ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

Αρ. Φακ.: 11.17.001.008.001
Τηλ: 22 818456
Φαξ: 22 304565

17 Ιουνίου 2020

ΣΤΑΛΗΚΕ (2)
Ημερ. 17/6/20
Υπ. ....

ΜΕ ΤΟ ΧΕΡΙ

Γενικό Διευθυντή
Τράπεζας Κύπρου Δημόσιας Εταιρείας Λτδ
(Υπόψιν
Περιφερειακής Διευθύντριας Λευκωσιας)

Χρυσαφίνης & Πολυβίου Δ.Ε.Π.Ε.
(Υπόψιν κ
Τ.Θ. 21238
1504 ΛΕΥΚΩΣΙΑ

ΑΠΟΦΑΣΗ

Άσκηση δικαιώματος πρόσβασης από τον κ.

Αναφέρομαι στην καταγγελία που υποβλήθηκε στο Γραφείο μου αναφορικά με το πιο πάνω θέμα και σε συνέχεια της μεταξύ μας αλληλογραφίας που λήγει με την επιστολή του Εξωτερικού Νομικού Συμβόλου της Τράπεζας Κύπρου Δημόσιας Εταιρείας Λτδ, Χρυσαφίνης & Πολυβίου Δ.Ε.Π.Ε., με ημερομηνία 05.06.2020 και σας πληροφορώ τα ακόλουθα:

Γεγονότα

1.1. Στις 21.01.2020, δέχτηκα παράπονο από τον κ. εναντίον της Τράπεζας Κύπρου Δημόσιας Εταιρείας Λτδ (στο εξής «η Τράπεζα») και της ασφαλιστικής εταιρείας Eurolife Ltd, ο οποίος, όπως αναφέρει, ζήτησε όπως έχει αντίγραφο του ασφαλιστικού συμβολαίου του με αριθμό Μ-056482.

Συγκεκριμένα, ο παραπονούμενος προσκόμισε αντίγραφο της αλληλογραφίας που είχε με τον κ. Περιφερειακό Διευθυντή Λευκωσίας Τράπεζας Κύπρου, ο οποίος, με επιστολή του με ημερομηνία 23.09.2019, τον ενημέρωνε ότι:

«....επειδή ο λογαριασμός σας έχει μεταφερθεί πριν από αρκετά χρόνια από την Λεμεσό, το πρωτότυπο συμβόλαιο της Οριοασφάλισης που αναφέρεστε, φαίνεται να έχει αρχειοθετηθεί σε χώρο που ο εντοπισμός του καθυστερεί και είναι αντικειμενικά δύσκολος και χρονοβόρος, γι' αυτό η Τράπεζα είναι πρόθυμη να ακυρώσει την οριοασφάλιση αυτή με την ενυπόγραφη αίτηση σας.».

1.2. Με βάση το καθήκον εξέτασης καταγγελιών που παρέχει στον Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα το άρθρο 57(1)(στ) του Κανονισμού (ΕΕ) 2016/679 (στο εξής «ο Κανονισμός») και το άρθρο 24(β) του Νόμου που προνοεί για την Προστασία των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και για την Ελεύθερη Κυκλοφορία των Δεδομένων Αυτών (Νόμος 125(Ι)/2018), με την ταυτάριθμη επιστολή του Γραφείου μου, ημερομηνίας 03.02.2020, στάλθηκε επιστολή στον Υπεύθυνο Προστασίας Δεδομένων της Τράπεζας και στον Υπεύθυνο Προστασίας Δεδομένων της Eurolife Ltd, με την οποία ενημερώθηκαν για το πιο πάνω παράπονο.

Στην ίδια επιστολή, ζήτησα τις θέσεις/απόψεις τους σχετικά με τους εν λόγω ισχυρισμούς και επιπρόσθετα να με πληροφορήσουν:

(α) Τους χώρους φύλαξης/αποθήκευσης παλαιών/ληχθέντων/ακυρωθέντων συμβολαίων και

(β) τα τεχνικά και οργανωτικά μέτρα φύλαξης και προστασίας τους.

1.3. Με επιστολή του Γραφείου μου με ημερομηνία 03.02.2020, ενημέρωσα τον παραπονούμενο ότι, κάλεσα τους Καθ'ων την καταγγελία να μου αναφέρουν τις θέσεις/απόψεις τους, το αργότερο μέχρι τις 23 Φεβρουαρίου 2020 και ότι θα ενημερωθεί γραπτώς για την απάντηση τους.

1.4. Στις 20.02.2020, η εταιρεία Eurolife Ltd απέστειλε επιστολή στο Γραφείο μου, στην οποία ανέφερε τα εξής:

- Η Τράπεζα είναι ο ιδιοκτήτης της ομαδικής σύμβασης οριοασφάλισης και έχει το δικαίωμα διαχείρισης της. Έχει την ευθύνη της ένταξης και αφαίρεσης μελών στην σύμβαση Οριοασφάλισης όπως και της υπογραφής, παράδοσης και φύλαξης των πρωτότυπων και αντιγράφων των συμβολαίων των μελών της οριοασφάλισης.

- Η ασφαλιστική εταιρεία Eurolife Ltd, έχει την υποχρέωση της πληρωμής του ωφελήματος που θα προκύψει με βάση τους όρους της σύμβασης.

- Όσον αφορά στο αίτημα του κ. , κανένα έντυπο δεν βρίσκεται στην φύλαξη της ασφαλιστικής εταιρείας Eurolife Ltd.

1.5. Με απαντητική της επιστολή ημερομηνίας 20.02.2020, η Δρ. Περιφερειακή Διευθύντρια Λευκωσίας της Τράπεζας, με πληροφόρησε ότι:

- Εφόσον καταρτισθεί συμβόλαιο οριοασφάλισης με πελάτη και εκχωρηθεί προς όφελος της Τράπεζας, αυτό φυλάγεται σε αρχειοθετημένο κουτί φύλαξης στο αρμόδιο υποκατάστημα της Τράπεζας.

- Όταν η Τράπεζα θα προβεί σε κλείσιμο κάποιου υποκαταστήματος ή ο αποθηκευτικός χώρος που διαθέτει το υποκατάστημα εξαντληθεί, τότε το αρχειοθετημένο κουτί φύλαξης καταλήγει στο κεντρικό αρχείο φύλαξης (θεματοφυλάκιο) της Τράπεζας, το οποίο κατέχει πιστοποίηση ISO και τηρεί όλα τα δέοντα μέτρα φύλαξης και ασφάλειας ως προς την προστασία των εγγράφων που καταλήγουν σε αυτό.

- Παρά τη σχετική έρευνα δεν κατέστη δυνατός ο εντοπισμός του συμβολαίου του πελάτη στο σχετικό αρχειοθετημένο κουτί φύλαξης.

- Η Τράπεζα έχει επιθεωρήσει και το φυσικό φάκελο του πελάτη όπου υπάρχουν όλες οι πρωτότυπες συμφωνίες/συμβόλαια και επικοινωνία με τον πελάτη συμπεριλαμβανομένου και έγγραφα ταυτοποίησής του όπου και πάλι δεν κατέστη δυνατό να εντοπιστεί το συγκεκριμένο συμβόλαιο.

1.6. Με βάση τα ανωτέρω και τα ενώπιον μου δεδομένα καθώς και τα στοιχεία και αποδείξεις της έρευνας, προκύπτει ότι, η Καθ'ης την καταγγελία εταιρεία Eurolife Ltd, ως ξεχωριστό νομικό πρόσωπο και συνεπώς ως ξεχωριστός υπεύθυνος επεξεργασίας δεν έχει προβεί σε παράνομη επεξεργασία προσωπικών δεδομένων και ως εκ τούτου δεν υπάρχει υπόθεση εναντίον της αλλά μόνο εναντίον της Καθ'ης την καταγγελία, Τράπεζας.

1.7. Στη συνέχεια, με επιστολή μου ημερομηνίας 11.05.2020, η Καθ'ης την καταγγελία πληροφορήθηκε ότι, εκ πρώτης όψεως διαπίστωσα παράβαση της υποχρέωσης της εκ των άρθρων 5(1)(στ), 5(2), 15, 32 και 33 του Κανονισμού, καθώς και του άρθρου 33(1)(γ) του Νόμου 125(I)/2018 και της ζητήθηκε να μου υποβάλει τις θέσεις/απόψεις της για τα πιο πάνω και τους λόγους για τους οποίους πιστεύει ότι δεν πρέπει να της επιβληθεί οποιαδήποτε διοικητική κύρωση, εντός προθεσμίας 4 εβδομάδων από την πιο πάνω ημερομηνία. Επιπρόσθετα, με την ίδια επιστολή, της ζητήθηκε να με πληροφορήσει τον κύκλο εργασιών της.

1.8. Στις 05.06.2020, οι Εξωτερικοί Νομικοί Σύμβουλοι της Τράπεζας, Γ
(Χρυσαφίνης & Πολυβίου Δ.Ε.Π.Ε.), ενεργώντας για λογαριασμό του πελατη τους, (Τράπεζα), μου απέστειλε επιστολή και μου ανέφερε, μεταξύ άλλων, ότι:

(α) Η οριοασφάλιση του πελάτη έχει συναφθεί στις 24 Ιανουαρίου 2000 για το ποσό των £20,000 (είκοσι χιλιάδων Λιρών Κύπρου) προς εξασφάλιση τρεχούμενου λογαριασμού στο όνομα της εταιρείας Λτδ.

(β) Σύμφωνα με την τότε διαδικασία αρχειοθέτησης της Τράπεζας *(επισυνάφθηκε μέρος της Πολιτικής/εσωτερικής διαδικασίας)*, το πρωτότυπο το κρατούσε ο πελάτης, ένα αντίγραφο έπρεπε να αρχειοθετηθεί στο φάκελο του πελάτη και ένα αντίγραφο αρχειοθετείτο σε ξεχωριστό φάκελο (box life). Εκ παραδρομής, φαίνεται να μην αρχειοθετήθηκε αντίγραφο στο φάκελο του πελάτη το 2000, με αποτέλεσμα ο φάκελος του, ο οποίος βρίσκεται στην κατοχή της Τράπεζας, να μην περιέχει το συγκεκριμένο αντίγραφο.

