ΤΥΠΟΠΟΙΗΜΕΝΟΙ ΟΡΟΙ "AXIA E- SHAREHOLDERS MEETING SERVICE"

ΠΑΡΑΡΤΗΜΑ ΙΙΙ ΟΡΟΙ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΤΜΗΜΑ Ι

Ρήτρα 1

Σκοπός και πεδίο εφαρμογής

α) Οι παρούσες τυποποιημένες συμβατικές ρήτρες (στο εξής: ρήτρες) έχουν ως σκοπό να διασφαλίζουν τη συμμόρφωση με το άρθρο 28 παράγραφοι 3 και 4 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός Προστασίας Δεδομένων).

β) Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία που απαριθμούνται στο προσάρτημα Α συμφώνησαν τις παρούσες ρήτρες προκειμένου να διασφαλίζεται η συμμόρφωση με το άρθρο 28 παράγραφοι 3 και 4 του κανονισμού (ΕΕ) 2016/679.

γ) Οι παρούσες ρήτρες εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα όπως καθορίζεται στο προσάρτημα Β.

δ) Τα προσαρτήματα Α έως Γ είναι αναπόσπαστο μέρος των ρητρών.

ε) Οι παρούσες ρήτρες δεν θίγουν τις υποχρεώσεις στις οποίες υπόκειται ο υπεύθυνος επεξεργασίας δυνάμει του κανονισμού (ΕΕ) 2016/679.

στ) Οι παρούσες ρήτρες δεν διασφαλίζουν από μόνες τους τη συμμόρφωση με τις υποχρεώσεις που σχετίζονται με τις διεθνείς διαβιβάσεις σύμφωνα με το κεφάλαιο V του κανονισμού (ΕΕ) 2016/679.

Ρήτρα 2

Αμετάβλητος χαρακτήρας των ρητρών

α) Τα μέρη δεσμεύονται να μην τροποποιούν τις ρήτρες παρά μόνο για να προσθέσουν ή να επικαιροποιήσουν πληροφορίες στα προσαρτήματα.

β) Η δέσμευση αυτή δεν εμποδίζει τα μέρη να ενσωματώνουν τις τυποποιημένες συμβατικές ρήτρες που ορίζονται στις παρούσες ρήτρες σε ευρύτερη σύμβαση ούτε να προσθέτουν άλλες ρήτρες ή πρόσθετες εγγυήσεις, υπό τον όρο ότι αυτές δεν αντιφάσκουν, άμεσα ή έμμεσα, προς τις ρήτρες ούτε θίγουν τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων.

Ρήτρα 3

Ερμηνεία

α) Όπου στις παρούσες ρήτρες χρησιμοποιούνται όροι που ορίζονται στον κανονισμό (ΕΕ) 2016/679, οι εν λόγω όροι έχουν την ίδια έννοια με αυτή που έχουν στον οικείο κανονισμό.

β) Η ανάγνωση και ερμηνεία των παρουσών ρητρών πραγματοποιούνται υπό το πρίσμα των διατάξεων του κανονισμού (ΕΕ) 2016/679.

γ) Οι παρούσες ρήτρες δεν ερμηνεύονται με τρόπο που αντιβαίνει προς τα δικαιώματα και τις υποχρεώσεις που προβλέπονται στον κανονισμό (ΕΕ) 2016/679 ή με τρόπο που θίγει τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων.

Ρήτρα 4

Ιεραρχία

Σε περίπτωση αντίφασης μεταξύ των παρουσών ρητρών και των διατάξεων συναφών συμφωνιών μεταξύ των μερών οι οποίες ισχύουν κατά τον χρόνο που συμφωνούνται ή συνάπτονται οι παρούσες ρήτρες, οι παρούσες ρήτρες υπερισχύουν.

Ρήτρα 5

Προαιρετική Ρήτρα σύνδεσης

α) Οποιαδήποτε οντότητα που δεν είναι συμβαλλόμενο μέρος των παρουσών ρητρών μπορεί, με τη συγκατάθεση όλων των συμβαλλόμενων μερών, να προσχωρήσει στις παρούσες ρήτρες ανά πάσα στιγμή, ως υπεύθυνος επεξεργασίας ή ως εκτελών την επεξεργασία, συμπληρώνοντας τα προσαρτήματα και υπογράφοντας το προσάρτημα Α.

β) Αφού συμπληρωθούν και υπογραφούν τα προσαρτήματα του στοιχείου α), η προσχωρούσα οντότητα λογίζεται ως συμβαλλόμενο μέρος των παρουσών ρητρών και έχει τα δικαιώματα και τις υποχρεώσεις υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, σύμφωνα με τον χαρακτηρισμό της στο προσάρτημα Α.

γ) Η προσχωρούσα οντότητα δεν έχει δικαιώματα ή υποχρεώσεις που απορρέουν από τις παρούσες ρήτρες όσον αφορά το διάστημα πριν καταστεί συμβαλλόμενο μέρος.

ΤΜΗΜΑ ΙΙ

ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΣΥΜΒΑΛΛΟΜΕΝΩΝ ΜΕΡΩΝ

Ρήτρα 6

Περιγραφή της επεξεργασίας

Οι λεπτομέρειες των πράξεων επεξεργασίας, ιδίως οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα και οι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας, καθορίζονται στο προσάρτημα Β.

Ρήτρα 7

Υποχρεώσεις των συμβαλλόμενων μερών

7.1. **Εντολές**

α) Ο εκτελών την επεξεργασία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο βάσει του δικαίου της Ένωσης ή του δικαίου του κράτους μέλους στο οποίο υπόκειται ο εκτελών

την επεξεργασία. Στην περίπτωση αυτή, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για την εν λόγω νομική απαίτηση πριν από την επεξεργασία, εκτός εάν το εν λόγω δίκαιο απαγορεύει αυτού του είδους την ενημέρωση για σοβαρούς λόγους δημόσιου συμφέροντος. Ο υπεύθυνος επεξεργασίας μπορεί επίσης να δίνει μεταγενέστερες εντολές καθ' όλη τη διάρκεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Οι εν λόγω εντολές είναι πάντοτε έγγραφες.

β) Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας, εάν, κατά την άποψη του εκτελούντος της επεξεργασία, κάποια εντολή του υπευθύνου επεξεργασίας παραβιάζει τον κανονισμό (ΕΕ) 2016/679 ή ενωσιακές ή εθνικές διατάξεις περί προστασίας δεδομένων.

