωρίς συγκατάθεση εφόσον συντρέχουν οι όροι που περιοριστικώς αναφέρονται στο Νόμο.

Συγκεκριμένα, για τα απλά δεδομένα, επιτρέπεται υπό τις προϋποθέσεις του άρθρου 5 (2) του Νόμου και για τα ευαίσθητα δεδομένα υπό τις προϋποθέσεις του άρθρου 6 (2) του Νόμου, δεδομένου ότι τηρούνται οι γενικές αρχές επεξεργασίας, όπως ορίζονται στο άρθρο 4(1) του Νόμου.

<u>Παραδείγματα τα οποία αφορούν στην πρώτη περίπτωση του άρθρου 5 (2) του Νόμου:</u>
Οι ασφαλιστικές εταιρείες μπορούν να συλλέγουν και γενικά να επεξεργάζονται απλά προσωπικά δεδομένα των πελατών τους, όταν για παράδειγμα:

«Η επεξεργασία είναι απαραίτητη για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από νόμο ή Κανονισμούς που εκδίδονται δυνάμει νόμου ή Κανονισμούς της Ευρωπαϊκής Ένωσης»,
ή

«η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης στην οποία συμβαλλόμενο μέρος είναι το υποκείμενο των δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου των δεδομένων, πριν από τη σύναψη σύμβασης»,

ή

«η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων».

Παραδείγματα τα οποία αφορούν στη δεύτερη περίπτωση του άρθρου 6 (2) του Νόμου, το οποίο ισχύει κατ' αναλογία και στην επεξεργασία μη ευαίσθητων προσωπικών δεδομένων:
Οι ασφαλιστικές εταιρείες μπορούν να συλλέγουν και γενικά να επεξεργάζονται ευαίσθητα προσωπικά δεδομένα των πελατών τους, όταν για παράδειγμα:

«Το υποκείμενο των δεδομένων έδωσε τη ρητή συγκατάθεσή του, εκτός αν η συγκατάθεση έχει αποσπασθεί παράνομα ή αντίκειται στα χρηστά ήθη ή ειδικός νόμος ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση»

ή

«η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου προσώπου, αν το υποκείμενο των δεδομένων τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του»

ή

«η επεξεργασία αφορά θέματα ιατρικών δεδομένων και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας».

ή

«η επεξεργασία πραγματοποιείται αποκλειστικά για στατιστικούς, ερευνητικούς, επιστημονικούς και ιστορικούς σκοπούς εφόσον, σύμφωνα με απόφαση του Επιτρόπου, κρίνεται ότι συντρέχουν σοβαροί λόγοι δημοσίου συμφέροντος, υπό τον όρο ότι λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των υποκειμένων των δεδομένων».

1.4. Το άρθρο 10 του Νόμου, που αφορά στο απόρρητο και στην ασφάλεια της επεξεργασίας, έχει ως εξής:

«(1) Η επεξεργασία δεδομένων είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνο κατ' εντολή του.
(2) Για τη διεξαγωγή της επεξεργασίας, ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.
(3) Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.

Ο Επίτροπος παρέχει εκάστοτε οδηγίες για το βαθμό ασφάλειας των δεδομένων, καθώς και για τα μέτρα προστασίας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία δεδομένων, ενόψει και των τεχνολογικών εξελίξεων.
(4) Αν η επεξεργασία διεξάγεται από εκτελούντα την επεξεργασία, η σχετική ανάθεση γίνεται υποχρεωτικά με γραπτή σύμβαση. Η ανάθεση προβλέπει υποχρεωτικά ότι ο εκτελών την επεξεργασία τη διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν.».