(γ) Αρχικά, ο λογαριασμός του πελάτη ήταν στο κατάστημα Μώλου στη Λεμεσό, το οποίο έχει τερματίσει τις εργασίες του. Τα αρχεία εκείνου του καταστήματος έχουν φυλαχθεί σε συγκεκριμένες αποθήκες και μέχρι σήμερα δεν κατέστη δυνατός ο εντοπισμός του συγκεκριμένου εγγράφου. Παρόλα αυτά, η Καθ'ης την καταγγελία δεν θεωρεί ότι έχει γίνει παραβίαση των άρθρων 4 και 5(1)(στ) του Κανονισμού, εφόσον δεν μπορεί να αποδειχθεί οποιαδήποτε παραβίαση της ασφάλειας που οδήγησε σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση προσωπικών δεδομένων που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. Αφενός δεν υπήρξε οποιαδήποτε απώλεια προσωπικών δεδομένων του πελάτη και αφετέρου το έντυπο δεν περιείχε στοιχεία, όπως αποτελέσματα ιατρικών εξετάσεων, αξιολογήσεις θεραπόντων ιατρών ή οποιαδήποτε δεδομένα που εμπίπτουν στις ειδικές κατηγορίες προσωπικών δεδομένων.

(δ) Η Τράπεζα δεν έχει την παραμικρή εύλογη υποψία ότι, το έντυπο βρίσκεται οπουδήποτε εκτός της Τράπεζας. Η δυσκολία στην ανεύρεση του οφείλεται στο γεγονός ότι, το 2000 η διαδικασία αρχειοθέτησης δεν προνοούσε ηλεκτρονική φύλαξη αρχείων και αφετέρου στη μεταφορά των λογαριασμών του πελάτη από τη Λεμεσό στη Λευκωσία σε κατάστημα που επίσης έχει τερματίσει τη λειτουργία του και τα αρχεία του μεταφέρθηκαν στα κεντρικά αρχεία της Τράπεζας. Συνεπώς, πιστεύουν ότι δεν έχει παραβιαστεί το άρθρο 32 του Κανονισμού, γι' αυτό η Τράπεζα δεν προέβη σε γνωστοποίηση της οποιασδήποτε παραβίασης προσωπικών δεδομένων, όπως προβλέπουν οι διατάξεις του άρθρου 33 του Κανονισμού.

(ε) Από το 2012, η εταιρεία Eurolife Ltd, έχει αυτοματοποιήσει την αποστολή βεβαίωσης πιστοποιητικών ασφαλίστρων και ως εκ τούτου ο παραπονούμενος λάμβανε σχετική ενημέρωση κάθε χρόνο τουλάχιστον από το 2012. Ως εκ τούτου, η Τράπεζα είναι σε συμμόρφωση με το άρθρο 15 του Κανονισμού, που αφορά στο δικαίωμα πρόσβασης. Με τις βεβαιώσεις ασφαλίστρων, η Τράπεζα του κοινοποιούσε σε ετήσια βάση, από το 2012, τα πιο κάτω στοιχεία:

- Αριθμός ασφαλιστικής σύμβασης
- Τίτλος ασφαλιστικής σύμβασης
- Ημερομηνία ανανέωσης
- Ονοματεπώνυμο ασφαλισμένου μέλους
- Αριθμό ταυτότητας ασφαλισμένου μέλους
- Αριθμό πιστοποιητικού ασφάλισης
- Ασφαλισμένο ποσό
- Ημερομηνία ένταξης
- Περίοδος κάλυψης
- Ασφάλιστρο ζωής
- Ασφάλιστρο ολικής ανικανότητας
- Πληρωθέν ασφάλιστρο

Τα πιο πάνω αποτελούν απόδειξη συμμόρφωσης των δραστηριοτήτων επεξεργασίας των δεδομένων.

(στ) Από το 2000 μέχρι σήμερα, η διαδικασία αρχειοθέτησης έχει βελτιωθεί σημαντικά. Συγκεκριμένα, πλέον οι αιτήσεις αρχειοθετούνται τόσο ηλεκτρονικά όσο και στους φακέλους των πελατών οι οποίοι βρίσκονται σε πυρασφαλή χώρο *(επισυνάφθηκε η σημερινή καταγεγραμμένη διαδικασία αρχειοθέτησης)*.

(ζ) Τα σημερινά μέτρα είναι κατάλληλα και αποτελεσματικά σύμφωνα με το άρθρο 5(2) και ότι από το 2000 μέχρι σήμερα οι διαδικασίες βελτιώνονται, αναβαθμίζονται και εξελίσσονται με την πάροδο της τεχνολογίας.

(η) Από το Μάιο 2018, η Τράπεζα συμμορφώνεται πλήρως με τον Κανονισμό. Συγκεκριμένα, εκτελεί όλα τα αιτήματα των πελατών της αναφορικά με τα δικαιώματα τους και προχωρεί σε άμεση ενημέρωση προς την Επίτροπο σχετικά με θέματα διαρροής πληροφοριών και ενεργεί βάσει των οδηγιών της. Περαιτέρω, η Τράπεζα έχει υιοθετήσει σχετική πολιτική διατήρησης αρχείων, την οποία έθεσε σε εφαρμογή το 2020. Η Τράπεζα έχει επίσης καταγράψει τις διαδικασίες της σε αρχείο δραστηριοτήτων και έχει διενεργήσει εκτίμηση αντικτύπου για όλες τις διαδικασίες και τα συστήματα που τις υποστηρίζουν. Όπου κρίθηκε αναγκαίο, προέβη σε αναθεώρηση διαδικασιών ή τέθηκαν χρονοδιαγράμματα για τις ενέργειες που απαιτούνται να λάβουν χώρα.

(θ) Αναφορικά με την διαδικασία αρχειοθέτησης, από το 2011 η Τράπεζα έχει ξεκινήσει τη σάρωση διάφορων συμφωνιών και εντύπων που υπογράφει ο πελάτης και σήμερα τα περισσότερα έντυπα είναι σαρωμένα. Αυτό βοηθά τόσο τον εύκολο αλλά και ασφαλέστερο τρόπο αρχειοθέτησης τους αλλά και την άμεση διαθεσιμότητα των στοιχείων αυτών σε περίπτωση που τα υποκείμενα των δεδομένων ασκούν το δικαίωμα πρόσβασης με βάση τον Κανονισμό. Συγκεκριμένα, πλέον οι εν λόγω αιτήσεις συμμετοχής αρχειοθετούνται τόσο ηλεκτρονικά όσο και στους φακέλους των πελατών οι οποίοι βρίσκονται σε πυρασφαλή χώρο.

(ι) Η Καθ'ης την καταγγελία δεν προέβη σε γνωστοποίηση του περιστατικού καθότι δεν υπάρχει η παραμικρή υποψία ότι το έγγραφο βρίσκεται εκτός της Τράπεζας. Λαμβάνοντας υπόψη το κλείσιμο των καταστημάτων, την συγχώνευση της Τράπεζας με την πρώην Λαϊκή Τράπεζα και των αλλαγών των αποθηκευτικών χώρων, δεν είναι σίγουρο κατά πόσο το σχετικό έγγραφο έχει χαθεί ή απλά έχει τοποθετηθεί σε λάθος χώρο με βάση τις διαδικασίες αρχειοθέτησης και ως εκ τούτου δεν κατέστη δυνατή μέχρι σήμερα η πρόσβαση στο συμβόλαιο οριοασφάλισης.

Νομικό Πλαίσιο

2.1. Άρθρο 4 - Ορισμοί:

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

««επεξεργασία»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.».

««σύστημα αρχειοθέτησης»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.».

««υπεύθυνος επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.».

««δεδομένα που αφορούν την υγεία»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.».

««παραβίαση δεδομένων προσωπικού χαρακτήρα»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία».

Το άρθρο 9(1) του Κανονισμού προβλέπει ότι οι **«ειδικές κατηγορίες προσωπικών δεδομένων»** νοούνται τα προσωπικά δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

2.2. Άρθρο 5 – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα:

Οι αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων ορίζονται στο άρθρο 5(1) του Κανονισμού. Μεταξύ αυτών, τα προσωπικά δεδομένα *«υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή*

φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).» (άρθρο 5(1)(στ)).

Επιπρόσθετα, η παρ. (2) του ίδιου άρθρου προβλέπει ότι «ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»)».

2.4. Άρθρο 15 – Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων:

2.4.1. Βάσει του άρθρου 15 του Κανονισμού:

«1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις ακόλουθες πληροφορίες:

α) τους σκοπούς της επεξεργασίας,

β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα,

γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,

δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

ε) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία,

στ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

ζ) όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους,

η) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που προβλέπεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.».

Περαιτέρω, τα εδάφια 3 και 4 του ίδιου άρθρου προβλέπουν ότι:

«3. Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Για επιπλέον αντίγραφα που ενδέχεται να ζητηθούν από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας μπορεί να επιβάλει την καταβολή εύλογου τέλους για διοικητικά έξοδα. Εάν το υποκείμενο των δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα και εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό, η ενημέρωση παρέχεται σε ηλεκτρονική μορφή που χρησιμοποιείται συνήθως.

4. Το δικαίωμα να λαμβάνεται αντίγραφο που αναφέρεται στην παράγραφο 3 δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.».

2.4.2. Η αιτιολογική σκέψη 63 του Κανονισμού ορίζει ότι:

«**Ένα υποκείμενο των δεδομένων θα πρέπει να έχει δικαίωμα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα τα οποία συλλέχθηκαν και το αφορούν** και να μπορεί να ασκεί το εν λόγω δικαίωμα ευχερώς και σε εύλογα τακτά διαστήματα, **προκειμένου να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας.** Αυτό περιλαμβάνει το δικαίωμα των υποκειμένων των δεδομένων να έχουν **πρόσβαση στα δεδομένα που αφορούν την υγεία τους, για παράδειγμα τα δεδομένα των ιατρικών αρχείων τους τα οποία περιέχουν πληροφορίες όπως διαγνώσεις, αποτελέσματα εξετάσεων, αξιολογήσεις από θεράποντες ιατρούς και κάθε παρασχεθείσα θεραπεία ή επέμβαση. Επομένως, κάθε υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να γνωρίζει και να του ανακοινώνεται ιδίως για ποιους σκοπούς γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, εφόσον είναι δυνατόν για πόσο διάστημα γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ποιοι αποδέκτες λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα, ποια λογική ακολουθείται στην τυχόν αυτόματη επεξεργασία δεδομένων προσωπικού χαρακτήρα** και ποιες θα μπορούσαν να είναι οι συνέπειες της εν λόγω επεξεργασίας, τουλάχιστον όταν αυτή βασίζεται σε κατάρτιση προφίλ. Ο υπεύθυνος επεξεργασίας θα πρέπει να δύναται να παρέχει πρόσβαση εξ αποστάσεως σε ασφαλές σύστημα μέσω του οποίου το υποκείμενο των δεδομένων αποκτά άμεση πρόσβαση στα δεδομένα που το αφορούν. Το δικαίωμα αυτό δεν θα πρέπει να επηρεάζει αρνητικά τα δικαιώματα ή τις ελευθερίες άλλων, όπως το επαγγελματικό απόρρητο ή το δικαίωμα διανοητικής ιδιοκτησίας και, ειδικότερα, το δικαίωμα δημιουργού που προστατεύει το λογισμικό. Ωστόσο, οι παράγοντες αυτοί δεν θα πρέπει να έχουν ως αποτέλεσμα την άρνηση παροχής κάθε πληροφορίας στο υποκείμενο των δεδομένων. Όταν ο υπεύθυνος επεξεργασίας επεξεργάζεται μεγάλες ποσότητες πληροφοριών σχετικά με το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας θα πρέπει να δύναται να ζητεί από το υποκείμενο, πριν δοθούν οι πληροφορίες, να προσδιορίζει τις πληροφορίες ή τις δραστηριότητες επεξεργασίας που σχετίζονται με το αίτημα.».