7.2. **Περιορισμός του σκοπού**

Ο εκτελών την επεξεργασία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο για τον συγκεκριμένο σκοπό ή σκοπούς της επεξεργασίας που ορίζονται στο προσάρτημα Β, εκτός αν λάβει περαιτέρω εντολές από τον υπεύθυνο επεξεργασίας.

7.3. **Διάρκεια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα**

Η επεξεργασία από τον εκτελούντα την επεξεργασία πραγματοποιείται μόνο για το χρονικό διάστημα που καθορίζεται στο προσάρτημα Β.

7.4. **Ασφάλεια της επεξεργασίας**

α) Ο εκτελών την επεξεργασία εφαρμόζει τουλάχιστον τα τεχνικά και οργανωτικά μέτρα που καθορίζονται στο προσάρτημα Γ προκειμένου να διασφαλίζει την ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Στο πλαίσιο αυτό συμπεριλαμβάνεται η προστασία των δεδομένων από παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων (στο εξής: παραβίαση δεδομένων προσωπικού χαρακτήρα). Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, τα συμβαλλόμενα μέρη λαμβάνουν δεόντως υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους που συντρέχουν για τα υποκείμενα των δεδομένων.

β) Ο εκτελών την επεξεργασία παρέχει σε μέλη του προσωπικού του πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία μόνο στο μέτρο που είναι απολύτως αναγκαίο για την εκτέλεση, τη διαχείριση και την παρακολούθηση της σύμβασης. Ο εκτελών την επεξεργασία διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα λαμβανόμενα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή υπόκεινται σε δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας.

7.5. **Ευαίσθητα δεδομένα**

Αν η επεξεργασία περιλαμβάνει δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά δεδομένα ή βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την

υγεία ή τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό φυσικού προσώπου, ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα (στο εξής: ευαίσθητα δεδομένα), ο εκτελών την επεξεργασία εφαρμόζει ειδικούς περιορισμούς και/ή πρόσθετες εγγυήσεις.

7.6. **Τεκμηρίωση και συμμόρφωση**

α) Τα συμβαλλόμενα μέρη είναι σε θέση να αποδείξουν τη συμμόρφωσή τους με τις παρούσες ρήτρες.

β) Ο εκτελών την επεξεργασία ανταποκρίνεται άμεσα και επαρκώς σε όλα τα αιτήματα πληροφοριών του υπευθύνου επεξεργασίας σχετικά με την επεξεργασία δεδομένων σύμφωνα με τις παρούσες ρήτρες.

γ) Ο εκτελών την επεξεργασία θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που καθορίζονται στις παρούσες ρήτρες και απορρέουν απευθείας από τον κανονισμό (ΕΕ) 2016/679. Επιπλέον, κατόπιν αιτήματος του υπευθύνου επεξεργασίας, ο εκτελών την επεξεργασία επιτρέπει και διευκολύνει ελέγχους των δραστηριοτήτων επεξεργασίας που καλύπτονται από τις παρούσες ρήτρες, σε εύλογα τακτά χρονικά διαστήματα ή αν υπάρχουν ενδείξεις μη συμμόρφωσης. Όταν αποφασίζει για επανεξέταση ή έλεγχο, ο υπεύθυνος επεξεργασίας μπορεί να λαμβάνει υπόψη σχετικές πιστοποιήσεις του εκτελούντος την επεξεργασία.

δ) Ο υπεύθυνος επεξεργασίας μπορεί να επιλέγει να διενεργήσει τον έλεγχο ο ίδιος ή να τον αναθέσει σε ανεξάρτητο ελεγκτή. Οι έλεγχοι είναι δυνατόν να περιλαμβάνουν και επιθεωρήσεις στους χώρους ή τις φυσικές εγκαταστάσεις του εκτελούντος την επεξεργασία, ενώ, όταν ενδείκνυται, διενεργούνται έπειτα από εύλογη προθεσμία προειδοποίησης.

ε) Τα συμβαλλόμενα μέρη θέτουν τις πληροφορίες που αναφέρονται στην παρούσα ρήτρα, συμπεριλαμβανομένων των αποτελεσμάτων τυχόν ελέγχων, στη διάθεση της/των αρμόδιας/-ων εποπτικής/-ών αρχής/-ών, κατόπιν σχετικού αιτήματός της/τους.

7.7. **Χρήση υπεργολάβων επεξεργασίας**

α) Ο εκτελών την επεξεργασία έχει τη γενική άδεια του υπευθύνου επεξεργασίας για την πρόσληψη υπεργολάβων επεξεργασίας από κατάλογο που έχει συμφωνηθεί. Ο εκτελών την επεξεργασία ενημερώνει ειδικά και εγγράφως τον υπεύθυνο επεξεργασίας για κάθε τυχόν σκοπούμενη αλλαγή στον εν λόγω κατάλογο η οποία αφορά την προσθήκη ή την αντικατάσταση υπεργολάβων επεξεργασίας τουλάχιστον πέντε (5) ημέρες πριν, παρέχοντας στον υπεύθυνο επεξεργασίας επαρκή χρόνο ώστε να μπορεί να εναντιωθεί στην εν λόγω αλλαγή πριν από την πρόσληψη του σχετικού υπεργολάβου ή των σχετικών υπεργολάβων επεξεργασίας. Ο εκτελών την επεξεργασία παρέχει στον υπεύθυνο επεξεργασίας τις πληροφορίες που απαιτούνται ώστε ο υπεύθυνος επεξεργασίας να είναι σε θέση να ασκήσει το δικαίωμα εναντίωσης.

β) Όταν ο εκτελών την επεξεργασία προσλαμβάνει υπεργολάβο επεξεργασίας για την εκτέλεση συγκεκριμένων δραστηριοτήτων επεξεργασίας (για λογαριασμό του υπευθύνου επεξεργασίας), το πράττει μέσω σύμβασης η οποία επιβάλλει στον υπεργολάβο επεξεργασίας, στην ουσία, τις ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων με αυτές που επιβάλλονται στον

εκτελούντα την επεξεργασία σύμφωνα με τις παρούσες ρήτρες. Ο εκτελών την επεξεργασία διασφαλίζει ότι ο υπεργολάβος επεξεργασίας συμμορφώνεται με τις υποχρεώσεις στις οποίες υπόκειται ο εκτελών την επεξεργασία σύμφωνα με τις παρούσες ρήτρες και τον κανονισμό (ΕΕ) 2016/679.