2. Ο ΠΕΡΙ ΤΗΣ ΠΑΡΕΜΠΟΔΙΣΗΣ ΚΑΙ ΚΑΤΑΠΟΛΕΜΗΣΗΣ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΝΟΜΟΣ ΤΟΥ 2007 (188(Ι)/2007)

Παραθέτω αυτούσιες τις ακόλουθες διατάξεις του Νόμου 188(Ι)/2007:

Άρθρο 2
«άλλες δραστηριότητες» περιλαμβάνουν τα ακόλουθα:
(α) Άσκηση επαγγελματικών δραστηριοτήτων ελεγκτών, εξωτερικών λογιστών και φορολογικών συμβούλων, περιλαμβανομένων συναλλαγών για λογαριασμό των πελατών τους στο πλαίσιο χρηματοοικονομικών δραστηριοτήτων.
(β) άσκηση επαγγελματικών δραστηριοτήτων εκ μέρους ανεξάρτητων επαγγελματιών νομικών, με εξαίρεση τις προνομιούχες πληροφορίες, όταν συμμετέχουν είτε-
(i) Βοηθώντας στο σχεδιασμό ή στην υλοποίηση συναλλαγών για τους πελάτες τους σχετικά με-
(αα) την αγορά και πώληση ακινήτων ή επιχειρήσεων,
(ββ) τη διαχείριση χρημάτων, τίτλων ή άλλων περιουσιακών στοιχείων των πελατών τους,
(γγ) το άνοιγμα ή τη διαχείριση τραπεζικών λογαριασμών, λογαριασμών ταμιευτηρίου ή λογαριασμών τίτλων,
(δδ) την οργάνωση των εισφορών των αναγκαίων για τη δημιουργία, λειτουργία, ή διοίκηση εταιρειών,
(εε) τη σύσταση, λειτουργία ή διοίκηση καταπιστευματικών εταιρειών, επιχειρήσεων ή ανάλογων μονάδων,
(ii) ενεργώντας εξ ονόματος και για λογαριασμό των πελατών τους στο πλαίσιο χρηματοοικονομικών συναλλαγών ή συναλλαγών επί ακινήτων.
(γ) κτηματικές συναλλαγές εκ μέρους κτηματομεσιτών, δυνάμει του περί Κτηματομεσιτών Νόμου, ως εκάστοτε ισχύει.
(δ) εμπόριο προϊόντων ή αγαθών, όπως πολύτιμων λίθων και μετάλλων, εφόσον η πληρωμή γίνεται σε μετρητά για ποσό ίσο ή μεγαλύτερο των 15.000 ευρώ ανεξάρτητα του αν η συναλλαγή διενεργείται με μια μόνο πράξη ή με περισσότερες, μεταξύ των οποίων φαίνεται να υπάρχει κάποια σχέση.
(ε) τις ακόλουθες υπηρεσίες εμπιστευμάτων και εταιρικών υπηρεσιών προς τρίτα μέρη:
(i) Σύσταση εταιρειών ή άλλων νομικών προσώπων·
(ii) άσκηση καθηκόντων διευθυντή ή γραμματέα εταιρείας, εταίρου συνεταιρισμού ή κατόχου ανάλογης θέσης σε σχέση με άλλα νομικά πρόσωπα ή νομικούς μηχανισμούς ώστε άλλο πρόσωπο να ασκήσει ανάλογα καθήκοντα·
(iii) παροχή εγγεγραμμένου γραφείου, επιχειρηματικής διεύθυνσης, ταχυδρομικής ή διοικητικής διεύθυνσης και οποιεσδήποτε άλλες σχετικές υπηρεσίες για εταιρεία, προσωπική εταιρεία ή κάθε άλλο νομικό πρόσωπο ή νομικό μηχανισμό·
(iv) άσκηση καθηκόντων εμπιστευματοδόχου σε ρητά εμπιστεύματα ή ανάλογο νομικό μηχανισμό ώστε άλλο πρόσωπο να ασκήσει ανάλογα καθήκοντα· και

(v) άσκηση καθηκόντων πληρεξούσιου μετόχου εξ ονόματος άλλου προσώπου, ή νομικού μηχανισμού ώστε άλλο πρόσωπο να ασκήσει ανάλογα καθήκοντα·
(στ) οποιαδήποτε από τις υπηρεσίες ή τις δραστηριότητες που καθορίζονται στο άρθρο 4 του περί της Ρύθμισης των Επιχειρήσεων Παροχής Διοικητικών Υπηρεσιών και Συναφών Θεμάτων Νόμου, όπως αυτός εκάστοτε τροποποιείται ή αντικαθίσταται·