2.5. Άρθρο 32 – Ασφάλεια επεξεργασίας:

2.5.1. Σύμφωνα με τις διατάξεις του άρθρου 32 του Κανονισμού, που αφορούν στην ασφάλεια της επεξεργασίας:

«1. 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, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:»

«β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,

γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,

δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.».

2.5.2. Στην παράγραφο 2 του ίδιου άρθρου, αναφέρεται ότι:

«Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία».

2.5.3. Σύμφωνα με το τελευταίο εδάφιο της αιτιολογικής σκέψης 39 του Κανονισμού:

«Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υφίστανται επεξεργασία κατά τρόπο που να διασφαλίζει την ενδεδειγμένη προστασία και εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων και για να αποτρέπεται κάθε ανεξουσιοδότητη πρόσβαση σε αυτά τα δεδομένα προσωπικού χαρακτήρα και στον εξοπλισμό που χρησιμοποιείται για την επεξεργασία τους ή η χρήση αυτών των δεδομένων προσωπικού χαρακτήρα και του εν λόγω εξοπλισμού.».

2.5.4. Η αιτιολογική σκέψη 74 του Κανονισμού αναφέρει ότι:

«Θα πρέπει να θεσπιστεί ευθύνη και υποχρέωση αποζημίωσης του υπευθύνου επεξεργασίας για οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα που γίνεται από τον υπεύθυνο επεξεργασίας ή για λογαριασμό του υπευθύνου επεξεργασίας. Ειδικότερα, ο υπεύθυνος επεξεργασίας θα πρέπει να υποχρεούται να υλοποιεί κατάλληλα και αποτελεσματικά μέτρα και να είναι σε θέση να αποδεικνύει τη συμμόρφωση των δραστηριοτήτων επεξεργασίας με τον παρόντα κανονισμό, συμπεριλαμβανομένης της αποτελεσματικότητας των μέτρων. Τα εν λόγω μέτρα θα πρέπει να λαμβάνουν υπόψη τη φύση, το πλαίσιο, το πεδίο εφαρμογής και τους σκοπούς της επεξεργασίας και τον κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.».

2.5.5. Αναφορικά με το άρθρο 32 του Κανονισμού, η αιτιολογική σκέψη 83 του Κανονισμού συμπληρώνει ότι:

«Για τη διατήρηση της ασφάλειας και την αποφυγή της επεξεργασίας κατά παράβαση του παρόντος κανονισμού, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να αξιολογεί τους κινδύνους που ενέχει η επεξεργασία και να εφαρμόζει μέτρα για το μετριασμό των εν λόγω κινδύνων, όπως για παράδειγμα μέσω κρυπτογράφησης. Τα εν λόγω μέτρα θα πρέπει να διασφαλίζουν κατάλληλο επίπεδο ασφάλειας, πράγμα που περιλαμβάνει και την εμπιστευτικότητα...Κατά την εκτίμηση του κινδύνου για την ασφάλεια των δεδομένων θα πρέπει να δίνεται προσοχή στους κινδύνους που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα...».

2.6. Άρθρο 33 – Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή:

2.6.1. Το άρθρο 33 του Κανονισμού ορίζει συγκεκριμένες υποχρεώσεις για τους υπευθύνους επεξεργασίας όσον αφορά στα περιστατικά παραβίασης προσωπικών δεδομένων. Συγκεκριμένα, σε περίπτωση παραβίασης προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των προσωπικών δεδομένων στην αρμόδια εποπτική αρχή, εκτός εάν η παραβίαση προσωπικών δεδομένων δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

2.6.2. Αναφορικά με τη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα, η αιτιολογική σκέψη 85 ορίζει τα εξής:

«Η παραβίαση δεδομένων προσωπικού χαρακτήρα μπορεί, εάν δεν αντιμετωπιστεί κατάλληλα και έγκαιρα, να έχει ως αποτέλεσμα σωματική, υλική ή μη υλική βλάβη για φυσικά πρόσωπα, όπως απώλεια του ελέγχου επί των δεδομένων τους προσωπικού χαρακτήρα ή ο περιορισμός των δικαιωμάτων τους, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, βλάβη της φήμης, απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο ή άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα για το ενδιαφερόμενο φυσικό πρόσωπο. Κατά συνέπεια, αμέσως μόλις ο υπεύθυνος επεξεργασίας λάβει γνώση μιας παραβίασης δεδομένων προσωπικού χαρακτήρα,

θα πρέπει αμελλητί και, ει δυνατόν, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, να γνωστοποιήσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή, εκτός εάν ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει, σύμφωνα με την αρχή της λογοδοσίας, ότι η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Εάν μια τέτοια γνωστοποίηση δεν μπορεί να επιτευχθεί εντός 72 ωρών, η γνωστοποίηση θα πρέπει να συνοδεύεται από αιτιολογία η οποία αναφέρει τους λόγους της καθυστέρησης και οι πληροφορίες μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.».

2.6.3. Σχετικά με το άρθρο 33 του Κανονισμού, η αιτιολογική σκέψη 87 του Κανονισμού συμπληρώνει ότι:

«Θα πρέπει να εξακριβώνεται κατά πόσον έχουν τεθεί σε εφαρμογή όλα τα κατάλληλα μέτρα τεχνολογικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης δεδομένων προσωπικού χαρακτήρα και την άμεση ενημέρωση της εποπτικής αρχής και του υποκειμένου των δεδομένων», όπως αναλυτικά αναφέρονται στις από 06-02-2018 Κατευθυντήριες Γραμμές της ΟΕ 29 *(Ομάδας Εργασίας του Άρθρου 29)* για την γνωστοποίηση παραβίασης δεδομένων (WP 250 rev. 1).

2.6.4. Σύμφωνα με τις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ (*νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων –EDPB)* για την Γνωστοποίηση παραβίασης προσωπικών δεδομένων *("Guidelines on Personal data breach notification under Regulation 2016/679 WP 250 rev. 1)*, ημερομηνίας 06.02.2018, δύο τύποι παραβίασης προσωπικών δεδομένων είναι αυτοί που κατηγοριοποιούνται ως «απώλεια» και «παραβίαση διαθεσιμότητας».

Συγκεκριμένα, σύμφωνα με τις ανωτέρω Κατευθυντήριες Γραμμές:

«Όσον αφορά την «απώλεια» δεδομένων προσωπικού χαρακτήρα, ο όρος θα πρέπει να ερμηνεύεται ως μια περίπτωση όπου τα δεδομένα μπορεί να εξακολουθούν να υπάρχουν, αλλά ο υπεύθυνος επεξεργασίας έχει χάσει τον έλεγχό τους ή την πρόσβαση σ' αυτά ή δεν τα έχει πλέον στην κατοχή του.».

«Παραβίαση διαθεσιμότητας» – όταν υπάρχει τυχαία ή μη εξουσιοδοτημένη απώλεια πρόσβασης[1] σε δεδομένα προσωπικού χαρακτήρα ή τυχαία ή μη εξουσιοδοτημένη καταστροφή δεδομένων προσωπικού χαρακτήρα.

«Παρότι το εάν έχει διαπραχθεί παραβίαση της εμπιστευτικότητας ή της ακεραιότητας είναι σχετικά σαφές, το εάν έχει διαπραχθεί παραβίαση της διαθεσιμότητας ενδέχεται να είναι λιγότερο προφανές. **Μια παραβίαση θα θεωρείται πάντα ότι συνιστά παραβίαση της διαθεσιμότητας όταν υπάρχει οριστική απώλεια ή καταστροφή δεδομένων προσωπικού χαρακτήρα.»**.

«Συνεπώς, ένα περιστατικό ασφάλειας που έχει ως αποτέλεσμα τη μη διαθεσιμότητα δεδομένων προσωπικού χαρακτήρα για ένα χρονικό διάστημα είναι επίσης ένα είδος παραβίασης, δεδομένου ότι η έλλειψη πρόσβασης στα δεδομένα μπορεί να έχει σημαντικό αντίκτυπο στα δικαιώματα και στις ελευθερίες των φυσικών προσώπων.».