γ) Κατόπιν αιτήματος του υπευθύνου επεξεργασίας, ο εκτελών την επεξεργασία παρέχει στον υπεύθυνο επεξεργασίας αντίγραφο της συμφωνίας με τον υπεργολάβο και κάθε τυχόν μεταγενέστερης πράξης τροποποίησής της. Στον βαθμό που είναι αναγκαίο για την προστασία επαγγελματικών απορρήτων ή άλλων εμπιστευτικών πληροφοριών, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα, ο εκτελών την επεξεργασία μπορεί να απαλείψει τις εμπιστευτικές πληροφορίες από το κείμενο της συμφωνίας πριν από την κοινοποίηση του αντιγράφου.

δ) Ο εκτελών την επεξεργασία παραμένει πλήρως υπεύθυνος έναντι του υπευθύνου επεξεργασίας για την εκπλήρωση των υποχρεώσεων του υπεργολάβου επεξεργασίας σύμφωνα με τη σύμβασή του με τον εκτελούντα την επεξεργασία. Ο εκτελών την επεξεργασία γνωστοποιεί στον υπεύθυνο επεξεργασίας κάθε περίπτωση μη εκπλήρωσης των συμβατικών υποχρεώσεων του υπεργολάβου επεξεργασίας.

ε) Ο εκτελών την επεξεργασία συμφωνεί με τον υπεργολάβο επεξεργασίας ρήτρα δικαιούχου τρίτου, βάσει της οποίας —σε περίπτωση που ο εκτελών την επεξεργασία έπαυσε να υφίσταται από πραγματική ή νομική άποψη ή κατέστη αφερέγγυος— ο υπεύθυνος επεξεργασίας έχει το δικαίωμα να καταγγείλει τη σύμβαση με τον υπεργολάβο επεξεργασίας και να του δώσει εντολή να διαγράψει ή να επιστρέψει τα δεδομένα προσωπικού χαρακτήρα.

7.8. **Διεθνείς διαβιβάσεις**

α) Κάθε διαβίβαση δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό από τον εκτελούντα την επεξεργασία πραγματοποιείται μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας ή προκειμένου να εκπληρωθεί ειδική απαίτηση του δικαίου της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο εκτελών την επεξεργασία και εκτελείται σύμφωνα με τους όρους του κεφαλαίου V του κανονισμού (ΕΕ) 2016/679.

β) Ο υπεύθυνος επεξεργασίας συμφωνεί ότι στις περιπτώσεις που ο εκτελών την επεξεργασία προσλαμβάνει υπεργολάβο επεξεργασίας σύμφωνα με τη ρήτρα 7.7 για την εκτέλεση συγκεκριμένων δραστηριοτήτων επεξεργασίας (για λογαριασμό του υπευθύνου επεξεργασίας) και οι εν λόγω δραστηριότητες επεξεργασίας περιλαμβάνουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα κατά την έννοια του κεφαλαίου V του κανονισμού (ΕΕ) 2016/679, ο εκτελών την επεξεργασία και ο υπεργολάβος επεξεργασίας μπορούν να διασφαλίζουν τη συμμόρφωση με το κεφάλαιο V του κανονισμού (ΕΕ) 2016/679 μέσω της χρήσης τυποποιημένων συμβατικών ρητρών που έχει εκδώσει η Επιτροπή σύμφωνα με το άρθρο 46 παράγραφος 2 του κανονισμού (ΕΕ) 2016/679, υπό τον όρο ότι πληρούνται οι προϋποθέσεις για τη χρήση των εν λόγω τυποποιημένων συμβατικών ρητρών.

Ρήτρα 8

Συνδρομή στον υπεύθυνο επεξεργασίας

α) Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας για κάθε αίτημα που έχει λάβει από υποκείμενο των δεδομένων. Δεν απαντά ο ίδιος στο αίτημα, εκτός αν λάβει σχετική εξουσιοδότηση από τον υπεύθυνο επεξεργασίας.

β) Ο εκτελών την επεξεργασία βοηθά τον υπεύθυνο επεξεργασίας στην εκπλήρωση της υποχρέωσής του να απαντά στα αιτήματα των υποκειμένων των δεδομένων για άσκηση των δικαιωμάτων τους, λαμβανομένης υπόψη της φύσης της επεξεργασίας. Κατά την εκπλήρωση των υποχρεώσεών του σύμφωνα με τα στοιχεία α) και β), ο εκτελών την επεξεργασία συμμορφώνεται με τις εντολές του υπευθύνου επεξεργασίας.

γ) Επιπρόσθετα στην υποχρέωση του εκτελούντος την επεξεργασία να βοηθά τον υπεύθυνο επεξεργασίας σύμφωνα με τη ρήτρα 8 στοιχείο β), ο εκτελών την επεξεργασία βοηθά επίσης τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις παρακάτω υποχρεώσεις, λαμβανομένων υπόψη της φύσης της επεξεργασίας δεδομένων και των πληροφοριών που διαθέτει ο εκτελών την επεξεργασία:

1) την υποχρέωση να διενεργεί εκτίμηση του αντικτύπου των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα (εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων), όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

2) την υποχρέωση να ζητεί τη γνώμη της/των αρμόδιας/-ων εποπτικής/-ών αρχής/-ών πριν από την επεξεργασία, όταν μια εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας.

3) την υποχρέωση να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα είναι ακριβή και επικαιροποιημένα, ενημερώνοντας χωρίς καθυστέρηση τον υπεύθυνο επεξεργασίας σε περίπτωση που ο εκτελών την επεξεργασία αντιληφθεί ότι τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται είναι ανακριβή ή παρωχημένα.

4) τις υποχρεώσεις που προβλέπονται στο άρθρο 32 του κανονισμού (ΕΕ) 2016/679.

δ) Τα συμβαλλόμενα μέρη καθορίζουν στο προσάρτημα Γ τα κατάλληλα τεχνικά και οργανωτικά μέτρα με τα οποία ο εκτελών την επεξεργασία υποχρεούται να βοηθά τον υπεύθυνο επεξεργασίας για την εφαρμογή της παρούσας ρήτρας, καθώς και το πεδίο εφαρμογής και την έκταση της απαιτούμενης βοήθειας.

Ρήτρα 9

Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο εκτελών την επεξεργασία συνεργάζεται με τον υπεύθυνο επεξεργασίας και τον βοηθά να συμμορφωθεί προς τις υποχρεώσεις του που απορρέουν από τα άρθρα 33 και 34 του κανονισμού (ΕΕ) 2016/679,

ανάλογα με την περίπτωση, λαμβανομένων υπόψη της φύσης της επεξεργασίας και των πληροφοριών που διαθέτει ο εκτελών την επεξεργασία.