«**Χρηματοοικονομικές δραστηριότητες»** περιλαμβάνουν τα ακόλουθα:
(α) Αποδοχή καταθέσεων από το κοινό·
(β) δανεισμός χρημάτων στο κοινό·
(γ) χρηματοδοτική μίσθωση, περιλαμβανομένης και χρηματοδότησης με ενοικιαγορά·
(δ) υπηρεσίες διακίνησης χρημάτων·
(ε) έκδοση και διαχείριση μέσων πληρωμής, όπως πιστωτικές κάρτες, ταξιδιωτικές επιταγές, επιταγές τραπεζίτη και ηλεκτρονικού χρήματος·
(στ) έκδοση εγγυήσεων και ανάληψη υποχρεώσεων·
(ζ) διεξαγωγή συναλλαγών για ίδιο λογαριασμό ή για λογαριασμό άλλου προσώπου που έχουν σχέση με-
(i) Αξίες ή τίτλους της χρηματαγοράς περιλαμβανομένων επιταγών, συναλλαγματικών, γραμματίων και ομόλογα καταθέσεων.
(ii) ξένο συνάλλαγμα·
(iii) προθεσμιακούς χρηματοδοτικούς τίτλους ή τίτλους με δικαίωμα επιλογής (options)·
(iv) τίτλους που αφορούν συνάλλαγμα και επιτόκια·
(v) αξιόγραφα·
(η) συμμετοχή σε εκδόσεις αξιογράφων και παροχή συναφών υπηρεσιών·
(θ) παροχή συμβουλών σε επιχειρήσεις σχετικά με τη διάρθρωση του κεφαλαίου, τη βιομηχανική στρατηγική και συναφή θέματα και παροχή συμβουλών καθώς και υπηρεσιών στον τομέα της συγχώνευσης και της αγοράς επιχειρήσεων·
(ι) διαμεσολάβηση στη χρηματαγορά·
(ια) επενδυτικές υπηρεσίες, περιλαμβανομένων της εμπορίας και διευθέτησης εμπορίας επενδύσεων, της διαχείρισης επενδύσεων, των συμβουλών για επενδύσεις και της ίδρυσης και λειτουργίας σχεδίων συλλογικών επενδύσεων**. Για τους σκοπούς** του **εδαφίου αυτού, ο όρος "επένδυση" περιλαμβάνει ασφάλειες ζωής επί μακροπρόθεσμης βάσης συνδεδεμένες ή μη με επενδυτικά σχέδια·**
(ιβ) υπηρεσίες ασφαλούς φύλαξης·
(ιγ) φύλαξη και διαχείριση αξιογράφων·
(ιδ) οποιαδήποτε από τις υπηρεσίες και δραστηριότητες-
(i) που καθορίζονται στο Μέρος Ι και ΙΙ του Τρίτου Παραρτήματος του περί των Επενδυτικών Υπηρεσιών και Δραστηριοτήτων και Ρυθμιζόμενων Αγορών Νόμου, ως εκάστοτε ισχύει και που παρέχονται σε σχέση με τα χρηματοοικονομικά μέσα, τα οποία απαριθμούνται στο Μέρος ΙΙΙ του ιδίου Παραρτήματος·
(ii) που καθορίζονται στο άρθρο 109 του περί των Ανοικτού Τύπου Οργανισμών Συλλογικών Επενδύσεων Νόμου, όπως αυτός εκάστοτε τροποποιείται ή αντικαθίσταται·
(iii) που καθορίζονται στα εδάφια (5) και (6) του άρθρου 6 του περί των Διαχειριστών Οργανισμών Εναλλακτικών Επενδύσεων Νόμου, όπως αυτός εκάστοτε τροποποιείται ή αντικαθίσταται·
(ιε) ασφαλιστικές εργασίες κλάδου ζωής και εργασίες διαμεσολάβησης για σύναψη ασφαλειών ζωής·
(ιστ) χωρίς επηρεασμό της γενικότητας των παραγράφων (δ) και (ε), οποιαδήποτε από τις υπηρεσίες που καθορίζονται στο Παράρτημα του περί Υπηρεσιών Πληρωμών Νόμου, ως εκάστοτε ισχύει·

Άρθρο 68

(1) Πρόσωπα που διεξάγουν χρηματοοικονομικές ή άλλες δραστηριότητες οφείλουν να τηρούν αρχεία και να φυλάσσουν για περίοδο τουλάχιστον πέντε ετών τα ακόλουθα έγγραφα:

(α) Αντίγραφα των αποδεικτικών στοιχείων της ταυτότητας του πελάτη·

(β) τα σχετικά αποδεικτικά στοιχεία και τις λεπτομέρειες όλων των επιχειρηματικών σχέσεων και συναλλαγών, συμπεριλαμβανομένων εγγράφων για την καταχώρηση των συναλλαγών στα λογιστικά βιβλία· και

(γ) τα σχετικά έγγραφα της αλληλογραφίας με τους πελάτες και άλλα πρόσωπα με τους οποίους διατηρείται επιχειρηματική σχέση.

(2) Η περίοδος των πέντε ετών υπολογίζεται μετά την εκτέλεση των συναλλαγών ή την περάτωση της επιχειρηματικής σχέσης.

(3) Τα πρόσωπα που διεξάγουν χρηματοοικονομικές ή άλλες δραστηριότητες οφείλουν να διασφαλίζουν ότι όλα τα έγγραφα που αναφέρονται στο εδάφιο (1) τίθενται έγκαιρα και χωρίς καθυστέρηση στη διάθεση της Μονάδας και των αρμοδίων Εποπτικών Αρχών για σκοπούς εκτέλεσης των καθηκόντων που τους αναθέτει ο παρών Νόμος.

3. Κανονισμός (ΕΕ) 679/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

Παρατίθεται αυτούσια το άρθρο 20 του Κανονισμού, ο οποίος τέθηκε σε ισχύ από τις 24 Μαΐου 2016, ενώ θα αρχίσει να εφαρμόζεται μετά από δύο χρόνια.

«Δικαίωμα στη φορητότητα των δεδομένων

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, όταν:

α) η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) ή σε σύμβαση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) και

β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

2. Κατά την άσκηση του δικαιώματος στη φορητότητα των δεδομένων σύμφωνα με την παράγραφο 1, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητά την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό.

3. Το δικαίωμα που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου ασκείται με την επιφύλαξη του άρθρου 17. Το εν λόγω δικαίωμα δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

4. Το δικαίωμα που αναφέρεται στην παράγραφο 1 δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.».

Με βάση τα πιο πάνω:
Σε περίπτωση που τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με ηλεκτρονικά μέσα και με δομημένο και συνήθως χρησιμοποιούμενο μορφότυπο, το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δικαιούται να εξασφαλίσει από τον υπεύθυνο επεξεργασίας αντίγραφο των δεδομένων που υποβάλλονται σε επεξεργασία, σε ηλεκτρονικό και δομημένο μορφότυπο συνήθους χρήσης ο οποίος επιτρέπει την περαιτέρω χρήση από το πρόσωπο στο οποίο αναφέρονται τα δεδομένα.

Εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει παράσχει τα δεδομένα προσωπικού χαρακτήρα και η επεξεργασία βασίζεται σε συγκατάθεση ή είναι αναγκαία για την εκτέλεση σύμβασης, το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δικαιούται να μεταφέρει τα εν λόγω δεδομένα και κάθε άλλη πληροφορία που διατηρείται σε αυτοματοποιημένο αρχείο σε άλλο αυτοματοποιημένο αρχείο, σε ηλεκτρονικό μορφότυπο συνήθους χρήσης, χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας από τον οποίο αποσύρονται τα δεδομένα προσωπικού χαρακτήρα.

ΜΕΡΟΣ Β - ΣΥΣΤΑΣΕΙΣ

Α. Οι ασφαλιστικές εταιρείες οφείλουν όπως υποβάλουν στο Γραφείο μου ξεχωριστό έντυπο Γνωστοποίησης για κάθε αρχείο που τηρούν και περιλαμβάνει προσωπικά δεδομένα, δεδομένου ότι το κάθε αρχείο εξυπηρετεί διαφορετικό σκοπό.

Για παράδειγμα, εάν τηρούν μόνο ένα αρχείο, το αρχείο διαχείρισης ασφαλειών και το εν λόγω αρχείο χρησιμοποιείται και για άλλους σκοπούς (για προώθηση προϊόντων και υπηρεσιών, για στατιστική ανάλυση/έρευνα αγοράς κ.λ.π.), τότε δεν χρειάζεται να υποβάλουν ξεχωριστή Γνωστοποίηση για το αρχείο που τηρούν για σκοπούς άλλους από τη διαχείριση ασφαλειών. Σε αντίθετη περίπτωση, θα πρέπει να υποβληθεί νέα, ξεχωριστή Γνωστοποίηση.

Β. Οι ασφαλιστικές εταιρείες θα πρέπει να λαμβάνουν χωριστή συγκατάθεση από τους πελάτες/ασφαλιζόμενους όταν η επεξεργασία των προσωπικών τους δεδομένων έχει πολλαπλούς σκοπούς.

Η συγκατάθεση που θα λαμβάνεται πρέπει να είναι ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας τους υπέρ της επεξεργασίας των δεδομένων που τους αφορούν. Συνεπώς:
(i) οι πελάτες/ασφαλιζόμενοι πρέπει να έχουν το δικαίωμα ελεύθερης επιλογής κατά πόσο ενδιαφέρονται για τις συγκεκριμένες υπηρεσίες που προσφέρονται από την ασφαλιστική εταιρεία στην οποία είναι πελάτες.

(ii) οι πελάτες/ασφαλιζόμενοι πρέπει να έχουν τη δυνατότητα να την αποσύρουν ανά πάσα στιγμή χωρίς αυτή τους η ενέργεια να έχει οποιεσδήποτε δυσμενείς επιπτώσεις, όπως για παράδειγμα οποιοδήποτε οικονομικό κόστος.

Να σημειωθεί επίσης ότι, ακόμα και στην περίπτωση που έχει ληφθεί η συγκατάθεση των πελατών/ασφαλιζόμενων, αν η συλλογή και η επεξεργασία των προσωπικών τους

δεδομένων προσκρούει σε μία από τις βασικές αρχές επεξεργασίας προσωπικών δεδομένων του άρθρου 4 του Νόμου τότε η τυχόν ληφθείσα συγκατάθεση δεν αίρει την παρανομία αυτή και, ως εκ τούτου, η επεξεργασία προσωπικών δεδομένων δεν είναι νόμιμη.

Από τα ανωτέρω, εξυπακούεται ότι, τυχόν «συγκατάθεση» των πελατών/ασφαλιζόμενων στο ασφαλιστήριο συμβόλαιο υπό τη μορφή προσχώρησης στους γενικούς του όρους, δεν αποτελεί «ελεύθερη, ρητή και ειδική δήλωση βουλήσεως».

Γ. Σύμφωνα με την αρχή της αναλογικότητας, οι ασφαλιστικές εταιρείες:
1. Κατά το στάδιο εξέτασης της αίτησης για ασφάλιση, θα πρέπει να συλλέγουν προσωπικά δεδομένα από τους ίδιους τους πελάτες/προτιθέμενους πελάτες τους. Μόνο σε εξαιρετικές περιπτώσεις και μετά από συγκατάθεση τους, επιτρέπεται να λαμβάνουν πληροφορίες από τρίτους (ιατρούς, άλλη ασφαλιστική εταιρεία κ.λ.π.). Η εν λόγω συγκατάθεση θα πρέπει να λαμβάνεται κατά περίπτωση, όπου κρίνεται απολύτως αναγκαίο. Όπως αναφέρεται στη Σύσταση Β πιο πάνω, τυχόν «συγκατάθεση» τους στο ασφαλιστήριο συμβόλαιο υπό τη μορφή προσχώρησης στους γενικούς του όρους, δεν αποτελεί «ελεύθερη, ρητή και ειδική δήλωση βουλήσεως».

2. Οφείλουν να συλλέγουν και γενικά να επεξεργάζονται μόνο όσα δεδομένα είναι απολύτως απαραίτητα για την πραγματοποίηση του σκοπού της επεξεργασίας, δηλαδή τη διαχείριση ασφαλειών και συγκεκριμένα την εξέταση της αίτησης για ασφάλιση και/ή την εξέταση/αξιολόγηση απαίτησης για καταβολή αποζημίωσης.

Δ. Βάσει του άρθρου 10 του Νόμου που αφορά στο απόρρητο και στην ασφάλεια της επεξεργασίας, οι ασφαλιστικές εταιρείες έχουν υποχρέωση όπως:

1. Συνάπτουν γραπτή σύμβαση με όλους όσοι εκτελούν εργασίες για λογαριασμό τους, όπως για παράδειγμα με τους ασφαλιστικούς σύμβουλους. Η σύμβαση θα πρέπει να αναφέρει ρητά τις διατάξεις του άρθρου 10 του Νόμου και ότι τα προσωπικά δεδομένα δεν θα χρησιμοποιούνται για άλλους σκοπούς.

2.Λαμβάνουν τα απαραίτητα μέτρα ώστε:
(i) να υπάρχουν διαφορετικά επίπεδα πρόσβασης στα προσωπικά δεδομένα των πελατών/ασφαλιζόμενων για τη διασφάλιση της ασφάλειας των δεδομένων,
(ii) η πρόσβαση να είναι ελεγχόμενη, δηλαδή η πρόσβαση να επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα με τη χρήση κωδικών πρόσβασης,
(iii) η πρόσβαση να καταγράφεται ούτως ώστε να είναι δυνατός ο μεταγενέστερος έλεγχος της πρόσβασης,
(iv) οι ενέργειες των χρηστών στα αυτοματοποιημένα συστήματα να ανιχνεύονται ανά πάσα στιγμή,
(v) οι κωδικοί πρόσβασης να διαθέτουν ικανοποιητικό βαθμό ασφάλειας ώστε να μην είναι εύκολη η αναπαραγωγή τους από μη εξουσιοδοτημένα πρόσωπα και
(vi) να μην είναι δυνατή η αλλοίωση των δεδομένων από μη εξουσιοδοτημένα πρόσωπα.

3. Οι ασφαλιστικές εταιρείες έχουν υποχρέωση όπως διασφαλίζουν ότι, το προσωπικό τους καθώς και οι εκτελούντες την επεξεργασία δεσμεύονται από ρήτρες εμπιστευτικότητας. Για το σκοπό αυτό, θα πρέπει να καταρτίσουν ειδικό Κώδικα Δεοντολογίας του προσωπικού και των εκτελούντων την επεξεργασία.

Ε. Έχοντας υπόψη τις διατάξεις των άρθρων 2 και 68(1)(α) του περί της Παρεμπόδισης και Καταπολέμησης της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες Νόμου του 2007 (188(Ι)/2007), μόνο οι ασφαλιστικές εταιρείες που παρέχουν ασφαλιστικές εργασίες κλάδου ζωής και εργασίες διαμεσολάβησης για σύναψη ασφαλειών ζωής, δικαιούνται να λαμβάνουν αντίγραφο του Δελτίου Πολιτικής Ταυτότητας των πελατών/ασφαλιζόμενων τους. Από την άλλη, οι ασφαλιστικές εταιρείες που παρέχουν ασφαλιστικές εργασίες κλάδου γενικής φύσεως, μπορούν να ζητούν από τους προτιθέμενους πελάτες τους να επιδεικνύουν το Δελτίο Πολιτικής Ταυτότητας τους με σκοπό την επαλήθευση/επιβεβαίωση της ορθότητας των στοιχείων που δηλώθηκαν από αυτούς στην Αίτηση για Ασφάλιση.

ΣΤ. Οι ασφαλιστικές εταιρείες πρέπει να σέβονται το δικαίωμα στη φορητότητα των δεδομένων που μπορούν οι πελάτες/ασφαλιζόμενοι να ασκήσουν στα προσωπικά δεδομένα που τους αφορούν και διατηρούνται σε αρχείο αυτοματοποιημένης μορφής.

Ζ. Οι ασφαλιστικές εταιρείες πρέπει να σέβονται το δικαίωμα πρόσβασης που μπορούν οι πελάτες/ασφαλιζόμενοι να ασκήσουν στα προσωπικά δεδομένα που τους αφορούν και διατηρούνται σε αρχείο αυτοματοποιημένης, μερικώς αυτοματοποιημένης ή μη αυτοματοποιημένης μορφής.

Ειρήνη Λοϊζίδου Νικολαΐδου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα

5 Οκτωβρίου 2016