[1] Αποτελεί κοινή παραδοχή ότι η «πρόσβαση» αποτελεί θεμελιώδες μέρος της «διαθεσιμότητας». Βλ., για παράδειγμα, το πρότυπο NIST SP800-53rev4, το οποίο ορίζει τη «διαθεσιμότητα» ως εξής: «Εξασφάλιση έγκαιρης και αξιόπιστης πρόσβασης σε πληροφορίες και χρήσης αυτών», διαθέσιμο στη διεύθυνση http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Το πρότυπο CNSSI-4009 αναφέρεται επίσης στην: «Έγκαιρη, αξιόπιστη πρόσβαση σε δεδομένα και υπηρεσίες των πληροφοριών για εξουσιοδοτημένους χρήστες.» Βλ. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Το πρότυπο ISO/IEC 27000:2016 ορίζει επίσης τη «διαθεσιμότητα» ως την «Ιδιότητα προσβασιμότητας και ετοιμότητας προς χρήση κατόπιν αιτήματος εξουσιοδοτημένου φορέα»: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Παρατίθενται επίσης τα ακόλουθα, σχετικά με την υπόθεση αποσπάσματα, των ίδιων Κατευθυντήριων Γραμμών:

«Οποιοδήποτε σχέδιο αντιμετώπισης παραβιάσεων θα πρέπει να εστιάζει στην προστασία των προσώπων και των δεδομένων προσωπικού χαρακτήρα τους. Συνεπώς, η γνωστοποίηση παραβιάσεων θα πρέπει να θεωρείται ένα εργαλείο που βελτιώνει τη συμμόρφωση όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα. **Παράλληλα, θα πρέπει να σημειωθεί ότι η μη αναφορά μιας παραβίασης είτε σε ένα πρόσωπο είτε σε μια εποπτική αρχή μπορεί να σημαίνει ότι, δυνάμει του άρθρου 83, είναι πιθανό να επιβληθεί κύρωση στον υπεύθυνο επεξεργασίας.**

Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία ενθαρρύνονται να σχεδιάζουν εκ των προτέρων και να εφαρμόζουν διαδικασίες με στόχο τον εντοπισμό και τον έγκαιρο περιορισμό μιας παραβίασης, την αξιολόγηση του κινδύνου για τα πρόσωπα[2] και, στη συνέχεια, τη λήψη απόφασης σχετικά με το αν είναι αναγκαία η ενημέρωση της αρμόδιας εποπτικής αρχής και η ανακοίνωση της παραβίασης στα ενδιαφερόμενα πρόσωπα, όταν είναι αναγκαίο. **Η γνωστοποίηση στην εποπτική αρχή θα πρέπει να αποτελεί μέρος αυτού του σχεδίου αντιμετώπισης περιστατικών.»**
«...βασικό χαρακτηριστικό οποιασδήποτε πολιτικής ασφάλειας δεδομένων είναι να παρέχει τη δυνατότητα, όταν είναι εφικτό, αποτροπής μιας παραβίασης και, αν παρ' ελπίδα αυτή συμβεί, έγκαιρης αντίδρασης.».

«Είναι επίσης σημαντικό να λαμβάνεται υπόψη ότι, **σε ορισμένες περιπτώσεις, η μη γνωστοποίηση μιας παραβίασης θα μπορούσε να υποδεικνύει είτε την απουσία υφιστάμενων μέτρων ασφάλειας είτε την ανεπάρκεια των υφιστάμενων μέτρων ασφάλειας.».**

«Η ΟΕ 29 θεωρεί ότι ένας υπεύθυνος επεξεργασίας θα πρέπει να θεωρείται ότι αποκτά «γνώση» όταν ο εν λόγω υπεύθυνος επεξεργασίας έχει εύλογο βαθμό βεβαιότητας ότι έχει προκύψει περιστατικό ασφάλειας το οποίο έχει ως αποτέλεσμα να τεθούν σε κίνδυνο τα δεδομένα προσωπικού χαρακτήρα.».

«Το άρθρο 26 αφορά τους από κοινού υπευθύνους επεξεργασίας και διευκρινίζει ότι οι από κοινού υπεύθυνοι επεξεργασίας καθορίζουν τις αντίστοιχες αρμοδιότητές τους όσον αφορά τη συμμόρφωση με τον ΓΚΠΔ[3]. Σ' αυτό θα περιλαμβάνεται ο καθορισμός του μέρους που θα έχει την ευθύνη για τη συμμόρφωση με τις υποχρεώσεις δυνάμει των άρθρων 33 και 34. Η ΟΕ29 συνιστά οι συμβατικές ρυθμίσεις μεταξύ των από κοινού υπευθύνων επεξεργασίας να περιλαμβάνουν διατάξεις που να καθορίζουν ποιος υπεύθυνος επεξεργασίας θα φέρει την ευθύνη για τη συμμόρφωση με τις υποχρεώσεις γνωστοποίησης παραβιάσεων του ΓΚΠΔ.»

«Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι, σε περίπτωση παραβίασης που «δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων», δεν απαιτείται γνωστοποίηση στην εποπτική αρχή. Ένα παράδειγμα μπορεί να είναι η περίπτωση όπου τα δεδομένα προσωπικού χαρακτήρα είναι ήδη διαθέσιμα στο κοινό και η κοινοποίησή τους δεν επιφέρει πιθανό κίνδυνο για το πρόσωπο.».

«Μια παραβίαση μπορεί να επηρεάζει μόνο ένα πρόσωπο ή μικρό αριθμό προσώπων ή και μερικές χιλιάδες, εάν όχι περισσότερα. Σε γενικές γραμμές, όσο υψηλότερος είναι ο αριθμός των επηρεαζόμενων προσώπων, τόσο μεγαλύτερο αντίκτυπο μπορεί να έχει μια παραβίαση. Ωστόσο, μια παραβίαση μπορεί να έχει σοβαρό αντίκτυπο ακόμη και σε ένα πρόσωπο, ανάλογα με τη φύση των δεδομένων προσωπικού χαρακτήρα και το πλαίσιο εντός του οποίου έχουν τεθεί σε κίνδυνο.».

---

[2] Αυτό μπορεί να διασφαλιστεί στο πλαίσιο της υποχρέωσης παρακολούθησης και επανεξέτασης μιας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ), η οποία αφορά τις διαδικασίες επεξεργασίας που ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (άρθρο 35 παράγραφοι 1 και 11).
[3] Βλ. επίσης αιτιολογική σκέψη 79 *(του Κανονισμού)*.

2.6.5. Παρατίθενται τα ακόλουθα αποσπάσματα από το βιβλίο των Λ. Κοτσαλή - Κ. Μενουδάκο, με τίτλο Γενικός Κανονισμός Προστασίας Δεδομένων - Νομική διάσταση και πρακτική εφαρμογή, κεφ. VI., που αφορούν στη γνωστοποίηση παραβιάσεων προσωπικών δεδομένων:

«Στον νέο Κανονισμό οι «αρχές της επεξεργασίας» συμπεριλαμβάνουν την «ακεραιότητα» και την «εμπιστευτικότητα» (άρθρο 5 παρ. 1 στ). Η υποχρέωση της εμπιστευτικότητας και της λήψης τεχνικών και οργανωτικών μέτρων ασφάλειας συμπεριλαμβανόταν στις υποχρεώσεις του υπευθύνου επεξεργασίας που είχε εισάγει ήδη η Οδηγία 95/46/ΕΚ: Ειδικότερα ο υπεύθυνος επεξεργασίας όφειλε να εξασφαλίζει επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγονται η επεξεργασία και η φύση των δεδομένων, έτσι ώστε να προστατεύονται τα δεδομένα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.».

«Ο Γενικός Κανονισμός Προστασίας Δεδομένων προσθέτει στην αντίστοιχη ρύθμιση (άρθρο 32) έναν ενδεικτικό κατάλογο μέτρων ασφαλείας, όπως η ψευδωνυμοποίηση και η κρυπτογράφηση αλλά και διαδικασιών που συνίστανται εν τέλει στην υιοθέτηση ολιστικής πολιτικής ασφάλειας. Ταυτόχρονα η λήψη τεχνικών και οργανωτικών μέτρων φαίνεται να υιοθετείται εμφατικά ως πρόσθετη υποχρέωση ή εγγύηση που εξισορροπεί μορφές ή διαδικασίες επεξεργασίας δεδομένων που ενέχουν κινδύνους για τα δικαιώματα των προσώπων.».

«Ο ενωσιακός νομοθέτης ορίζει τι αντιλαμβάνεται ως παραβίαση δεδομένων προσωπικού χαρακτήρα: σύμφωνα με το άρθρο 4(12) πρόκειται για την παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. Όπως διευκρινίζει η Ομάδα του Άρθρου 29 ενδέχεται να πρόκειται για μία παραβίαση της εμπιστευτικότητας, της διαθεσιμότητας ή της ακεραιότητας των δεδομένων ή για ένα συνδυασμό αυτών. Ο Κανονισμός υποχρεώνει σε γνωστοποίηση της παραβίασης δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή».

«Η Ομάδα του Άρθρου 29 διευκρινίζει ωστόσο ότι για να αντιμετωπιστεί μία παραβίαση ως παραβίαση διαθεσιμότητας θα πρέπει να συντρέχει μία μόνιμη απώλεια ή καταστροφή δεδομένων. Σημειώνει ωστόσο ότι ενδεχομένως και μία μη μόνιμη παραβίαση που οδηγεί σε μη διαθεσιμότητα να απαιτεί γνωστοποίηση λαμβάνοντας υπόψη πιθανούς κινδύνους για τα δικαιώματα των προσώπων. Βλ. Article 29 Data Protection Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, 03/10/2017 (WP 250), σελ. 6».

2.7. Αποφάσεις

Χρήσιμη παραπομπή μπορεί να γίνει και στα πιο κάτω αποσπάσματα της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα:

Απόφαση Αρ. 98/2013

«Καταρχάς η ασφάλεια εξειδικεύεται σε τρεις βασικούς στόχους, ήτοι την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, ενώ συμπληρωματικοί στόχοι, ιδίως από τη σκοπιά της προστασίας των προσωπικών δεδομένων, αποτελούν ιδίως η μη αποποίηση της ευθύνης (ή λογοδοσία) καθώς και ο διαχωρισμός των δεδομένων ανάλογα με το σκοπό της επεξεργασίας. Κατά τα διεθνώς αποδεκτά πρότυπα ασφάλειας πληροφοριακών συστημάτων (π.χ. βλ. σειρά ISO/IEC 27000) τα κατάλληλα μέτρα κατά το άρθρο 10 παρ. 3 ν. 2472/1997 εντάσσονται σε ένα Σύστημα Ασφάλειας Πληροφοριακών Συστημάτων (ISMS). Το εν λόγω Σύστημα προϋποθέτει την εκπόνηση μελέτης επικινδυνότητας με βάση τους κινδύνους και τη φύση των δεδομένων, και μεταξύ άλλων περιλαμβάνει την κατάρτιση πολιτικής και σχεδίων ασφάλειας, όπου προσδιορίζονται συγκεκριμένα τεχνικά και οργανωτικά μέτρα. Τα μέτρα αυτά, εκτός του ότι πρέπει να εφαρμόζονται, επιπλέον παρακολουθούνται και αξιολογούνται με σκοπό τη διαρκή προσαρμογή τους στις επιχειρησιακές

ανάγκες του υπευθύνου επεξεργασίας και στις τεχνολογικές εξελίξεις, τις οποίες οφείλει να λαμβάνει υπ΄ όψιν ο υπεύθυνος επεξεργασίας (βλ. άρθρο 17 παρ. 1 Οδηγία 95/46/ΕΚ).».