9.1. **Παραβίαση δεδομένων που αφορά δεδομένα που επεξεργάζεται ο υπεύθυνος επεξεργασίας**

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που αφορά δεδομένα που επεξεργάζεται ο υπεύθυνος επεξεργασίας, ο εκτελών την επεξεργασία βοηθά τον υπεύθυνο επεξεργασίας:

α) να γνωστοποιήσει την παραβίαση δεδομένων προσωπικού χαρακτήρα στην/στις αρμόδια/-ες εποπτική/-ές αρχή/-ές, αμελλητί από τη στιγμή που ο υπεύθυνος επεξεργασίας απέκτησε γνώση του γεγονότος, κατά περίπτωση/(εκτός αν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων)·

β) να συγκεντρώσει τις παρακάτω πληροφορίες, οι οποίες, σύμφωνα με το άρθρο 33 παράγραφος 3 του κανονισμού (ΕΕ) 2016/679, αναφέρονται στη γνωστοποίηση του υπευθύνου επεξεργασίας και πρέπει να περιλαμβάνουν κατ' ελάχιστο:

1) τη φύση των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα·

2) τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα·

3) τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Όταν και στον βαθμό που δεν είναι δυνατόν να παρασχεθούν όλες αυτές οι πληροφορίες ταυτόχρονα, στην αρχική γνωστοποίηση περιλαμβάνονται οι πληροφορίες που είναι διαθέσιμες τη δεδομένη στιγμή, ενώ πρόσθετες πληροφορίες παρέχονται σε μεταγενέστερο χρόνο και χωρίς αδικαιολόγητη καθυστέρηση μόλις καταστούν διαθέσιμες.

γ) να συμμορφωθεί, σύμφωνα με το άρθρο 34 του κανονισμού (ΕΕ) 2016/679 με την υποχρέωση να ανακοινώνει αμελλητί στο υποκείμενο των δεδομένων την παραβίαση δεδομένων προσωπικού χαρακτήρα, όταν αυτή ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

9.2. **Παραβίαση δεδομένων που αφορά δεδομένα που επεξεργάζεται ο εκτελών την επεξεργασία**

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που αφορά δεδομένα που επεξεργάζεται ο εκτελών την επεξεργασία, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση από τη στιγμή που αποκτά γνώση της παραβίασης. Η εν λόγω γνωστοποίηση περιλαμβάνει κατ' ελάχιστο:

α) περιγραφή της φύσης της παραβίασης (συμπεριλαμβανομένων, όπου είναι δυνατόν, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων και αρχείων δεδομένων)·

β) τα στοιχεία του σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες σχετικά με την παραβίαση των δεδομένων προσωπικού χαρακτήρα·

γ) τις ενδεχόμενες συνέπειες και τα ληφθέντα ή προτεινόμενα προς λήψη μέτρα για την αντιμετώπιση της παραβίασης, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Όταν και στον βαθμό που δεν είναι δυνατόν να παρασχεθούν όλες αυτές οι πληροφορίες ταυτόχρονα, στην αρχική γνωστοποίηση περιλαμβάνονται οι πληροφορίες που είναι διαθέσιμες τη δεδομένη στιγμή, ενώ πρόσθετες πληροφορίες παρέχονται σε μεταγενέστερο χρόνο και χωρίς αδικαιολόγητη καθυστέρηση μόλις καταστούν διαθέσιμες.

Τα συμβαλλόμενα μέρη καθορίζουν στο προσάρτημα Γ όλα τα άλλα στοιχεία που πρέπει να παρέχονται από τον εκτελούντα την επεξεργασία κατά την παροχή βοήθειας στον υπεύθυνο επεξεργασίας για τη συμμόρφωση προς τις υποχρεώσεις του υπευθύνου επεξεργασίας σύμφωνα με τα άρθρα 33 και 34 του κανονισμού (ΕΕ) 2016/679.

ΤΜΗΜΑ ΙΙΙ

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Ρήτρα 10

Μη συμμόρφωση με τις ρήτρες και καταγγελία

α) Με την επιφύλαξη των διατάξεων του κανονισμού (ΕΕ) 2016/679, σε περίπτωση που ο εκτελών την επεξεργασία παραβιάζει τις υποχρεώσεις του σύμφωνα με τις παρούσες ρήτρες, ο υπεύθυνος επεξεργασίας μπορεί να δώσει εντολή στον εκτελούντα την επεξεργασία να αναστείλει την επεξεργασία δεδομένων προσωπικού χαρακτήρα έως ότου ο τελευταίος συμμορφωθεί με τις παρούσες ρήτρες ή καταγγελθεί η σύμβαση. Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας σε περίπτωση που αδυνατεί να συμμορφωθεί με τις παρούσες ρήτρες, για οποιονδήποτε λόγο.

β) Ο υπεύθυνος επεξεργασίας έχει δικαίωμα να καταγγείλει τη σύμβαση στον βαθμό που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις παρούσες ρήτρες, αν:

1) η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον εκτελούντα την επεξεργασία ανεστάλη από τον υπεύθυνο επεξεργασίας σύμφωνα με το στοιχείο α) και η συμμόρφωση με τις παρούσες ρήτρες δεν αποκαταστάθηκε εντός εύλογου χρονικού διαστήματος και, σε κάθε περίπτωση, εντός ενός μηνός από την ημερομηνία της αναστολής.

2) ο εκτελών την επεξεργασία παραβιάζει ουσιωδώς ή με τρόπο διαρκή τις παρούσες ρήτρες ή τις υποχρεώσεις του βάσει του κανονισμού (ΕΕ) 2016/679.

3) ο εκτελών την επεξεργασία δεν συμμορφώνεται με δεσμευτική απόφαση αρμόδιου δικαστηρίου ή της/των αρμόδιας/-ων εποπτικής/-ών αρχής/-ών όσον αφορά τις υποχρεώσεις του σύμφωνα με τις παρούσες ρήτρες ή τον κανονισμό (ΕΕ) 2016/679.

γ) Ο εκτελών την επεξεργασία έχει δικαίωμα να καταγγείλει τη σύμβαση στον βαθμό που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις παρούσες ρήτρες αν, παρόλο που έχει ενημερώσει τον υπεύθυνο επεξεργασίας ότι οι εντολές του παραβιάζουν εφαρμοστέες νομικές απαιτήσεις σύμφωνα με τη ρήτρα 7.1 στοιχείο β), ο υπεύθυνος επεξεργασίας εμμένει στη συμμόρφωση με τις εν λόγω εντολές.

δ) Μετά την καταγγελία της σύμβασης, ο εκτελών την επεξεργασία, κατ' επιλογή του υπευθύνου επεξεργασίας, διαγράφει όλα τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται για λογαριασμό του υπευθύνου επεξεργασίας και πιστοποιεί στον υπεύθυνο επεξεργασίας ότι το έχει πράξει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, εκτός αν το δίκαιο της Ένωσης ή του κράτους μέλους απαιτεί την αποθήκευση των δεδομένων προσωπικού χαρακτήρα. Έως τη διαγραφή ή την επιστροφή των δεδομένων, ο εκτελών την επεξεργασία συνεχίζει να διασφαλίζει τη συμμόρφωση με τις παρούσες ρήτρες.

ΠΡΟΣΑΡΤΗΜΑ Α

Κατάλογος συμβαλλόμενων μερών

Υπεύθυνος/-οι επεξεργασίας: Η εκάστοτε εταιρική οντότητα όπως αναφέρεται ως συμβαλλόμενη στην κυρίως σύμβαση παροχής της υπηρεσίας των εξ αποστάσεως Γενικών Συνελεύσεων

Εκτελών/-ούντες την επεξεργασία:

Όνομα: ΕΛΛΗΝΙΚΟ ΚΕΝΤΡΙΚΟ ΑΠΟΘΕΤΗΡΙΟ ΤΙΤΛΩΝ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ (ATHEXCSD)

Διεύθυνση: Λεωφόρος Αθηνών 110, 104 42, Αθήνα, Ελλάδα

Θέση και στοιχεία επικοινωνίας του υπευθύνου επικοινωνίας: Υπεύθυνος Προστασίας Δεδομένων, dataprotectionofficer@athexgroup.gr

ΠΡΟΣΑΡΤΗΜΑ Β

Περιγραφή της επεξεργασίας

Κατηγορίες υποκειμένων δεδομένων των οποίων τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία

Στο πλαίσιο της παροχής της υπηρεσίας «AXIA E- SHAREHOLDERS' MEETING SERVICE» («Υπηρεσία»), η οποία αφορά την παροχή ολοκληρωμένης τεχνικής λύσης για την πραγματοποίηση Γενικής Συνέλευσης (εφεξής «Γ.Σ.») εκδοτριών εταιρειών από απόσταση σε πραγματικό χρόνο μέσω χρήσης ηλεκτρονικών μέσων, τυγχάνουν επεξεργασίας δεδομένα προσωπικού χαρακτήρα των μετόχων των εκδοτριών εταιρειών καθώς και φυσικά πρόσωπα πέραν των μετόχων, που θα συμμετάσχουν στην εξ αποστάσεως Γενική Συνέλευση όπως τα Μέλη του Διοικητικού Συμβουλίου των εκδοτριών, τα διοικητικά στελέχη των εκδοτριών, ελεγκτές και λοιπά τρίτα πρόσωπα.

Κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία

Κατά την παροχή της Υπηρεσίας, τυγχάνουν επεξεργασίας δεδομένα προσωπικού χαρακτήρα, όπως:

- Δεδομένα ταυτοποίησης, όπως ονοματεπώνυμο, πατρώνυμο, ΑΔΤ ή ισοδύναμο έγγραφο.
- Δεδομένα σχετικά με την ιδιότητα βάσει της οποίας τα πρόσωπα δικαιούνται να συμμετάσχουν στη Γενική Συνέλευση και τα σχετικά αποδεικτικά έγγραφα.
- Ηλεκτρονική διεύθυνση (e-mail) με σκοπό τη συμμετοχή του φυσικού προσώπου στην τηλεδιάσκεψη.

- Δεδομένα εικόνας και ήχου σε περίπτωση που ο συμμετέχων στη Γενική Συνέλευση πάρει τον λόγο κατά τη διάρκειά της.
- Αριθμός και κατηγορία μετοχών που κατέχει ο μέτοχος.
- Κωδικός Αριθμός Μερίδας στο Σύστημα Άυλων Τίτλων (Σ.Α.Τ.)
- Δεδομένα που αφορούν στη συμμετοχή και την άσκηση δικαιώματος ψήφου του Μετόχου στη Γενική Συνέλευση, συμπεριλαμβανομένων των δεδομένων που απαιτούνται για την συμμετοχή σε ηλεκτρονική τηλεδιάσκεψη (π.χ. κωδικοί πρόσβασης).
- Τυχόν άλλα δεδομένα των μετόχων και των λοιπών συμμετεχόντων, η επεξεργασία των οποίων κρίνεται αναγκαία κατά την εκτέλεση της Υπηρεσίας.

Φύση της επεξεργασίας

Ο εκτελών την επεξεργασία αναλαμβάνει δια του παρόντος την επεξεργασία των ανωτέρω δεδομένων προσωπικού χαρακτήρα, τα οποία είναι απαραίτητα για την παροχή της Υπηρεσίας, όπως αναλύεται στους ειδικούς όρους «AXIA E- SHAREHOLDERS' MEETING SERVICE». Συμφωνείται μεταξύ των συμβαλλομένων μερών ότι απαγορεύεται οποιαδήποτε άλλη μορφή επεξεργασίας προσωπικών δεδομένων από τον εκτελούντα την επεξεργασία.

Σκοπός/-οί για τον οποίο ή τους οποίους τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για λογαριασμό του υπευθύνου επεξεργασίας

Τα δεδομένα προσωπικού χαρακτήρα, όπως περιγράφονται ανωτέρω, τυγχάνουν επεξεργασίας για το σκοπό της παροχής της υπηρεσίας «AXIA E- SHAREHOLDERS' MEETING SERVICE», η οποία αποτελεί ολοκληρωμένη τεχνική λύση για την πραγματοποίηση Γ.Σ. από απόσταση, σε πραγματικό χρόνο και περιλαμβάνει την υπηρεσία Zoom Meetings μέσω της οποίας παρέχεται η δυνατότητα συμμετοχής στη τηλεδιάσκεψη (video conference) και τη διαδικτυακή πλατφόρμα μέσω της οποίας παρέχεται η δυνατότητα διεξαγωγής της Γενικής Συνέλευσης (ψηφοφορία μετόχων κ.λπ.)