Απόφαση Αρ. 44/2019

«Εν όψει των ανωτέρω η Αρχή κρίνει ότι η ελεγχόμενη εταιρία AMPNI ως υπεύθυνος επεξεργασίας:

Αφενός, δεν εφάρμοσε το σύνολο των αρχών του άρθρου 5 παρ. 1 ΓΚΠΔ και 6 παρ. 1 ΓΚΠΔ σχετικά με τη νομιμότητα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα ..... που λάμβανε χώρα στη χρησιμοποιούμενη υπολογιστική υποδομή ..... αλλά και στο πλαίσιο κάθε μεταγενέστερης ή περαιτέρω επεξεργασίας των ίδιων δεδομένων προσωπικού χαρακτήρα, ούτε απέδειξε κατ' αρ. 5 παρ. 2 ΓΚΠΔ την τήρηση αυτών.

Αφετέρου, παραβίασε τις διατάξεις των άρθρων 5 παρ. 1 εδ. α' και στ' και παρ. 2 σε συνδυασμό με τα άρθρα 24 παρ. 1 και 2 και 32 παρ. 1 και 2 ΓΚΠΔ σχετικά με την αρχή της ασφαλούς επεξεργασίας (ιδίως της «εμπιστευτικότητας») των δεδομένων προσωπικού χαρακτήρα που λάμβανε χώρα στη χρησιμοποιούμενη υπολογιστική υποδομή ..... από την μη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων, αλλά και στο πλαίσιο κάθε μεταγενέστερης ή περαιτέρω επεξεργασίας των ίδιων δεδομένων προσωπικού χαρακτήρα, ώστε να παρέλκει η εξέταση της τήρησης των αρχών επεξεργασίας των εδαφίων β', γ', δ' και ε' της παρ. 1 του άρθρου 5 καθώς και του άρθρου 6 παρ. 1 ΓΚΠΔ...».

3. Σκεπτικό

3.1. Τα δεδομένα που περιλαμβάνονται σε ασφαλιστήριο συμβόλαιο και αφορούν σε πρόσωπο εν ζωή συνιστούν **«δεδομένα προσωπικού χαρακτήρα».**

Τα δε δεδομένα που αφορούν στην υγεία και/ή στο ιατρικό ιστορικό φυσικού προσώπου εν ζωή, στο μέτρο που αποκαλύπτεται αμέσως ή εμμέσως η ταυτότητα του, αποτελούν **«ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα»**, σύμφωνα με τον ορισμό που δίδεται στο άρθρο 9(1) του Κανονισμού.

Τα ασφαλιστήρια συμβόλαια που τηρούνται από την Εταιρεία και αφορούν στους πελάτες-ασφαλίζομενους της συνιστά **«σύστημα αρχειοθέτησης»** βάσει του ορισμού στο άρθρο 4(6) του Κανονισμού.

Η συλλογή, καταχώρηση, χρήση, αναζήτηση, συσχέτιση/συνδυασμός και η αποθήκευση προσωπικών δεδομένων αποτελούν **επεξεργασία προσωπικών δεδομένων**, κατά την έννοια του άρθρου 4(2) του Κανονισμού.

Υπεύθυνος επεξεργασίας είναι *η Τράπεζα Κύπρου Δημόσια Εταιρεία Λτδ* (άρθρο 4(7) του Κανονισμού).

Υποκείμενα των δεδομένων είναι *οι πελάτες της Τράπεζας Κύπρου Δημόσιας Εταιρείας Λτδ* (άρθρο 4(1) του Κανονισμού).

3.2. Τα προσωπικά δεδομένα για να τύχουν νόμιμης επεξεργασίας θα πρέπει να πληρούνται σωρευτικά οι προϋποθέσεις τήρησης των αρχών που διέπουν την επεξεργασία προσωπικών δεδομένων (άρθρο 5 του Κανονισμού), όπως εξάλλου προκύπτει και από την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ) ημερ. 16.01.2019 στην υπόθεση C-496/2017 Deutsche Post AG κατά Hauptzollamt Köln[4]. Σύμφωνα με την εν λόγω Απόφαση, η ύπαρξη ενός νόμιμου

[4] «57. Ωστόσο, κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι σύμφωνη, αφενός, προς τις αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων, τις οποίες θέτει το άρθρο 6 της οδηγίας 95/46 ή το άρθρο 5 του κανονισμού 2016/679 και, αφετέρου, προς τις βασικές αρχές της νόμιμης επεξεργασίας δεδομένων που απαριθμεί το άρθρο 7 της οδηγίας αυτής ή το άρθρο 6 του κανονισμού αυτού (πρβλ. αποφάσεις της 20ής Μαΐου 2003, Österreichischer

θεμελίου (άρθρου 6(1) του Κανονισμού) δεν απαλλάσσει τον υπεύθυνο επεξεργασίας από την υποχρέωση τήρησης των αρχών (άρθρο 5 του Κανονισμού).

3.3. Όπως σχετικά αναφέρει και ο Γρηγόρης Τσόλιας, Δικηγόρος, Μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και Μέλος του Expert Group της Ε.Ε. για τον Κανονισμό 2016/679 και την Οδηγία 2016/680:

«Σωρευτική πλήρωση προϋποθέσεων εφαρμογής και τήρησης αρχών αρ.5 παρ.1 και 6 ΓΚΠΔ *(Γενικός Κανονισμός Προστασίας Δεδομένων)*

• Η ύπαρξη ενός νόμιμου θεμελίου (αρ. 6 παρ.1 ΓΚΠΔ () δεν απαλλάσσει τον υπ. επ *(υπεύθυνο επεξεργασίας)* από την υποχρέωση τήρησης των αρχών του άρ.5 παρ.1 ΓΚΠΔ. Η κατά παράβαση των αρχών του αρ.5 ΓΚΠΔ μη νόμιμη συλλογή και επεξεργασία δεν θεραπεύεται από την ύπαρξη νόμιμου σκοπού

• Εάν παραβιάζεται μια από τις αρχές του άρθρου 5 παρ.1 ΓΚΠΔ (π.χ. θεμιτή και νόμιμη επεξεργασία, ασφάλεια) παρέλκει η εξέταση των λοιπών αρχών ή του άρθρου 6 παρ.1 ΓΚΠΔ.».

3.4. Επιπλέον, **ο υπεύθυνος επεξεργασίας βαρύνεται με το περαιτέρω καθήκον να αποδεικνύει ανά πάσα στιγμή τη συμμόρφωση του με τις αρχές** που διέπουν την επεξεργασία προσωπικών δεδομένων, όπως εκτίθενται στο άρθρο 5 του Κανονισμού. **Συγκεκριμένα, η λογοδοσία εντάσσεται στις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων και** συνεπάγεται τη δυνατότητα του υπευθύνου επεξεργασίας να αποδεικνύει συμμόρφωση με τον Κανονισμό. Επιπλέον, δίνει τη δυνατότητα στον υπεύθυνο επεξεργασίας να δύναται να ελέγξει και να τεκμηριώσει νομικά μια επεξεργασία που διενεργεί σύμφωνα με τις νομικές βάσεις που του παρέχει ο Κανονισμός.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα με διαφανή τρόπο συνιστά έκφανση της αρχής της θεμιτής επεξεργασίας και συνδέεται με την αρχή της λογοδοσίας, παρέχοντας το δικαίωμα στα υποκείμενα των δεδομένων να ασκούν έλεγχο επί των δεδομένων τους καθιστώντας υπόλογους τους υπεύθυνους επεξεργασίας (βλέπε Κατευθυντήριες Γραμμές ΟΕ 29, Guidelines on transparency under Regulation 2016/679, WP260).

Η αρχή της λογοδοσίας, στην ουσία μεταθέτει στον υπεύθυνο επεξεργασίας «το βάρος της απόδειξης» της νομιμότητας της επεξεργασίας.

3.5.1. Επιπροσθέτως, **ο υπεύθυνος επεξεργασίας βαρύνεται με την υποχρέωση να λαμβάνει, κατά το άρθρο 32 του Κανονισμού, τα κατάλληλα τεχνικά και οργανωτικά μέτρα** που να διασφαλίζουν το κατάλληλο επίπεδο ασφάλειας και προστασίας των προσωπικών δεδομένων ανάλογα προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Ειδικότερα, ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων που μπορεί να οδηγήσουν σε παραβίαση προσωπικών δεδομένων, κατά την έννοια του άρθρου 4(12) του Κανονισμού.

3.5.2. Από το γράμμα και τον σκοπό των διατάξεων της αιτιολογικής σκέψης 83 του Κανονισμού, είναι σαφές ότι, **η υποχρέωση τήρησης της ασφάλειας της επεξεργασίας από τον υπεύθυνο επεξεργασίας έχει τόσο προληπτικό, όσο και κατασταλτικό χαρακτήρα.** Προληπτικό, ούτως ώστε τα εφαρμοστέα μέτρα να μπορούν να αποτρέπουν περιστατικά παραβίασης προσωπικών δεδομένων και κατασταλτικό, ούτως ώστε τυχόν περιστατικό να μπορεί να ανιχνευθεί και να διερευνηθεί.

Παρόλο που όπως αναφέρει η Καθ'ης στην επιστολή της ημερομηνίας 20.02.2020, τα συμβόλαια οριοασφάλισης φυλάγονται σε αρχειοθετημένο κουτί φύλαξης στο αρμόδιο υποκατάστημα της

Rundfunk κ.λπ., C-465/00, C-138/01 και C-139/01, EU:C:2003:294, σκέψη 65, καθώς και της 13ης Μαΐου 2014, Google Spain και Google, C-131/12, EU:C:2014:317, σκέψη 71).»