Διάρκεια της επεξεργασίας

Για όσο διάστημα διαρκεί η σύμβαση παροχής της υπηρεσίας

Αντικείμενο, φύση και διάρκεια επεξεργασίας για την επεξεργασία από υπο-εκτελούντες την επεξεργασία (υπεργολάβους επεξεργασίας)

Η Υπηρεσία παρέχει τη δυνατότητα συμμετοχής σε τηλεδιάσκεψη (video conference) μέσω της εφαρμογής Zoom που διατίθεται από την εταιρεία Zoom Video Communications Inc. ("Zoom"). Στο πλαίσιο αυτό, η Zoom ενεργεί ως υπεργολάβος επεξεργασίας, καθώς επεξεργάζεται για λογαριασμό της ATHEXCSD δεδομένα προσωπικού χαρακτήρα μετόχων και λοιπών συμμετεχόντων στη Γενική Συνέλευση, τα οποία συλλέγονται κατά την διεξαγωγή Γενικής Συνέλευσης από απόσταση, σε πραγματικό χρόνο, χωρίς τη φυσική παρουσία των μετόχων και των λοιπών συμμετεχόντων.

Τα δεδομένα που διαβιβάζονται στη Zoom τηρούνται in-transit και at-rest σε εγκαταστάσεις της Zoom που βρίσκονται εντός της Ευρωπαϊκής Ένωσης. Ωστόσο για εξαιρετικές περιπτώσεις όπως η παροχή τεχνικής υποστήριξης, που ενδέχεται να πραγματοποιηθεί διαβίβαση δεδομένων εκτός ΕΟΧ, η ATHEXCSD, προς τήρηση της νομιμότητας της επεξεργασίας και σύμφωνα με το Κεφάλαιο V του ΓΚΠΔ, έχει εξετάσει και διασφαλίσει την ύπαρξη τυποποιημένων συμβατικών ρητρών (SCC) για διαβιβάσεις δεδομένων εκτός ΕΟΧ καθώς και πρόσθετων μέτρων που λαμβάνει η Zoom.

Στον παρακάτω σύνδεσμο παρέχεται λίστα με τους υπεργολάβους επεξεργασίας της Zoom, οι οποίοι ενδέχεται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό της: Zoom Third-Party Subprocessors & Zoom Affiliates | Zoom.

ΠΡΟΣΑΡΤΗΜΑ Γ

Τεχνικά και οργανωτικά μέτρα, συμπεριλαμβανομένων των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας των δεδομένων

<u>Α. Οργανωτικά Μέτρα</u>

1. Πολιτικές Διαχείρισης Ασφαλείας Πληροφοριών και Προστασίας Δεδομένων

- Θέσπιση Πολιτικής για την προστασία προσωπικών δεδομένων.
- Θέσπιση Πολιτικής Ασφαλείας Πληροφοριών.
- Οι πολιτικές έχουν κοινοποιηθεί σε όλο το προσωπικό και σε εξωτερικούς συνεργάτες κατά περίπτωση και διενεργούνται σε ετήσια βάση εκπαιδεύσεις.
- Οι ανωτέρω Πολιτικές αναφέρουν μεταξύ άλλων:
  - Τους ρόλους και τις υποχρεώσεις του προσωπικού
  - Τα βασικά μέτρα που έχουν υιοθετηθεί για την προστασία των προσωπικών δεδομένων, τους εκτελούντες την επεξεργασία και τα τρίτα μέρη που συμμετέχουν στην επεξεργασία δεδομένων
- Πιστοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών κατά το διεθνές πρότυπο ασφάλειας ISO-27001.

2. Καθορισμός ειδικών Ρόλων και Αρμοδιοτήτων τους

- Οι ρόλοι και οι αρμοδιότητες του προσωπικού που αφορούν στην επεξεργασία προσωπικών δεδομένων είναι σαφώς ορισμένοι στις Πολιτικές Ασφαλείας Πληροφοριών και Προστασίας Προσωπικών Δεδομένων.
- Κατά την διάρκεια εσωτερικής αναδιοργάνωσης ή τερματισμού και τροποποίησης εργασιών, διενεργείται η ανάκληση των δικαιωμάτων και των αρμοδιοτήτων σύμφωνα με καταγεγραμμένες διαδικασίες.
- Έχουν οριστεί σαφώς οι αρμόδιοι για συγκεκριμένα καθήκοντα ασφαλείας πληροφοριών και προστασίας δεδομένων, συμπεριλαμβανομένου του ορισμού Υπευθύνου Ασφαλείας Πληροφοριών (CISO) και Υπευθύνου Προστασίας Δεδομένων (DPO).
- Τα καθήκοντα και οι αρμοδιότητες του Υπευθύνου Ασφαλείας Πληροφοριών και του Υπευθύνου Προστασίας Δεδομένων είναι σαφώς καθορισμένα και καταγεγραμμένα στους εσωτερικούς κανονισμούς και τις πολιτικές της Εταιρείας.
- Υφίσταται διαχωρισμός καθηκόντων και σχετικών αρμοδιοτήτων, για την προστασία από μη εξουσιοδοτημένη τροποποίησης/απώλεια/διαρροή/χρήση προσωπικών δεδομένων.

3. Πολιτική Διαχείρισης Χρηστών

- Υφίστανται κατάλληλα δικαιώματα πρόσβασης για κάθε ρόλο σύμφωνα με τις ανάγκες του καθώς και Πολιτική Διαχείρισης Χρηστών όπου μεταξύ άλλων καθορίζονται οι απαραίτητοι κανόνες ελέγχου πρόσβασης, τα δικαιώματα πρόσβασης και οι περιορισμοί για συγκεκριμένους ρόλους ανά χρήστη.
- Είναι σαφώς καθορισμένοι και καταγεγραμμένοι ο διαχωρισμός των ρόλων ως προς τα δικαιώματα πρόσβασης και οι ρόλοι με αυξημένα δικαιώματα πρόσβασης.

4. Διαχείριση Πόρων

- Ο Εκτελών την Επεξεργασία διατηρεί ενημερωμένο κατάλογο των πληροφοριακών πόρων που χρησιμοποιούνται για την επεξεργασία των προσωπικών δεδομένων (υλικό, λογισμικό και υποδομές δικτύου).
- Οι πληροφοριακοί πόροι διαβαθμίζονται ως προς την κρισιμότητά τους και επιθεωρούνται σε περιοδική βάση.
- Οι ρόλοι και οι προσβάσεις στους πληροφοριακούς πόρους είναι καθορισμένοι και καταγεγραμμένοι.

5. Διαχείριση Αλλαγών

- Όλες οι αλλαγές στα πληροφοριακά συστήματα είναι τεκμηριωμένες, εγκεκριμένες και επισκοπούνται αρμοδίως.
- Η ανάπτυξη λογισμικού διενεργείται σε ειδικό χωριστό περιβάλλον από το περιβάλλον παραγωγής. Όταν είναι απαραίτητος ο έλεγχος, χρησιμοποιούνται εικονικά δεδομένα ή τεχνικές απομάκρυνσης ή τροποποίησης δεδομένων.
- Υφίσταται Πολιτική Διαχείρισης Αλλαγών, βάσει της οποίας τεκμηριώνονται οι αλλαγές, οι ρόλοι/χρήστες που έχουν δικαιώματα υλοποίησης αλλαγών και οι σχετικές εγκριτικές διαδικασίες.

6. Επεξεργασία Προσωπικών Δεδομένων

- Υφίστανται διαδικασίες για την επεξεργασία των προσωπικών δεδομένων με σκοπό την επίτευξη του κατάλληλου επιπέδου προστασίας τους και για τις οποίες ενημερώνεται τακτικά το προσωπικό της Εταιρείας.
- Η Εταιρεία ως Εκτελών την Επεξεργασία παρέχει επαρκή και τεκμηριωμένα στοιχεία της συμμόρφωσης με τον ΓΚΠΔ στον Υπεύθυνο Επεξεργασίας.

7. Διαχείριση περιστατικών ασφαλείας/προσωπικών δεδομένων

- Υφίσταται σχέδιο αντιμετώπισης περιστατικών ασφαλείας και παραβίασης προσωπικών δεδομένων με αναλυτικές διαδικασίες με σκοπό την αποτελεσματική ανταπόκριση σε τυχόν περιστατικά παραβίασης προσωπικών δεδομένων το οποίο περιλαμβάνει ενέργειες για τον περιορισμό κινδύνων καθώς και διακριτούς ρόλους και αρμοδιότητες του αρμόδιου προσωπικού.

8. Επιχειρησιακή συνέχεια

- Ο Εκτελών την Επεξεργασία διαθέτει Σχέδιο Επιχειρησιακής Συνέχειας και Σχέδιο Ανάκτησης Πληροφοριακών Συστημάτων από Καταστροφή (BCP/DRP), τα οποία είναι εγκεκριμένα από τη Διοίκηση και επιθεωρούνται ως προς την επάρκεια και αποτελεσματικότητα τους τουλάχιστον σε ετήσια βάση (το Σχέδιο Επιχειρησιακής Συνέχειας έχει πιστοποιηθεί κατά το διεθνές πρότυπο επιχειρησιακής συνέχειας ISO-22301).
- Τα ανωτέρω σχέδια περιλαμβάνουν σαφείς δράσεις και ανάθεση σχετικών ρόλων και αρμοδιοτήτων.
- Υφίστανται εναλλακτικές εγκαταστάσεις για την αποτελεσματική εφαρμογή των ανωτέρω σχεδίων.

9. Τήρηση εμπιστευτικότητας

- Ο εκτελών την επεξεργασία διασφαλίζει ότι το προσωπικό κατανοεί τις ευθύνες και τις υποχρεώσεις που συνδέονται με την επεξεργασία προσωπικών δεδομένων. Οι ρόλοι και οι ευθύνες του προσωπικού γνωστοποιούνται σαφώς.
- Πριν την ανάληψη των καθηκόντων τους οι εργαζόμενοι γνωρίζουν και αποδέχονται την πολιτική ασφαλείας του οργανισμού και υπογράφουν σύμβαση τήρησης εμπιστευτικότητας.

10. Εκπαίδευση και ευαισθητοποίηση ασφαλείας πληροφοριών

- Παρέχεται επαρκής πληροφόρηση προς το προσωπικό σχετικά με τα μέτρα ασφαλείας στα πληροφοριακά συστήματα. Οι υπάλληλοι που σχετίζονται με θέματα επεξεργασίας προσωπικών δεδομένων είναι ενημερωμένοι και ευαισθητοποιημένοι σχετικά με θέματα προστασίας προσωπικών δεδομένων και τις ανάλογες υποχρεώσεις τους.
- Παρέχονται εξειδικευμένα προγράμματα εκπαίδευσης και ευαισθητοποίησης σε θέματα ασφαλείας πληροφοριών και προστασίας προσωπικών δεδομένων για όλο το προσωπικό σε ετήσια τουλάχιστον βάση.

11. Διαχείριση κινδύνων ασφαλείας πληροφοριών

- Διενεργείται σε νέα κρίσιμα πληροφοριακά συστήματα / υπηρεσίες αξιολόγηση κινδύνων ασφαλείας πληροφοριών. Επιπλέον σε περιοδική βάση διενεργείται και επαναξιολόγηση κινδύνων ασφαλείας πληροφοριών σε υφιστάμενα κρίσιμα πληροφοριακά συστήματα / υπηρεσίες.

Β. Τεχνικά μέτρα

1. Έλεγχοι πρόσβασης/ταυτοποίησης

- Η πρόσβαση των χρηστών στα πληροφοριακά συστήματα είναι ελεγχόμενη (περιλαμβάνοντας δημιουργία, έγκριση, αναθεώρηση και διαγραφή λογαριασμών χρηστών).

- Αποφεύγεται η χρήση κοινών λογαριασμών χρήστη.
- Υφίστανται κατάλληλοι μηχανισμοί ελέγχου πρόσβασης (ταυτοποίησης).
- Υφίσταται κατάλληλη πολιτική κωδικών πρόσβασης. Η πολιτική ορίζει τουλάχιστον το μήκος του κωδικού πρόσβασης, την πολυπλοκότητα, την περίοδο ισχύος, καθώς επίσης και αριθμό αποδεκτών ανεπιτυχών προσπαθειών σύνδεσης. Οι κωδικοί πρόσβασης αποθηκεύονται σε κρυπτογραφημένη μορφή (hash).
- Χρησιμοποιείται σε κρίσιμα συστήματα κυρίως όπου τηρούνται προσωπικά δεδομένα, έλεγχος ταυτοποίησης χρήστη δύο παραγόντων (2 factor authentication).

2. Αρχεία καταγραφής και παρακολούθησης

- Υφίστανται αρχεία καταγραφής δραστηριοτήτων στα συστήματα/εφαρμογές που κατά κανόνα χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων, τα οποία περιλαμβάνουν όλους τους τύπους πρόσβασης στα εν λόγω δεδομένα. Οι δραστηριότητες των χρηστών (συμπεριλαμβανομένων των διαχειριστών) καταγράφονται.
- Τα αρχεία καταγραφής προστατεύονται επαρκώς με κατάλληλα μέτρα ασφαλείας.

3. Ασφάλεια βάσεων δεδομένων/εφαρμογών

- Στις βάσεις δεδομένων και στις εφαρμογές πραγματοποιείται επεξεργασία των προσωπικών δεδομένων που είναι απαραίτητα σύμφωνα με τους σκοπούς της επεξεργασίας.
- Τεχνικές ψευδωνυμοποίησης ή ανωνυμοποίησης υλοποιούνται όπου απαιτείται.
- Εφαρμόζεται τείχος προστασίας επιπέδου εφαρμογών Web (Web Application Firewall) από εξειδικευμένο πάροχο.

4. Ασφάλεια δικτύου/επικοινωνιών

- Οι επικοινωνίες σχετικά με προσβάσεις μέσω του Internet είναι κρυπτογραφημένες μέσω κατάλληλων πρωτοκόλλων κρυπτογράφησης.
- Η ασύρματη πρόσβαση στο σύστημα, επιτρέπεται μόνο για συγκεκριμένους χρήστες και διεργασίες οι οποίοι προστατεύονται μέσω μηχανισμών κρυπτογράφησης.
- Η απομακρυσμένη πρόσβαση στα συστήματα προστατεύεται επαρκώς από κινδύνους κυβερνοασφάλειας και ασφάλειας πληροφοριών.
- Η δικτυακή κίνηση προς και από τα πληροφοριακά συστήματα παρακολουθείται και ελέγχεται μέσω κατάλληλων μηχανισμών προστασίας firewalls και IDS/IPS.
- Εφαρμόζεται προστασία αποστέρησης παροχής υπηρεσιών (anti-DDoS protection), τόσο σε επίπεδο εφαρμογής, όσο και σε επίπεδο δικτύου από εξειδικευμένους παρόχους.

5. Ασφάλεια από κακόβουλο λογισμικό

- Υφίσταται συνεχώς ενημερωμένη προστασία από κακόβουλο λογισμικό.

6. Αντίγραφα ασφαλείας

- Υφίστανται διαδικασίες για τη δημιουργία αντιγράφων ασφαλείας και την επαναφορά δεδομένων.
- Στα αντίγραφα ασφαλείας παρέχεται το κατάλληλο επίπεδο φυσικής ασφαλείας.
- Τα αντίγραφα ασφαλείας όπου αυτό απαιτείται σύμφωνα με τη διαβάθμισή τους, είναι κρυπτογραφημένα., ελέγχονται για ύπαρξη ransomware και προστατεύονται από οποιαδήποτε αλλοίωση για προκαθορισμένο ελάχιστο διάστημα.

7. Ασφάλεια κύκλου ζωής εφαρμογής

- Κατά την ανάπτυξη των εφαρμογών ακολουθούνται βέλτιστες πρακτικές, πλαίσια και πρότυπα.
- Οι απαιτήσεις ασφαλείας καθορίζονται από τα αρχικά στάδια ανάπτυξης της εφαρμογής.
- Υιοθετούνται, κατ' αναλογία με τις απαιτήσεις ασφαλείας, ειδικές τεχνολογίες και τεχνικές που έχουν σχεδιαστεί για την προστασία της ιδιωτικότητας και των δεδομένων.
- Κατά τη διάρκεια της ανάπτυξης, διεξάγονται οι απαιτούμενοι έλεγχοι για την τήρηση των αρχικών απαιτήσεων ασφαλείας.
- Πραγματοποιούνται οι απαραίτητοι έλεγχοι ασφαλείας (vulnerability assessments, penetration tests) πριν την ένταξη της εφαρμογής στις επιχειρησιακές διαδικασίες, ώστε να προχωρήσει η ένταξη της στο περιβάλλον παραγωγής.
- Διεξάγονται περιοδικοί τεχνικοί έλεγχοι ασφαλείας (vulnerability assessments, penetration tests), όπου αυτό κρίνεται απαραίτητο βάσει των πολιτικών ασφαλείας.
- Λαμβάνεται ενημέρωση σχετικά με τις τεχνικές ευπάθειες των συστημάτων που χρησιμοποιούνται.
- Οι νέες εκδόσεις του λογισμικού ελέγχονται και αξιολογούνται πριν εγκατασταθούν σε παραγωγικό περιβάλλον.

8. Διαγραφή δεδομένων / επαναχρησιμοποίηση

- Σε όλα τα ηλεκτρονικά μέσα αποθήκευσης στα οποία υπάρχουν προσωπικά δεδομένα, εκτελείται ασφαλής διαγραφή/απομαγνητισμός των δεδομένων, μέσω λογισμικού, πριν από την απόσυρσή τους. Σε περιπτώσεις όπου αυτό δεν είναι εφικτό (CD, DVD, κ.λπ.) πραγματοποιείται φυσική καταστροφή του μέσου.
- Διενεργείται ασφαλής καταστροφή των εγγράφων στα οποία υπήρχε αποθήκευση προσωπικών δεδομένων με χρήση καταστροφέα εγγράφων ή άλλης ασφαλούς μεθόδου.

- Όπου λαμβάνει χώρα η χρήση υπηρεσιών τρίτων μερών για την ασφαλή καταστροφή των μέσων ή των εγγράφων, συνάπτεται συμφωνία παροχής υπηρεσιών και σχετικά πρωτόκολλά καταστροφής με καταγραφή των αρχείων που καταστράφηκαν.

9. Φυσική Ασφάλεια

- Οι χώροι όπου έχουν εγκατασταθεί κρίσιμα συστήματα και υποδομές του πληροφοριακού συστήματος δεν είναι προσβάσιμοι από μη εξουσιοδοτημένο προσωπικό. Ορίζονται ζώνες ασφαλείας και προστατεύονται από κατάλληλους μηχανισμούς εισόδου.
- Υφίστανται μέθοδοι σαφούς αναγνώρισης, μέσω κατάλληλων μέσων (π.χ. ειδικών ταυτοτήτων) για το σύνολο του προσωπικού και των επισκεπτών που έχουν πρόσβαση στις εγκαταστάσεις της Εταιρείας.
- Τα συστήματα ανίχνευσης μη εξουσιοδοτημένης πρόσβασης εγκαθίστανται σε όλες τις ζώνες ασφαλείας.
- Υφίσταται αυτόματο σύστημα πυρανίχνευσης και κατάσβεσης πυρκαγιάς, σύστημα υγρανίχνευσης, σύστημα κλιματισμού, εναλλακτικό σύστημα παροχής ηλεκτρικού ρεύματος (γεννήτριες) και σύστημα παροχής συνεχούς τροφοδοσίας (UPS).
- Το προσωπικό εξωτερικών συνεργατών έχει περιορισμένη και ελεγχόμενη πρόσβαση στις περιοχές με κρίσιμα συστήματα.