Τράπεζας, τα οποία καταλήγουν στο κεντρικό αρχείο φύλαξης (θεματοφυλάκιο) της Τράπεζας, το οποίο, όπως ισχυρίζεται η Καθ'ης, κατέχει πιστοποίηση ISO και τηρεί όλα τα δέοντα μέτρα φύλαξης και ασφάλειας, εντούτοις το αποτέλεσμα ήταν ότι, το ασφαλιστήριο συμβόλαιο του παραπονούμενου δεν κατέστει δυνατό να ανευρεθεί. **Συνεπώς, διαπιστώνεται ότι, δεν λειτούργησαν κατά τον ορθό και ενδεδειγμένο τρόπο τα οργανωτικά και/ή τεχνικά μέτρα ασφάλειας, ως μέτρα προληπτικής φύσης, με επακόλουθο την αδυναμία ανεύρεσης του ασφαλιστήριου συμβολαίου.**

3.6.1. **Η απώλεια /παραβίαση της διαθεσιμότητας (αδυναμία εντοπισμού) του ασφαλιστήριου συμβολαίου του παραπονούμενου συνιστά παραβίαση προσωπικών δεδομένων** και αποδεικνύει την έλλειψη επαρκών και κατάλληλων τεχνικών και οργανωτικών μέτρων κατά το άρθρο 32 του Κανονισμού.

3.6.2. Αμέσως μόλις η Καθ'ης έλαβε γνώση της παραβίασης προσωπικών δεδομένων, θα έπρεπε αμελλητί και, αν είναι δυνατόν, εντός 72 ωρών από τη στιγμή που απέκτησε γνώση του γεγονότος, να γνωστοποιήσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο Γραφείο μου, όπως προβλέπουν οι διατάξεις του άρθρου 33 του Κανονισμού.

- Η Γνωστοποίηση στο Γραφείο μου δεν ήταν απαραίτητη εάν η Καθ'ης μπορούσε να αποδείξει ότι, η παραβίαση προσωπικών δεδομένων δεν θα προκαλούσε κίνδυνο για τα δικαιώματα και τις ελευθερίες του παραπονούμενου, **κάτι το οποίο η Καθ'ης δεν έπραξε.**

- Εάν μια τέτοια γνωστοποίηση δεν μπορούσε να επιτευχθεί εντός 72 ωρών, η γνωστοποίηση θα έπρεπε να συνοδεύεται από αιτιολογία η οποία θα ανέφερε τους λόγους της καθυστέρησης και οι πληροφορίες θα μπορούσαν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση, **κάτι το οποίο η Καθ'ης δεν έπραξε.**

- Σημειώνω ότι, το γεγονός ότι, ενημερώθηκα για την συγκεκριμένη παραβίαση προσωπικών δεδομένων μέσω της υποβολής παραπόνου/καταγγελίας στο Γραφείο μου από τον παραπονούμενο, είναι άσχετο και άνευ σημασίας, αφού **η υποχρέωση γνωστοποίησης παραβίασης προσωπικών δεδομένων βαρύνει τον υπεύθυνο επεξεργασίας.**

3.6.3. Συνεπώς, τα υποκείμενα των δεδομένων θα πρέπει να έχουν δικαίωμα πρόσβασης στα προσωπικά δεδομένα που τους αφορούν και να μπορούν να ασκούν το εν λόγω δικαίωμα ευχερώς και σε εύλογα τακτά διαστήματα, ούτως ώστε να έχουν επίγνωση και να επαληθεύουν τη νομιμότητα της επεξεργασίας. **Στην παρούσα υπόθεση, η μη ανεύρεση του ασφαλιστήριου συμβολαίου του παραπονούμενου προκάλεσε κίνδυνο για τα δικαιώματα του αφού, ο παραπονούμενος στερήθηκε του δικαιώματος πρόσβασης στο ασφαλιστήριο συμβόλαιο του, με αποτέλεσμα αφενός να μην μπορεί να ελέγξει την ορθότητα/ακρίβεια/εγκυρότητα των δεδομένων που περιέχονται σε αυτό και αφετέρου να μην μπορεί να επαληθεύσει τη νομιμότητα της επεξεργασίας.**

3.6.4. Ενόψει των όσων αναφέρθηκαν στις παραγράφους 3.6.1. – 3.6.3. ανωτέρω, η Καθ'ης την καταγγελία είχε υποχρέωση γνωστοποίησης του περιστατικού παραβίασης προσωπικών δεδομένων *(απώλεια/παραβίαση της διαθεσιμότητας - αδυναμία εντοπισμού - του ασφαλιστήριου συμβολαίου του παραπονούμενου).*

4. Συμπεράσματα

Στην υπό εξέταση περίπτωση, από τα στοιχεία του φακέλου της υπόθεσης και την παραδοχή της Καθ'ης την καταγγελία ότι, το επίμαχο ασφαλιστήριο συμβόλαιο δεν κατέστει δυνατό να ανευρεθεί, **εκ πρώτης όψεως, έχω την άποψη ότι, η Τράπεζα δεν συμμορφώθηκε με τις ακόλουθες υποχρεώσεις της που απορρέουν από τον Κανονισμό, δεδομένου ότι:**

4.1. Αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων

Βάσει του άρθρου 5(1)(στ) του Κανονισμού:
Δεν έλαβε τα απαραίτητα οργανωτικά και/ή τεχνικά μέτρα ώστε να εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά («ακεραιότητα και εμπιστευτικότητα»). Ως εκ τούτου, από την έλλειψη των κατάλληλων τεχνικών και/ή οργανωτικών μέτρων, επήλθε ο κίνδυνος για την εμπιστευτικότητα και/ή ακεραιότητα των δεδομένων προσωπικού χαρακτήρα μέσω της απώλειας[5] και/ή παραβίασης της διαθεσιμότητας[6] (αδυναμίας εντοπισμού) του ασφαλιστήριου συμβολαίου του παραπονούμενου.

Βάσει του άρθρου 5(2) και της αιτιολογικής σκέψης 74 του Κανονισμού:
Δεν υλοποίησε κατάλληλα και αποτελεσματικά μέτρα και δεν ήταν σε θέση να αποδείξει τη συμμόρφωση των δραστηριοτήτων επεξεργασίας της με τον Κανονισμό συμπεριλαμβανομένης της αποτελεσματικότητας των μέτρων αυτών.

4.2. Ασφάλεια επεξεργασίας

Βάσει του άρθρου 32 και της αιτιολογικής σκέψης 83 του Κανονισμού:

(α) Παρέβηκε της υποχρέωσης της να λάβει τα κατάλληλα οργανωτικά και/ή τεχνικά μέτρα για την ασφάλεια του ασφαλιστήριου συμβολαίου που περιείχε προσωπικά δεδομένα και την προστασία του από τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση που αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. Τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.

(β) Δεν αξιολόγησε τους κινδύνους που ενέχει η επεξεργασία και δεν έλαβε/εφάρμοσε μέτρα για τον μετριασμό των εν λόγω κινδύνων, όπως είναι η τυχαία ή παράνομη καταστροφή και η απώλεια.

---

[5] Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ (νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων –EDPB) για την Γνωστοποίηση παραβίασης προσωπικών δεδομένων: «Όσον αφορά την «απώλεια» δεδομένων προσωπικού χαρακτήρα, ο όρος θα πρέπει να ερμηνεύεται ως μια περίπτωση όπου τα δεδομένα μπορεί να εξακολουθούν να υπάρχουν, αλλά ο υπεύθυνος επεξεργασίας έχει χάσει τον έλεγχό τους ή την πρόσβαση σ' αυτά ή δεν τα έχει πλέον στην κατοχή του.».

[6] Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ (νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων –EDPB) για την Γνωστοποίηση παραβίασης προσωπικών δεδομένων:«Παραβίαση διαθεσιμότητας» – όταν υπάρχει τυχαία ή μη εξουσιοδοτημένη απώλεια πρόσβασης σε δεδομένα προσωπικού χαρακτήρα ή τυχαία ή μη εξουσιοδοτημένη καταστροφή δεδομένων προσωπικού χαρακτήρα.».

«Παρότι το εάν έχει διαπραχθεί παραβίαση της εμπιστευτικότητας ή της ακεραιότητας είναι σχετικά σαφές, το εάν έχει διαπραχθεί παραβίαση της διαθεσιμότητας ενδέχεται να είναι λιγότερο προφανές. Μια παραβίαση θα θεωρείται πάντα ότι συνιστά παραβίαση της διαθεσιμότητας όταν υπάρχει οριστική απώλεια ή καταστροφή δεδομένων προσωπικού χαρακτήρα.».

4.3. Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή

Βάσει του άρθρου 33 του Κανονισμού, δεν υπέβαλε τη σχετική γνωστοποίηση στο Γραφείο μου, εντός εβδομήντα δύο (72) ωρών από τη στιγμή που έλαβε γνώση του περιστατικού.

Σύμφωνα με τις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ *(νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων –EDPB)* για την Γνωστοποίηση παραβίασης προσωπικών δεδομένων *("Guidelines on Personal data breach notification under Regulation 2016/679 WP 250 rev. 1)*, ημερομηνίας 06.02.2018, **η μη γνωστοποίηση μιας παραβίασης θα μπορούσε να υποδεικνύει είτε την απουσία υφιστάμενων μέτρων ασφάλειας είτε την ανεπάρκεια των υφιστάμενων μέτρων ασφάλειας.**

4.4. Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

Βάσει του άρθρου 15 του Κανονισμού:

Η μη λήψη των δεόντων οργανωτικών και/ή τεχνικών μέτρων ασφάλειας, σύμφωνα με τα οριζόμενα στο άρθρο 32 του Κανονισμού, συνετέλεσε σε περιστατικό παραβίασης προσωπικών δεδομένων, σύμφωνα με τις διατάξεις του άρθρου 4(12) του Κανονισμού και σε μη ικανοποίηση του δικαιώματος πρόσβασης του παραπονούμενου στο ασφαλιστήριο συμβόλαιο του (άρθρο 15 του Κανονισμού).

Να σημειωθεί ότι, όπως ορίζουν οι Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ για την Γνωστοποίηση παραβίασης προσωπικών δεδομένων, **μια παραβίαση μπορεί δυνητικά να έχει διάφορες σημαντικές δυσμενείς συνέπειες στα πρόσωπα, οι οποίες μπορούν να οδηγήσουν σε σωματική, υλική ή ηθική βλάβη. Αυτή η βλάβη μπορεί να περιλαμβάνει απώλεια του ελέγχου επί των δεδομένων προσωπικού χαρακτήρα τους, περιορισμό των δικαιωμάτων τους, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας και οικονομική απώλεια. Μπορεί επίσης να περιλαμβάνει οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα γι' αυτά τα πρόσωπα[7].**

4.5. Οι ισχυρισμοί του Εξωτερικού Νομικού Συμβόλου της Καθ'ης την καταγγελία, όπως αναφέρονται στην επιστολή του με ημερομηνία 05.06.2020 απαντώνται ως κάτωθι:

Παρ.1 της Καθ'ης - συμβόλαιο οριοασφάλισης

(α) Ο ισχυρισμός της Καθ'ης την καταγγελία ότι, δεν υπήρξε παραβίαση της ασφάλειας (άρθρα 4(12), 5(1)(στ) και 32 του Κανονισμού), είναι αβάσιμος αφού, σύμφωνα με την Ευρωπαϊκή Επιτροπή[8], παραβίαση δεδομένων επέρχεται όταν σημειώνεται συμβάν ασφαλείας σε σχέση με τα δεδομένα για τα οποία ευθύνεται μία εταιρεία ή ένας οργανισμός, το οποίο έχει ως αποτέλεσμα την παραβίαση του απορρήτου, της **διαθεσιμότητας** ή της ακεραιότητας.

Εάν αυτό συμβεί, και είναι πιθανό η παραβίαση να θέτει σε κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικού προσώπου, η εταιρεία ή ο οργανισμός πρέπει να ειδοποιήσει την εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 72 ωρών αφού αντιληφθεί την παραβίαση. Ως

[7] Βλ. επίσης αιτιολογικές σκέψεις 85 και 75 (του Κανονισμού 679/2016).

[8] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_el

οργανισμός, είναι ζωτικής σημασίας να εφαρμόζετε τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αποφυγή ενδεχόμενων παραβιάσεων δεδομένων.

Επιπρόσθετα, Η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα αναφέρει ότι[9]:

«Παραδοσιακά, ο όρος ασφάλεια πληροφορίας/δεδομένων (information/data security), χρησιμοποιείται για να περιγράψει τη μεθοδολογία, καθώς και τις μεθόδους και τεχνικές που ακολουθούνται προκειμένου να επιτευχθούν οι εξής στόχοι:

- **Εμπιστευτικότητα** (confidentiality): Τα δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- **Ακεραιότητα** (integrity): Τα δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.
- **Διαθεσιμότητα (availability): Τα δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.**

Πλήγμα σε οποιοδήποτε από τα ανωτέρω –από τυχαία ή εσκεμμένη ενέργεια– συνιστά, γενικά, **περιστατικό ασφάλειας.».**

Στην προκειμένη περίπτωση, σημειώθηκε συμβάν ασφάλειας σε σχέση με το Συμβόλαιο που αφορά στον παραπονούμενο, για το οποίο ευθύνεται η Τράπεζα, ως ο υπεύθυνος επεξεργασίας του συστήματος αρχειοθέτησης της, το οποίο είχε ως αποτέλεσμα την παραβίαση της διαθεσιμότητας του συμβολαίου και κατ' επέκταση την αδυναμία ικανοποίησης του δικαιώματος πρόσβασης του παραπονούμενου σε προσωπικό δεδομένο που τον αφορά (συμβόλαιο).

(β) Ο ισχυρισμός της Καθ'ης την καταγγελία ότι, δεν υπήρξε οποιαδήποτε απώλεια προσωπικών δεδομένων του κ. είναι αβάσιμος και έγκειται πιθανόν στο γεγονός ότι, εσφαλμένα θεωρεί ότι, το συμβόλαιο πρέπει να περιέχει/αναγράφει προσωπικά δεδομένα που αφορούν αποκλειστικά στην υγεία του κ. ούτως ώστε αυτό να αποτελεί «δεδομένο προσωπικού χαρακτήρα».

Βάσει της αιτιολογικής σκέψης 26 του Κανονισμού που συμπληρώνει το άρθρο 4(1) του Κανονισμού, το οποίο αφορά στον ορισμό «δεδομένα προσωπικού χαρακτήρα»:

«Οι αρχές της προστασίας δεδομένων θα πρέπει να εφαρμόζονται σε κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο. Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου. Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας.....».

[9] https://www.dpa.gr/portal/page?_pageid=33,211421&_dad=portal&_schema=PORTAL

Από τα ανωτέρω συνάγεται ότι, ΟΠΟΙΑΔΗΠΟΤΕ ΠΛΗΡΟΦΟΡΙΑ αναφέρεται σε φυσικό πρόσωπο εν ζωή, αποτελεί «δεδομένο προσωπικού χαρακτήρα». Ως εκ τούτου, τα προσωπικά δεδομένα που περιλαμβάνονται στο ασφαλιστήριο συμβόλαιο του παραπονούμενου συνιστούν **«δεδομένα προσωπικού χαρακτήρα».**

(γ) Συνεπώς, ο ισχυρισμός της Καθ'ης την καταγγελία ότι, το επίμαχο συμβόλαιο οριοασφάλισης δεν περιέχει δεδομένα που αφορούσαν στην υγεία του παραπονούμενου, δεν αναιρεί την υποχρέωση ότι πρέπει να τηρούνται κάθε φορά τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα ασφάλειας, δεδομένου ότι το εν λόγω συμβόλαιο αφορά στον παραπονούμενο και συνεπώς είναι προσωπικό δεδομένο του.

(δ) Ο ισχυρισμός της Καθ'ης την καταγγελία ότι, η Τράπεζα είναι σε συμμόρφωση με το άρθρο 15 του Κανονισμού, που αφορά στο δικαίωμα πρόσβασης, λόγω του ότι, με τις βεβαιώσεις ασφαλίστρων, η Τράπεζα του κοινοποιούσε σε ετήσια βάση, από το 2012, στοιχεία που αφορούν στην ασφαλιστική σύμβαση του, είναι απορριπτέος ως αβάσιμος και δεν ευσταθεί.

Για το σκοπό αυτό, επισυνάφθηκε, ως Παράρτημα 3, αντίγραφο δείγματος του εντύπου «Βεβαίωση Πληρωμής Ασφαλίστρων Ομαδικής Ασφαλιστικής Σύμβασης Ζωής», στο οποίο αναγράφεται ότι: *«Το Πιστοποιητικό αυτό εκδίδεται με μοναδικό σκοπό την κατάθεση του στο Τμήμα Εσωτερικών Προσόδων, εάν ζητηθεί, και δεν έχει οποιαδήποτε άλλη αξία ή σκοπό, και ούτε αποτελεί εγγύηση ότι το ασφάλιστρο θα φοροαπαλλαχθεί.»:*

Ο παραπονούμενος λάμβανε μεν ετήσια ΠΛΗΡΟΦΟΡΗΣΗ/ΕΝΗΜΕΡΩΣΗ για το ασφαλιστικό συμβόλαιο του με αριθμό Μ-056482, όμως το ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗΣ ΠΟΥ ΑΣΚΗΣΕ ΣΤΟ ΙΔΙΟ ΤΟ ΑΣΦΑΛΙΣΤΙΚΟ ΣΥΜΒΟΛΑΙΟ, ΔΕΝ ΙΚΑΝΟΠΟΙΗΘΗΚΕ ΜΕΧΡΙ ΣΗΜΕΡΑ, λόγω του ότι, όπως παραδέχτηκε η Καθ'ης την καταγγελία, δεν κατέστει δυνατό να ανευρεθεί.

Από τα ανωτέρω, συνάγεται ότι, η Τράπεζα ΔΕΝ ήταν σε θέση να ικανοποιήσει το δικαίωμα πρόσβασης του παραπονούμενου, στερώντας του τη δυνατότητα να ελέγξει τη νομιμότητα της επεξεργασίας και κατά συνέπεια παραβίασε, εκ πρώτης όψεως, τις διατάξεις του άρθρου 15 του Κανονισμού.

Η Τράπεζα παραδέχτηκε την μη ανεύρεση του επίμαχου Συμβολαίου στις ακόλουθες επιστολές της:

- **Επιστολή με ημερομηνία 20 Φεβρουαρίου 2020 της Δρ. Περιφερειακής Διευθύντριας Λευκωσίας της Τράπεζας:**

«Παρά τη σχετική έρευνα δεν κατέστη δυνατός ο εντοπισμός του συμβολαίου του πελάτη στο σχετικό αρχειοθετημένο κουτί φύλαξης.».

«Η Τράπεζα έχει επιθεωρήσει και το φυσικό φάκελο του πελάτη όπου υπάρχουν όλες οι πρωτότυπες συμφωνίες/συμβόλαια και επικοινωνία με τον πελάτη συμπεριλαμβανομένου και έγγραφα ταυτοποιήσεις του όπου και πάλι δεν κατέστη δυνατό να εντοπιστεί το συγκριμένο συμβόλαιο.».

- **Επιστολή με ημερομηνία 05 Ιουνίου 2020 (παράγραφος 1 – Συμβόλαιο Οριοασφάλισης):**

«Εκ παραδρομής, φαίνεται να μην αρχειοθετήθηκε αντίγραφο στο φάκελο του πελάτη το 2000, με αποτέλεσμα ο φάκελος του, ο οποίος βρίσκεται στην κατοχή της Τράπεζας, να μην περιέχει το συγκεκριμένο αντίγραφο.».

«Τα αρχεία εκείνου του καταστήματος έχουν φυλαχθεί σε συγκεκριμένες αποθήκες και μέχρι σήμερα δεν κατέστη δυνατός ο εντοπισμός του συγκεκριμένου εγγράφου.».

«Η δυσκολία στην ανεύρεση του οφείλεται στο γεγονός ότι,....».

- **Επιστολή με ημερομηνία 05 Ιουνίου 2020 (παράγραφος 5 – Ελαφρυντικά–Καταληκτικά Σχόλια):**

«Λαμβάνοντας υπόψη το κλείσιμο των καταστημάτων, την συγχώνευση της Τράπεζας με την πρώην Λαϊκή Τράπεζα και των αλλαγών των αποθηκευτικών χώρων, δεν είναι σίγουρο κατά πόσο το σχετικό έγγραφο έχει χαθεί ή απλά έχει τοποθετηθεί σε λάθος χώρο με βάση τις διαδικασίες αρχειοθέτησης και ως εκ τούτου δεν κατέστη δυνατή μέχρι σήμερα η πρόσβαση στο συμβόλαιο οριοασφάλισης.»

Παρ.1 της Καθ'ης - συμβόλαιο οριοασφάλισης και Παρ. 5 της Καθ'ης - Ελαφρυντικά-Καταληκτικά σχόλια

Η Καθ'ης την καταγγελία δεν κατόρθωσε να μου αποδείξει ότι, πράγματι το επίμαχο συμβόλαιο βρίσκεται εντός των εγκαταστάσεων της Τράπεζας, αφού μέχρι σήμερα δεν ανευρέθηκε, στοιχείο που αποδεικνύει την μη ύπαρξη ορθής αρχειοθέτησης εγγράφων, συνέπεια της λήψης ανεπαρκών μέτρων ασφάλειας, υποχρέωση που υπέχει η ίδια ως υπεύθυνος επεξεργασίας του συστήματος αρχειοθέτησής της (άρθρο 32 του Κανονισμού).

Η Τράπεζα όφειλε, βάσει των διατάξεων των άρθρων 5(1)(στ) και 32 του Κανονισμού, να είχε υιοθετήσει/εφαρμόσει συγκεκριμένες διαδικασίες για την ορθή οργάνωση/αρχειοθέτηση/ταξινόμηση τόσο του ηλεκτρονικού όσο και του φυσικού συστήματος αρχειοθέτησής της.

Επιπροσθέτως, όφειλε να έχει διαδικασίες για την εκπόνηση προγραμματισμένων έλεγχων (εσωτερικών και/ή εξωτερικών, σε ετήσια βάση), όπου να αποτυπώνεται και να ελέγχεται η τήρηση των μέτρων ασφαλείας και η αποτελεσματικότητά τους. Αποτέλεσμα των ελέγχων, θα μπορούσε να ήταν η τροποποίηση της υφιστάμενης πολιτικής ασφαλείας, κάποιων μέτρων ασφαλείας ή η προσθήκη νέων.

Παρ.3 της Καθ'ης - σχέση με τους πελάτες

Η σχέση που έχει η Τράπεζα με τους πελάτες της, όπως καταγράφεται στην παράγραφο 3 της επιστολής της Καθ'ης την καταγγελία με ημερομηνία 5 Ιουνίου 2020 και η πρόταση της Τράπεζας που έκανε στον παραπονούμενο για επιστροφή όλων των ασφαλίστρων, δεν εμπίπτουν στις αρμοδιότητες μου και ως εκ τούτου δεν εξετάζονται και δεν αξιολογούνται. Επιπλέον, είναι πληροφορίες που δεν σχετίζονται με την ουσία εξέτασης της παρούσας υπόθεσης, **που είναι η λήψη αντιγράφου του ασφαλιστικού συμβολαίου του παραπονούμενου με αριθμό Μ-056482 κατά την άσκηση του δικαιώματος πρόσβασης του στα προσωπικά δεδομένα που τον αφορούν (άρθρο 15 του Κανονισμού)**.

Εν πάση περιπτώσει, είναι αυτονόητο ότι, η πρόταση της Τράπεζας για επιστροφή όλων των ασφαλίστρων στον κ. οδηγεί σε αναίρεση της άσκησης του δικαιώματος πρόσβασης από την πλευρά του υποκειμένου των δεδομένων και αδυναμία ελέγχου της νομιμότητας της επεξεργασίας που διενεργεί η Τράπεζα. Η αδυναμία ικανοποίησης του δικαιώματος πρόσβασης, οφείλεται σε έλλειψη που αφορά στον τρόπο λειτουργίας του αρχείου της Τράπεζας και συνιστά και έλλειψη των μέτρων επιμέλειας τα οποία όφειλε να τηρήσει ως υπεύθυνος επεξεργασίας ώστε να αποφευχθεί το λάθος.

Παρ. 5 της Καθ'ης - Ελαφρυντικά-Καταληκτικά σχόλια

Ο ισχυρισμός της Καθ'ης την καταγγελία ότι, *«μέχρι σήμερα δεν έχει επιβληθεί στην Τράπεζα πρόστιμο από την Επίτροπο σε σχέση με θέματα συμμόρφωσης της Τράπεζας με τον Κανονισμό»* δεν ευσταθεί αφού, μέχρι σήμερα έχουν επιβληθεί τέσσερις διοικητικές κυρώσεις (Αρ. Φακέλων: Α/Π

8/2006, Α/Π 48/2010, Α/Π 61/2014, Α/Π 67/2017 και Α/Π 56/2017), οι οποίες όμως δεν θα προσμετρηθούν κατά την επιμέτρηση της ποινής, αφού δεν αφορούν σε παρόμοιας φύσεως παραβίαση.

5. Κυρώσεις

5.1.1. Όπως ορίζεται στις διατάξεις του άρθρου 83(5) του Κανονισμού, παράβαση των διατάξεων των **άρθρων 5 και 15**, επισύρει, «σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 20 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο».

5.1.2. Όπως ορίζεται στις διατάξεις του άρθρου 83(4) του Κανονισμού, παράβαση των διατάξεων των **άρθρων 32 και 33**, επισύρει, «σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 10 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο».

5.1.3. Παρατίθεται αυτούσια η παράγραφος 2 του άρθρου 83 του Κανονισμού:

«2. Τα διοικητικά πρόστιμα, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, επιβάλλονται επιπρόσθετα ή αντί των μέτρων που αναφέρονται στο άρθρο 58 παράγραφος 2 στοιχεία α) έως η) και στο άρθρο 58 παράγραφος 2 στοιχείο ι). Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη τα ακόλουθα:

α) η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβάνοντας υπόψη τη φύση, την έκταση ή το σκοπό της σχετικής επεξεργασίας, καθώς και τον αριθμό των υποκειμένων των δεδομένων που έθιξε η παράβαση και το βαθμό ζημίας που υπέστησαν,

β) ο δόλος ή η αμέλεια που προκάλεσε την παράβαση,

γ) οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων,

δ) ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν δυνάμει των άρθρων 25 και 32,

ε) τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, στ) ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της,

ζ) οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση,

η) ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, ειδικότερα εάν και κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση,

θ) σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται στο άρθρο 58 παράγραφος 2 κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα,

ι) η τήρηση εγκεκριμένων κωδίκων δεοντολογίας σύμφωνα με το άρθρο 40 ή εγκεκριμένων μηχανισμών πιστοποίησης σύμφωνα με το άρθρο 42 και

ια) κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.».

6. Επιμέτρηση ποινής

Λαμβάνοντας υπόψη τις διατάξεις του άρθρου 83 του Κανονισμού, που αφορά στους Γενικούς Όρους επιβολής διοικητικών προστίμων, κατά την επιμέτρηση του διοικητικού προστίμου έλαβα υπόψην μου τους πιο κάτω μετριαστικούς (α – ζ) και επιβαρυντικούς (η – ι) παράγοντες:

(α) Τη φύση της παράβασης: Η παράβαση αφορά στη συμβατική σχέση της Τράπεζας με το υποκείμενο των δεδομένων.

(β) Τον αριθμό των υποκειμένων των δεδομένων που έθιξε η παράβαση: επηρεάζεται ένα πρόσωπο.

(γ) Τις κατηγορίες προσωπικών δεδομένων που επηρεάζει η παράβαση: Δεδομένου ότι, μέχρι σήμερα το συμβόλαιο οριοασφάλισης δεν ανευρέθηκε, θεωρώ ότι, τα προσωπικά δεδομένα που περιλαμβάνονταν σε αυτό, είναι κατ' ελάχιστον, το ονοματεπώνυμο, ο αριθμός συμβολαίου και ο αριθμός ταυτότητας, ως το πλέον διαδεδομένο στοιχείο αναγνώρισης/ταυτοποίησης

(δ) Το γεγονός ότι η Καθ'ής την καταγγελία προέβηκε σε ενέργειες για να μετριάσει τη ζημία που υπέστηκε το υποκείμενο των δεδομένων:

Η Καθ'ης την καταγγελία έκανε πρόταση στον κ. για επιστροφή όλων των ασφαλίστρων συμπεριλαμβανομένων και των τόκων με την ενυπόγραφη εντολή ακύρωσης της ασφάλισης.

(ε) Το γεγονός ότι η Καθ'ής την καταγγελία συνεργάστηκε επαρκώς με το Γραφείο μου για την επανόρθωση της παράβασης.

(στ) Το γεγονός ότι, η Καθ'ής την καταγγελία με πληροφόρησε ότι, τουλάχιστον εκ των υστέρων, έχει λάβει επιπρόσθετα μέτρα που θα συνέτειναν στην ενίσχυση/βελτίωση της ασφάλειας και προστασίας των ασφαλιστήριων συμβολαίων των πελατών-ασφαλιζόμενης της.

(ζ) Ο υπεύθυνος επεξεργασίας δεν αποκόμισε οικονομικό όφελος, ούτε προκάλεσε υλική ζημία στο υποκείμενο των δεδομένων.

(η) Τη διάρκεια της παράβασης: Δεν μπορεί να καθοριστεί επακριβώς, καθότι τα στοιχεία που λήφθηκαν υπόψιν μου, προέκυψαν στα πλαίσια της διερεύνησης.

(θ) Το γεγονός ότι ενημερώθηκα για την παράνομη επεξεργασία κατόπιν καταγγελίας στο Γραφείο μου και όχι απευθείας από την Καθ'ης την καταγγελία.

(ι) Το γεγονός ότι πρόκειται περί παραβιάσεις λόγω επεξεργασίας προσωπικών δεδομένων (άρθρα 5(1)(στ), 5(2), 32 και 33), οι οποίες κρίνονται ως μεγαλύτερης βαρύτητας και διάρκειας αλλά επίσης περί μη ικανοποίησης του δικαιώματος πρόσβασης ενός υποκειμένου.

7. Κατάληξη

Υπό το φώς των ανωτέρω και με βάση τις εξουσίες που μου απονέμουν οι διατάξεις του άρθρου 58(2)(θ) του Κανονισμού, έχω την άποψη ότι, εκ πρώτης όψεως, η μη ανεύρεση, μέχρι σήμερα, του επίμαχου ασφαλιστήριου οριοασφάλισης του κ. παραβιάζει τις διατάξεις των άρθρων 5(1)(στ), 5(2), 15, 32 και 33 του Κανονισμού.

Ως εκ τούτου, ΑΠΟΦΑΣΙΣΑ όπως:

Ως εκ τούτου, αποφάσισα όπως επιβάλω στην Καθ'ης την καταγγελία, Τράπεζα Κύπρου Δημόσια Εταιρεία Λτδ, υπό την ιδιότητα της ως υπεύθυνου επεξεργασίας συστήματος αρχειοθέτησης, τη χρηματική ποινή των €15,000 (δεκαπέντε χιλιάδων ευρώ) για τη διάπραξη παράβασης της υποχρέωσης της εκ των άρθρων 5(1)(στ), 5(2), 15, 32 και 33 του Κανονισμού.

Ειρήνη Λοϊζίδου Νικολαΐδου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα