Σύμβαση επεξεργασίας δεδομένων (κατά το άρθρο 28 του ΓΚΠΔ)

μεταξύ

του **Χρήστη** (όπως ορίζεται στην Κύρια σύμβαση)

(εφεξής «**Πελάτης**»)

και

της **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 Μόναχο, Γερμανία

(εφεξής «**Ανάδοχος**»)
(ο Πελάτης και ο Ανάδοχος αποτελούν εφεξής ένα «**Συμβαλλόμενο μέρος**» και από κοινού τα «**Συμβαλλόμενα μέρη**»).

Προοίμιο

(A) Η παρούσα Σύμβαση επεξεργασίας δεδομένων (εφεξής «**Σύμβαση**») ισχύει για όλες τις δραστηριότητες, κατά τις οποίες ο Ανάδοχος έρχεται σε επαφή με προσωπικά δεδομένα (όπως ορίζεται στο εδάφιο 1.5 παρακάτω) του Πελάτη, τρίτων παρόχων ή άλλων εμπλεκομένων, όσον αφορά τη δραστηριότητα που περιγράφεται στο εδάφιο 2 των Γενικών προϋποθέσεων για τη χρήση της πλατφόρμας και, εφόσον απαιτηθεί, συμπεριλαμβανομένων των μεμονωμένων συμβάσεων που συνάπτονται για περαιτέρω υπηρεσίες (εφεξής «**Κύρια σύμβαση**»).

(B) Σύμφωνα με την παρούσα Σύμβαση, ο Πελάτης ενεργεί ως υπεύθυνος επεξεργασίας και ο Ανάδοχος ως εκτελών την επεξεργασία στο πλαίσιο μιας επεξεργασίας προσωπικών δεδομένων, σύμφωνα με το άρθρο 28 του ΓΚΠΔ (όπως ορίζεται στη συνέχεια).

Τα συμβαλλόμενα μέρη συμφωνούν τα εξής:

1 Ορισμοί και ερμηνείες

1.1 Ως «**Ευρωπαϊκή νομοθεσία**» νοείται το εφαρμοστέο δίκαιο της Ευρωπαϊκής Ένωσης, οι ισχύοντες νόμοι των σημερινών κρατών μελών της Ευρωπαϊκής Ένωσης, καθώς και οι εφαρμοστέοι νόμοι οποιουδήποτε κράτους, που στη συνέχεια γίνεται κράτος μέλος της Ευρωπαϊκής Ένωσης.

1.2 Ως «**Ευρωπαϊκό δίκαιο περί προστασίας δεδομένων**» νοείται το εφαρμοστέο δίκαιο της Ευρωπαϊκής Ένωσης για την επεξεργασία προσωπικών δεδομένων (ιδιαίτερα ο Γενικός κανονισμός για την προστασία δεδομένων), οι ισχύοντες νόμοι των σημερινών κρατών μελών της Ευρωπαϊκής Ένωσης για την επεξεργασία προσωπικών δεδομένων (ιδιαίτερα ο Ομοσπονδιακός νόμος για την προστασία των προσωπικών δεδομένων στην ενημερωμένη του έκδοση), καθώς

και οι εφαρμοστέοι νόμοι οποιουδήποτε κράτους για την επεξεργασία προσωπικών δεδομένων, που στη συνέχεια γίνεται κράτος μέλος της Ευρωπαϊκής Ένωσης.

1.3 Ως «**Γενικός κανονισμός για την προστασία δεδομένων**» νοείται ο ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός κανονισμός για την προστασία δεδομένων).

1.4 Ως «**BDSG**» νοείται ο Ομοσπονδιακός νόμος για την προστασία των προσωπικών δεδομένων.

1.5 Τα «**Προσωπικά δεδομένα**» ερμηνεύονται όπως ορίζεται στον BDSG/Γενικό κανονισμό για την προστασία δεδομένων.

2 Αντικείμενο της επεξεργασίας δεδομένων / υποχρεώσεις του Πελάτη

2.1 Η παρούσα σύμβαση ρυθμίζει τις υποχρεώσεις των συμβαλλόμενων μερών, όσον αφορά την επεξεργασία των προσωπικών δεδομένων του Πελάτη από τον Ανάδοχο, στο πλαίσιο της Κύριας σύμβασης που αναφέρεται στο Παράρτημα 1.

2.2 Το αντικείμενο και η διάρκεια της επεξεργασίας, της φύσης και του σκοπού της επεξεργασίας, η φύση των προσωπικών δεδομένων, οι κατηγορίες των ενδιαφερόμενων προσώπων, οι υποχρεώσεις και τα δικαιώματα του υπεύθυνου προσώπου προκύπτουν από το Παράρτημα 1 της παρούσας σύμβασης και την περιγραφή των παρεχόμενων υπηρεσιών της Κύριας σύμβασης.

2.3 Ο Πελάτης παραμένει υπεύθυνος υπό την έννοια του ΓΚΠΔ και εγγυάται τη νομιμότητα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εμπλεκομένων ατόμων (οδηγός και/ή περαιτέρω άτομα). Σε σχέση με τα παραπάνω, ο Πελάτης ανταποκρίνεται ειδικότερα στη διευρυμένη υποχρέωση ενημέρωσης και διασφαλίζει, ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα υπόκειται σε νομική βάση στο πλαίσιο της προστασίας δεδομένων προσωπικού χαρακτήρα (π.χ., σύναψη μιας συμφωνίας εκμετάλλευσης, περιορισμός της επεξεργασίας σε σκοπούς της σχέσης απασχόλησης).

3 Υποχρεώσεις του Ανάδοχου

3.1 Ο Ανάδοχος επεξεργάζεται τα προσωπικά δεδομένα του Πελάτη αποκλειστικά για τους σκοπούς που αναφέρονται στο Παράρτημα 1 και στο πλαίσιο της Κύριας σύμβασης, καθώς και για λογαριασμό και σύμφωνα με τις οδηγίες του Πελάτη που αναφέρονται στο Παράρτημα 1. Ο Ανάδοχος δε θα επεξεργαστεί τα προσωπικά δεδομένα για οποιονδήποτε άλλο σκοπό βάσει της παρούσας σύμβασης. Αυτό δεν επηρεάζει την επεξεργασία εκτός του πλαισίου της παρούσας σύμβασης για ίδιους σκοπούς, σύμφωνα με το εδάφιο 8.3.4 της Κύριας σύμβασης. Απαγορεύεται η δημιουργία αντιγράφων ή διπλότυπων των προσωπικών δεδομένων χωρίς να το γνωρίζει ο Πελάτης. Εξαιρούνται τα αντίγραφα ασφαλείας, εφόσον απαιτούνται για την εξασφάλιση της ορθής

επεξεργασίας δεδομένων, καθώς και δεδομένα που απαιτούνται για τη συμμόρφωση με τις νόμιμες απαιτήσεις διατήρησης.

3.2 Μετά την ολοκλήρωση της παροχής των υπηρεσιών επεξεργασίας, ο Ανάδοχος πρέπει είτε να παραδώσει στον Πελάτη όλα τα προσωπικά δεδομένα του Πελάτη κατ' επιλογή του, και/ή να τα διαγράψει σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων, εφόσον δεν έρχονται σε σύγκρουση με τη νόμιμη περίοδο διατήρησης και εφόσον ο Ανάδοχος δεν τα επεξεργάζεται για δικούς του σκοπούς, εκτός του πλαισίου της παρούσας σύμβασης, σύμφωνα με το εδάφιο 8.3.4. της Κύριας σύμβασης. Το ίδιο ισχύει για το υλικό σχετικά με το δοκιμαστικό υλικό και το υλικό απόρριψης. Η πλήρης διαγραφή ή παράδοση των δεδομένων στον Πελάτη πρέπει να επιβεβαιωθεί κατ' απαίτησή του γραπτώς με ημερομηνία.

3.3 Εφόσον περιλαμβάνεται στο εύρος των υπηρεσιών, ο Ανάδοχος υποστηρίζει τον Πελάτη κατά την άσκηση των δικαιωμάτων των εμπλεκομένων (πρόσβαση, δικαίωμα, αντίταξη, διαγραφή) κατόπιν αντίστοιχης εντολής του Πελάτη.

3.4 Ο Ανάδοχος επιβεβαιώνει ότι έχει διορίσει έναν υπεύθυνο επεξεργασίας, εφόσον απαιτείται από τον νόμο (βλ. Άρθρο 38 του BDSG, άρθρο 37 του ΓΚΠΔ).

3.5 Ο Ανάδοχος είναι υποχρεωμένος να ειδοποιήσει αμέσως τον Πελάτη για τα αποτελέσματα των ελέγχων από τις εποπτικές αρχές προστασίας δεδομένων, στον βαθμό που αυτές συνδέονται με την επεξεργασία των δεδομένων του Πελάτη. Ο Ανάδοχος θα διορθώσει τυχόν διαπιστωμένα παράπονα εντός εύλογου χρονικού διαστήματος και θα ενημερώσει σχετικά τον Πελάτη.

3.6 Η επεξεργασία των δεδομένων από τον Ανάδοχο και τους υπεργολάβους που έχει εγκρίνει ο Πελάτης πραγματοποιείται αποκλειστικά στο έδαφος της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, σε κράτος μέλος της Ευρωπαϊκής Ένωσης ή σε άλλο συμβαλλόμενο κράτος της Συμφωνίας για τον Ευρωπαϊκό Οικονομικό Χώρο. Για κάθε μεταφορά σε άλλη χώρα (εφεξής «**Τρίτη χώρα**»), απαιτείται η προηγούμενη ρητή συγκατάθεση του Πελάτη και μπορεί να πραγματοποιηθεί μόνο εάν πληρούνται οι ειδικοί όροι για την εξαγωγή δεδομένων σε τρίτες χώρες (βλ. άρθρο 40 και επόμενα του ΓΚΠΔ). Για τον σκοπό αυτό, απαιτούνται οι πληροφορίες στο Παράρτημα 1 και πρέπει να επισυναφθούν πρόσθετα (συμβατικά) έγγραφα, εάν απαιτείται.

3.7 Ο Ανάδοχος οφείλει να κατατοπίσει τους εργαζομένους που εμπλέκονται στην εκτέλεση του έργου, όσον αφορά τις σχετικές διατάξεις για την προστασία προσωπικών δεδομένων, και να τους δεσμεύσει σχετικά με το απόρρητο των δεδομένων (βλ. Άρθρο 28 του ΓΚΠΔ, παρ. 3 β)), όπως και να διασφαλίσει, λαμβάνοντας τα κατάλληλα μέτρα, ότι οι αντίστοιχοι εργαζόμενοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μόνο κατ’ εντολή του Πελάτη.

3.8 Ο Ανάδοχος παρακολουθεί τακτικά την τήρηση των διατάξεων περί προστασίας δεδομένων της παρούσας σύμβασης και τις τεκμηριωμένες οδηγίες του Πελάτη καθόλη τη διάρκεια ισχύος της σύμβασης. Τα αποτελέσματα των ελέγχων πρέπει να υποβάλλονται στον Πελάτη κατ' απαίτηση, στο μέτρο που αυτά αφορούν την επεξεργασία των δεδομένων του Πελάτη. Τα μέτρα

παρακολούθησης πρέπει να περιγράφονται σε μια προσέγγιση για την προστασία των δεδομένων, η οποία πρέπει να υποβληθεί στον Πελάτη κατόπιν αιτήματος.

3.9 Λαμβάνοντας υπόψη τη φύση της επεξεργασίας και αν είναι δυνατόν, ο Ανάδοχος πρέπει να υποστηρίξει τον Πελάτη με κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να ανταποκριθεί στην υποχρέωσή του να απαντήσει σε αιτήματα σχετικά με την άσκηση των δικαιωμάτων των ενδιαφερόμενων προσώπων που αναφέρονται στο κεφάλαιο III του Γενικού κανονισμού για την προστασία δεδομένων. Ο Πελάτης πρέπει να αναλάβει τα έξοδα που προκύπτουν από τον Ανάδοχο.

3.10 Λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει, ο Ανάδοχος πρέπει να υποστηρίξει τον Πελάτη σχετικά με την εκπλήρωση των υποχρεώσεων που προβλέπονται στα άρθρα 32 έως 36 του Γενικού κανονισμού για την προστασία δεδομένων.

4 Τεχνικά και οργανωτικά μέτρα για την ασφάλεια των δεδομένων

4.1 Ο Ανάδοχος θα λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων (βλ. άρθρο 32 του ΓΚΠΔ). Ειδικότερα, ο Ανάδοχος υποχρεούται να εφαρμόσει τα τεχνικά και οργανωτικά μέτρα που έχουν συμφωνηθεί συμβατικά στο Παράρτημα 2 της παρούσας σύμβασης. Κατά τη διάρκεια της σχέσης συνεργασίας, τα μέτρα αυτά πρέπει να προσαρμόζονται από τον Ανάδοχο στην τεχνική και οργανωτική εξέλιξη, χωρίς να μειώνεται το επίπεδο προστασίας. Οι σημαντικές αλλαγές πρέπει να συμφωνηθούν γραπτώς.

4.2 Ο Ανάδοχος θα ενημερώσει τον Πελάτη κατόπιν αιτήματος για την πραγματική συμμόρφωση με τα τεχνικά και οργανωτικά μέτρα.

4.3 Ο Ανάδοχος υποχρεούται να παρέχει επαρκή τεκμηρίωση της επεξεργασίας των δεδομένων, βάσει της οποίας ο Πελάτης μπορεί να αποδείξει την ορθή επεξεργασία των δεδομένων. Τα αποδεικτικά στοιχεία μπορούν επίσης να παρέχονται με εγκεκριμένη διαδικασία πιστοποίησης, σύμφωνα με το άρθρο 42 του Γενικού κανονισμού για την προστασία δεδομένων.

5 Υπεργολάβος

5.1 Ο Ανάδοχος εξουσιοδοτείται διά του παρόντος να δεσμεύει τους υπεργολάβους που αναφέρονται στο Παράρτημα 1.

5.2 Γενικά επιτρέπεται η συμμετοχή περαιτέρω υπεργολάβων. Ωστόσο, ο Ανάδοχος θα ενημερώσει τον Πελάτη για τυχόν προβλεπόμενη αλλαγή σε σχέση με τη συμμετοχή ή την αντικατάσταση των υπεργολάβων. Ο Πελάτης μπορεί να υποβάλει ένσταση για τις προβλεπόμενες αλλαγές. Ως μη σχέσεις υπεργολαβίας υπό την έννοια της παρούσας ρύθμισης, πρέπει να νοούνται οι εν λόγω παροχές υπηρεσιών, τις οποίες χρησιμοποιεί ο Ανάδοχος ως βοηθητική υπηρεσία σε τρίτους, προκειμένου να συμβάλει στην εκτέλεση της εντολής. Σε αυτές περιλαμβάνονται, π.χ. υπηρεσίες τηλεπικοινωνιών, προσωπικό καθαρισμού, ελεγκτές ή η απόρριψη φορέων δεδομένων. Ωστόσο, ο Ανάδοχος είναι υποχρεωμένος να λαμβάνει τις κατάλληλες και συμβατές συμβατικές συμφωνίες

και να λαμβάνει μέτρα ελέγχου, προκειμένου να εξασφαλίσει την προστασία και την ασφάλεια των δεδομένων του Πελάτη, ακόμη και στην περίπτωση εξωτερικών αναθέσεων βοηθητικών υπηρεσιών.

5.3 Εάν ο Ανάδοχος χρησιμοποιεί έναν υπεργολάβο, ο Ανάδοχος πρέπει να εξασφαλίσει ότι επιβάλλονται σε αυτόν οι ίδιες υποχρεώσεις προστασίας δεδομένων μέσω (i) σύμβασης που θα συναφθεί μεταξύ του υπεργολάβου και του Αναδόχου ή (ii) άλλων νομικών μέσων του ευρωπαϊκού δικαίου προστασίας των δεδομένων, όπως έχουν επιβληθεί στον Ανάδοχο βάσει της παρούσας σύμβασης. Ειδικότερα, ο Ανάδοχος πρέπει να εξασφαλίσει ότι ο υπεργολάβος παρέχει επαρκείς εγγυήσεις, προκειμένου να λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα κατά τρόπον, ώστε η επεξεργασία προσωπικών δεδομένων να πραγματοποιείται σύμφωνα με τις απαιτήσεις του ΓΚΠΔ. Κατόπιν γραπτού αιτήματος του Πελάτη, ο Ανάδοχος θα παράσχει στον Πελάτη πληροφορίες σχετικά με το ουσιώδες περιεχόμενο της σύμβασης και την εφαρμογή των υποχρεώσεων προστασίας δεδομένων στην υπεργολαβική σχέση, εάν απαιτείται με εξέταση των σχετικών εγγράφων της σύμβασης. Ο Ανάδοχος δεν επιτρέπεται να αποκρύψει τους εμπορικούς όρους. Ο Πελάτης είναι υποχρεωμένος να διατηρεί το απόρρητο των πληροφοριών που έχει συγκεντρώσει.

6 Δικαίωμα ελέγχου

6.1 Ο Πελάτης έχει το δικαίωμα να ελέγξει ο ίδιος ή να αναθέσει τον έλεγχο της τήρησης των υποχρεώσεων που απορρέουν από την παρούσα σύμβαση σε διορισμένο κατάλληλο τρίτο μέρος (συμπεριλαμβανομένων των οδηγιών που έχουν εκδοθεί).

6.2 Ο Ανάδοχος θα παράσχει στον Πελάτη επαρκή υποστήριξη κατά τη διάρκεια των ελέγχων. Ειδικότερα, ο Ανάδοχος παρέχει πρόσβαση στις εγκαταστάσεις της επεξεργασίας δεδομένων και παρέχει τις απαραίτητες πληροφορίες.

6.3 Στην περίπτωση που ένας έλεγχος οδηγήσει στο συμπέρασμα ότι ο Ανάδοχος ή/και η επεξεργασία δεν συμμορφώνονται με τους όρους της παρούσας σύμβασης ή/και του Ευρωπαϊκού δικαίου περί προστασίας δεδομένων, ο Ανάδοχος θα λάβει όλα τα απαραίτητα διορθωτικά μέτρα για να εξασφαλίσει τη συμμόρφωση με τους όρους της παρούσας σύμβασης ή/και του Ευρωπαϊκού δικαίου περί προστασίας δεδομένων.

6.4 Το κόστος που προκύπτει για τον Πελάτη μέσω της διενέργειας ελέγχου, βαρύνει τον ίδιο. Το κόστος που προκύπτει για τον Ανάδοχο μέσω της διενέργειας ελέγχου από τον Πελάτη, μπορεί να το απαιτήσει από τον Πελάτη, εφόσον ο Πελάτης διενεργεί ή μπορεί να διενεργήσει έλεγχο περισσότερες από μία φορές ανά ημερολογιακό έτος.

6.5 Οι έλεγχοι του Αναδόχου πρέπει να ανακοινώνονται εγκαίρως και δεν επιτρέπεται να επηρεάζουν δυσανάλογα τις επιχειρηματικές δραστηριότητες του Αναδόχου.

7 Υποχρεώσεις ειδοποίησης

Ο Ανάδοχος ενημερώνει αμέσως τον Πελάτη εάν, κατά τη γνώμη του Αναδόχου, μια εντολή που δόθηκε από τον Πελάτη παραβιάζει το ευρωπαϊκό δίκαιο περί προστασίας δεδομένων. Η δικαίως αμφισβητούμενη εντολή δεν χρειάζεται να τηρηθεί, εκτός εάν δεν αλλάξει ή επιβεβαιωθεί ρητά από τον Πελάτη. Ο Ανάδοχος δεν υποχρεούται να ελέγχει ουσιαστικά τις εντολές.

Ο Ανάδοχος πρέπει να ενημερώνει καταλλήλως τον Πελάτη χωρίς καθυστέρηση, σε περίπτωση εντοπισμού σφαλμάτων ή παρατυπιών στην επεξεργασία δεδομένων ή υποψίας για παραβίαση της προστασίας των δεδομένων (συλλογικά, «**Συμβάν**»). Ο Πελάτης πρέπει να τεκμηριώσει το Συμβάν, συμπεριλαμβανομένων όλων των πραγματικών περιστάσεων, των αποτελεσμάτων τους και όλων των διορθωτικών μέτρων και, κατόπιν αιτήματος του Πελάτη, αυτές οι τεκμηριωμένες πληροφορίες πρέπει να διαβιβάζονται στον Πελάτη αμέσως εγγράφως ή ηλεκτρονικά.

8 Ευθύνη και απαλλαγή

8.1 Ο Ανάδοχος ευθύνεται για ζημίες που προκλήθηκαν από πρόθεση ή/και βαριά αμέλεια εκ μέρους του Αναδόχου ή των βοηθών εκπλήρωσης. Για ζημιές που βασίζονται σε απλή αμέλεια του Αναδόχου ή των βοηθών εκπλήρωσης, ο Ανάδοχος είναι υπεύθυνος μόνο αν παραβιάζεται μια βασική υποχρέωση. Οι βασικές υποχρεώσεις είναι ουσιαστικές συμβατικές υποχρεώσεις, που καθιστούν δυνατή τη δυνατότητα ορθής εφαρμογής της σύμβασης και στην εκπλήρωση των οποίων ο Πελάτης έχει εναποθέσει την εμπιστοσύνη του. Σε περίπτωση απλής αμέλειας σχετικά με την παραβίαση των εν λόγω βασικών υποχρεώσεων, η ευθύνη του Αναδόχου περιορίζεται στις τυπικά προβλεπόμενες ζημίες.

8.2 Ο Πελάτης απαλλάσσει τον Ανάδοχο από όλες τις αξιώσεις τρίτων μερών (συμπεριλαμβανομένων των ενδιαφερόμενων προσώπων ή/και των αρχών προστασίας δεδομένων), τις ζημίες και τα έξοδα λόγω παραβίασης από τον Πελάτη των διατάξεων της παρούσας σύμβασης ή/και του Ευρωπαϊκού δικαίου περί προστασίας δεδομένων. Αυτό δεν ισχύει αν ο Πελάτης δεν ευθύνεται για την παραβίαση ή αν ο Ανάδοχος συνέβαλε στην παραβίαση.

9 Διάρκεια ισχύος

Η διάρκεια ισχύος της παρούσας σύμβασης αντιστοιχεί στη διάρκεια ισχύος της Κύριας σύμβασης. Με τη λήξη της Κύριας σύμβασης για οποιονδήποτε λόγο, η παρούσα σύμβαση τερματίζεται αυτόματα. Η καταγγελία για σημαντικό λόγο παραμένει ανεπηρέαστη.

10 Λοιπά

10.1 Οι υπηρεσίες του Αναδόχου βάσει της παρούσας σύμβασης αντισταθμίζονται από τη ρύθμιση περί αποζημίωσης που καθορίζεται στην Κύρια σύμβαση.

10.2 Εάν τα προσωπικά δεδομένα του Πελάτη τίθενται σε κίνδυνο από τον Ανάδοχο λόγω μέτρων τρίτων μερών (π.χ. κατάσχεση ή δήμευση), λόγω διαδικασίας πτώχευσης ή διακανονισμού ή από άλλα παρόμοια συμβάντα, ο Ανάδοχος πρέπει να ενημερώνει αμέσως τον Πελάτη.

10.3 Σε περίπτωση που μεμονωμένες διατάξεις της παρούσας σύμβασης είναι ή καταστούν αναποτελεσματικές, αυτό δεν επηρεάζει την εγκυρότητα των υπόλοιπων διατάξεων. Σε περίπτωση αναποτελεσματικότητας μιας ρήτρας, τα Συμβαλλόμενα μέρη συμφωνούν σε έναν εναλλακτικό κανονισμό που βασίζεται στο πραγματικό και οικονομικό επίπεδο του σκοπού της σύμβασης.

10.4 Σε περίπτωση αποχώρησης της Μεγάλης Βρετανίας από την Ευρωπαϊκή Ένωση, ο Ανάδοχος υποχρεούται να ολοκληρώσει όλες τις συμφωνίες και να εκτελέσει όλες τις απαραίτητες ενέργειες, προκειμένου να επιτρέψει την επεξεργασία δεδομένων στη Μεγάλη Βρετανία βάσει του αντικειμένου της σύμβασης από την ημερομηνία απόσυρσης, σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων. Στο βαθμό που, κατά τη στιγμή της αποχώρησης, δεν υπάρχει θετική απόφαση καταλληλότητας από την Ευρωπαϊκή Επιτροπή, υπό το σημερινό πρίσμα πρόκειται ιδιαίτερα για τυποποιημένες ρήτρες προστασίας δεδομένων βάσει του άρθρου 46 παρ. 2 γ) για τη διαβίβαση προσωπικών δεδομένων σε υπεύθυνους επεξεργασίας, οι οποίοι είναι εγκατεστημένοι σε τρίτες χώρες, όπου δεν εξασφαλίζεται επαρκές επίπεδο προστασίας.

Εάν ο Ανάδοχος δεν ανταποκριθεί σε αυτές τις υποχρεώσεις, ο Πελάτης δικαιούται να απαιτήσει από τον Ανάδοχο, με ισχύ από τη στιγμή της αποχώρησης της Μεγάλης Βρετανίας από την Ευρωπαϊκή Ένωση, να παρασχεθούν οι σχετικές υπηρεσίες από μια συνδεδεμένη επιχείρηση ή τμήμα συνδεδεμένης επιχείρησης με μόνιμη έδρα στο έδαφος της Ευρωπαϊκής Ένωσης, χωρίς ο Πελάτης να επιβαρύνεται με πρόσθετα έξοδα ή δαπάνες.

10.5 Η παρούσα Σύμβαση επεξεργασίας δεδομένων διατίθεται σε 18 γλωσσικές εκδόσεις, όπου η γερμανική αρχική έκδοση έχει προτεραιότητα σε περίπτωση αποκλίσεων.

10.6 Η παρούσα σύμβαση υπόκειται στη νομοθεσία της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, με εξαίρεση τον νόμο περί πωλήσεων των Ηνωμένων Εθνών. Αποκλειστική δικαιοδοσία είναι το Μόναχο.

10.7 Τα ακόλουθα παραρτήματα αποτελούν μέρος της σύμβασης:

Παράρτημα 1 – Περιγραφή της επεξεργασίας προσωπικών δεδομένων
Παράρτημα 2 – Τεχνικά και οργανωτικά μέτρα

ΠΑΡΑΡΤΗΜΑ 1 – Περιγραφή της επεξεργασίας προσωπικών δεδομένων

1 Κύρια σύμβαση

Η Κύρια σύμβαση υπό την έννοια του εδαφίου 2.1 του κύριου μέρους της σύμβασης είναι οι «Γενικές προϋποθέσεις για τη χρήση της πλατφόρμας».

Τίτλος / Συμβαλλόμενα μέρη: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 Μόναχο / **Χρήστης**

2 Αντικείμενο και διάρκεια της σύμβασης

Το αντικείμενο της εντολής προκύπτει από το εδάφιο 1 (*Αντικείμενο*) και το εδάφιο 8 (*Δεδομένα του χρήστη και προστασία δεδομένων*) της Κύριας σύμβασης. Η διάρκεια της εντολής προκύπτει από το εδάφιο 7 (*Σύναψη σύμβασης, διάρκεια σύμβασης και δικαιώματα καταγγελίας*) της Κύριας σύμβασης.

3 Πεδίο εφαρμογής, φύση και σκοπός της επεξεργασίας δεδομένων / των μέτρων επεξεργασίας δεδομένων

Το πεδίο εφαρμογής, η φύση και ο σκοπός της επεξεργασίας προσωπικών δεδομένων προκύπτουν από το εδάφιο 8 της Κύριας σύμβασης.

Λεπτομερής περιγραφή του αντικειμένου της εντολής, όσον αφορά το πεδίο εφαρμογής, τη φύση και τον σκοπό:

Για να καταστεί δυνατή η παροχή υπηρεσιών τις οποίες προσφέρει ο Ανάδοχος (όπως ορίζεται στην Κύρια σύμβαση), ο Ανάδοχος πρέπει να συλλέγει τα προσωπικά δεδομένα του Πελάτη μέσω συνδεδεμένων οχημάτων ή κινητών συσκευών, στο βαθμό που απαιτείται για την παροχή των υπηρεσιών (και, ενδεχομένως, προσωπικά δεδομένα που μεταφέρονται από τρίτο μέρος, με το οποίο ο χρήστης έχει συμφωνήσει υπηρεσίες τρίτων), και να τα μεταφέρει και να τα αποθηκεύει στην πλατφόρμα του Αναδόχου. Ο Ανάδοχος θα επεξεργαστεί τα δεδομένα που είναι αποθηκευμένα στην πλατφόρμα, στον βαθμό που είναι απαραίτητο για την παροχή της υπηρεσίας (για παράδειγμα, για να αναλύσει και να αξιολογήσει την οδηγική συμπεριφορά των οδηγών και τη χρήση του συνδεδεμένου οχήματος ή της κινητής συσκευής με βάση τα προσωπικά δεδομένα, και να υποβάλει στον Πελάτη προσφορές προσαρμοσμένες ειδικά σε αυτόν, όπως εκπαίδευση οδηγών, λεπτομέρειες εξοπλισμού και προτάσεις για αύξηση της απόδοσης). Το ακριβές πεδίο εφαρμογής, η φύση και ο σκοπός προκύπτουν ιδίως από τις πρόσθετες ατομικές συμβάσεις που πρόκειται να συναφθούν.

4 Κύκλος ενδιαφερόμενων ατόμων (κατηγορίες ενδιαφερόμενων ατόμων)

Η επεξεργασία προσωπικών δεδομένων αφορά τις ακόλουθες ομάδες ατόμων:

- **Οδηγοί και άλλοι εργαζόμενοι** (εργαζόμενοι της ίδιας της εταιρείας του Πελάτη), π.χ. *εργαζόμενοι, μαθητευόμενοι, υποψήφιοι, πρώην υπάλληλοι.*

- **Οδηγοί** οι οποίοι δεν είναι υπάλληλοι.
- **Άτομα επικοινωνίας** φορτωτών/εκφορτωτών ή άλλοι εταίροι του Πελάτη, και
- **Εργαζόμενοι του ομίλου** (υπάλληλοι άλλης εταιρείας του ομίλου του Πελάτη).

5 Φύση των προσωπικών δεδομένων

Η επεξεργασία προσωπικών δεδομένων περιλαμβάνει τους ακόλουθους τύπους προσωπικών δεδομένων:

- Όνομα του οδηγού και αριθμό αναγνώρισης οδηγού
- Αριθμός πλαισίου οχήματος
- Δεδομένα θέσης
- Δεδομένα για τους χρόνους οδήγησης και ανάπαυσης
- Δεδομένα για την οδική συμπεριφορά
- Δεδομένα για την κατάσταση του συνδεδεμένου οχήματος
- Δεδομένα για την κατάσταση του ρυμουλκούμενου
- Δεδομένα για την κατάσταση των υπερκατασκευών και των παραρτημάτων, των συγκροτημάτων και άλλων κατασκευαστικών στοιχείων του οχήματος
- Δεδομένα για την κατάσταση τυχόν συνδεδεμένων συσκευών IOT
- Δεδομένα για την κατάσταση των κινητών συσκευών
- Δεδομένα φορτίου
- Δεδομένα εντολών και
- Στοιχεία επικοινωνίας των αρμόδιων ατόμων επικοινωνίας φορτωτών/εκφορτωτών ή άλλων εταίρων του Πελάτη.

6 Τεκμηριωμένες οδηγίες

Δια του παρόντος, ο Πελάτης παρέχει εντολή στον Ανάδοχο να επεξεργαστεί τα προσωπικά δεδομένα, όπως προβλέπεται στο εδάφιο 8 της Κύριας σύμβασης. Αυτό περιλαμβάνει ειδικότερα την ακόλουθη επεξεργασία:

- Τα προσωπικά δεδομένα διαβιβάζονται μέσω του συνδεδεμένου οχήματος ή της κινητής συσκευής στην πλατφόρμα που βασίζεται στο cloud του Αναδόχου και αποθηκεύονται εκεί.
- Τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία σύμφωνα με την παρούσα σύμβαση, μόνο εφόσον απαιτείται για την εκπλήρωση της Κύριας σύμβασης. Το εδάφιο 8.3.4 της Κύριας σύμβασης παραμένει ανεπηρέαστο.
- Ο Ανάδοχος διαβιβάζει τα προσωπικά δεδομένα σε τρίτο πάροχο (όπως ορίζεται στην Κύρια Σύμβαση), εφόσον και στον βαθμό που η διαβίβαση στον τρίτο πάροχο απαιτείται για την παροχή των υπηρεσιών τρίτων προς τον Πελάτη (όπως ορίζονται στην Κύρια σύμβαση).
- Ο Ανάδοχος θα αναλύσει και θα αξιολογήσει την οδηγική συμπεριφορά των οδηγών και τη χρήση του συνδεδεμένου οχήματος, με βάση τα προσωπικά δεδομένα, και θα υποβάλει στον Πελάτη προσφορές προσαρμοσμένες ειδικά σε αυτόν, όπως εκπαίδευση οδηγών, λεπτομέρειες εξοπλισμού και προτάσεις για αύξηση της απόδοσης.

7 Τόπος επεξεργασίας

- Γερμανία.
- Ηνωμένο Βασίλειο. Εφόσον για τα δεδομένα που υποβάλλονται σε επεξεργασία για σκοπούς IT Hosting και/ή υποστήριξης IT εντός της Ευρωπαϊκής Ένωσης, έχουν συναφθεί αντίστοιχες συμβάσεις επεξεργασίας δεδομένων.
- Εφόσον ο Ανάδοχος χρησιμοποιεί υπεργολάβους εκτός Ευρωπαϊκής Ένωσης για σκοπούς IT Hosting και/ή υποστήριξης IT (βλ. εδάφιο 8 του παρόντος Παραρτήματος 1), η διαβίβαση προσωπικών δεδομένων πραγματοποιείται βάσει των τυποποιημένων συμβατικών ρητρών / τυποποιημένων ρητρών προστασίας δεδομένων που συνάπτονται μεταξύ του Αναδόχου και του υπεργολάβου για τη διαβίβαση προσωπικών δεδομένων σε υπεύθυνους επεξεργασίας, οι οποίοι βρίσκονται εγκατεστημένοι σε τρίτες χώρες, κατά το άρθρο 46, παρ. 2 γ) του ΓΚΠΔ.

8 Υπεργολάβος

Ο Ανάδοχος χρησιμοποιεί τους ακόλουθους υπεργολάβους (οι οποίοι ενδεχομένως μπορούν να χρησιμοποιήσουν επιπλέον υπεργολάβους):

Αρ.	υπεργολάβων (εταιρεία, διεύθυνση, άτομο επικοινωνίας)	Κατηγορίες δεδομένων που υποβάλλονται σε επεξεργασία	Βήματα επεξεργασίας / σκοπός της επεξεργασίας δεδομένων υπεργολάβων
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Όλα τα προσωπικά δεδομένα της πλατφόρμας που σχετίζονται με το Τμήμα πωλήσεων (δηλ. το μέρος όπου ένας πελάτης μπορεί να εγγραφεί στην πλατφόρμα και να πραγματοποιήσει παραγγελίες)	Φιλοξενία πλατφόρμας
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Όλα τα προσωπικά δεδομένα της πλατφόρμας που σχετίζονται με το Τμήμα πωλήσεων (δηλ. το μέρος όπου ένας πελάτης μπορεί να εγγραφεί στην πλατφόρμα και να πραγματοποιήσει παραγγελίες)	Υποστήριξη IT σχετικά με την πλατφόρμα
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 ΗΠΑ https://aws.amazon.com/de/compliance/contact/	Όλα τα άλλα προσωπικά δεδομένα χρήστη, που διαβιβάζονται στον Ανάδοχο μέσω του οχήματος	Φιλοξενία πλατφόρμας / Υποστήριξη IT σχετικά με τη φιλοξενία πλατφόρμας
4	Εάν χρειαστεί, μελλοντικά αντί του αρ. 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 ΗΠΑ https://aws.amazon.com/de/compliance/contact/	Όλα τα άλλα προσωπικά δεδομένα χρήστη, που διαβιβάζονται στον Ανάδοχο μέσω του οχήματος	Φιλοξενία πλατφόρμας

5	MAN Service und Support GmbH Dachauer Straße 667 80995 München Γερμανία	Όλα τα προσωπικά δεδομένα που απαιτούνται για την επεξεργασία των αιτημάτων των πελατών στο πλαίσιο της υποστήριξης 1ου και 2ου επιπέδου	1st Level Support
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 ΗΠΑ	Όλα τα προσωπικά δεδομένα που απαιτούνται για την επεξεργασία της τιμολόγησης / επεξεργασίας των εντολών	Φιλοξενία πλατφόρμας (EU Tenant – Gehosted by Amazon Web Services (EU) – βλ. εδάφιο 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Γερμανία	Όλα τα άλλα προσωπικά δεδομένα χρήστη, που διαβιβάζονται στον Ανάδοχο μέσω του συνδεδεμένου οχήματος και/ή της κινητής συσκευής	Φιλοξενία πλατφόρμας
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Γερμανία	Όλα τα άλλα προσωπικά δεδομένα χρήστη, που διαβιβάζονται στον Ανάδοχο μέσω του οχήματος TBM1/2	Φιλοξενία πλατφόρμας
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Σουηδία	Όλα τα άλλα προσωπικά δεδομένα χρήστη, που διαβιβάζονται στον Ανάδοχο μέσω του οχήματος	Φιλοξενία πλατφόρμας
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Γερμανία	Όλα τα άλλα προσωπικά δεδομένα χρήστη, που διαβιβάζονται στον Ανάδοχο μέσω του οχήματος	Φιλοξενία πλατφόρμας

ΠΑΡΑΡΤΗΜΑ 2 – Τεχνικά και οργανωτικά μέτρα
Τα τεχνικά και οργανωτικά μέτρα που πρέπει να λάβει ο Ανάδοχος για τη διασφάλιση ενός κατάλληλου επιπέδου προστασίας από τον κίνδυνο περιγράφονται στην προσέγγιση για την προστασία των δεδομένων της πλατφόρμας RIO και περιλαμβάνουν ιδιαίτερα τα εξής:

1. Ψευδωνυμοποίηση

Όσον αφορά τα προσωπικά δεδομένα που χρησιμοποιούνται για σκοπούς αξιολόγησης, οι οποίοι είναι επίσης εφικτοί με ψευδωνυμοποιημένα δεδομένα, χρησιμοποιούνται τεχνικές ψευδωνυμοποίησης. Αρχικά, καθορίζεται εκ των προτέρων για κάθε πεδίο δεδομένων αν πρέπει να ψευδωνυμοποιηθεί, καθώς θα καθιστούσε δυνατή την εξαγωγή συμπερασμάτων για ένα άτομο. Τα κλειδιά ψευδωνυμοποίησης αποθηκεύονται σε ένα «Data Safe», για το οποίο έχει ρυθμιστεί ο μέγιστος δυνατός περιορισμός πρόσβασης.

2. Κρυπτογράφηση

Τα κινητά τερματικά επικοινωνούν κρυπτογραφημένα με το τελικό σημείο, χρησιμοποιώντας ένα ειδικό για τη συσκευή πιστοποιητικό συσκευής. Τα δεδομένα μεταφέρονται στη συνέχεια σε κρυπτογραφημένη μορφή μέσα στην πλατφόρμα RIO («Ubiquitous encryption» ή «encryption everywhere»).

3. Εξασφάλιση της εμπιστευτικότητας

Όλοι οι εργαζόμενοι λαμβάνουν και θα λαμβάνουν υποδείξεις σχετικά με τις υποχρεώσεις εμπιστευτικότητάς τους και δεσμεύονται εγγράφως για το απόρρητο των δεδομένων.

Η χρησιμοποιούμενη υποδομή IT που παρέχεται από την Amazon Web Services (εφεξής AWS) στο πλαίσιο ενός Cloud (IaaS & PaaS). Ο έλεγχος πρόσβασης παρέχεται από τον χειριστή του Data Center της AWS: Τα κέντρα επεξεργασίας δεδομένων υψηλής ασφάλειας της AWS χρησιμοποιούν σύγχρονα μέτρα ηλεκτρονικής παρακολούθησης και πολυεπίπεδα συστήματα ελέγχου πρόσβασης. Τα κέντρα επεξεργασίας δεδομένων στελεχώνονται όλο το εικοσιτετράωρο με εκπαιδευμένο προσωπικό ασφαλείας και η πρόσβαση εξασφαλίζεται αυστηρά σύμφωνα με την αρχή των ελάχιστων δικαιωμάτων και αποκλειστικά για τον σκοπό της διαχείρισης του συστήματος.

Η πρόσβαση στα εξαρτήματα υλικού (προγράμματα-πελάτες) της TTB Digital Services GmbH πραγματοποιείται σύμφωνα με τα εκάστοτε ισχύοντα κατάλληλα τυπικά μέτρα, κατά περίπτωση. Αυτά περιλαμβάνουν π.χ. περιορισμούς πρόσβασης μέσω συστημάτων διαχωρισμού (κόμβων), συστήματα παρακολούθησης βίντεο, συστήματα συναγερμού ή/και επιτήρησης, ηλεκτρονικά ή μηχανικά ασφαλισμένες πόρτες, κτίρια με προστασία από διάρρηξη, τεκμηριωμένες άδειες πρόσβασης (επισκέπτες, εξωτερικό προσωπικό) ή δηλωμένες ασφαλείς περιοχές.

Οι έλεγχοι πρόσβασης περιλαμβάνουν μέτρα για την ασφάλεια των συσκευών, την ασφάλεια δικτύου και την ασφάλεια εφαρμογών.

Διάφορα μέτρα εφαρμόζονται ως μέτρα προστασίας συσκευών στο όχημα: Τα κινητά τερματικά είναι μόνιμα εγκατεστημένα στο όχημα και διαθέτουν Secure Boot (ασφαλή εκκίνηση), δηλ. δεν υπάρχει

δυνατότητα φόρτωσης και εκκίνησης ενός ξένου λειτουργικού συστήματος. Τα κινητά τερματικά επικοινωνούν κρυπτογραφημένα με το τελικό σημείο, χρησιμοποιώντας ένα ειδικό για τη συσκευή πιστοποιητικό συσκευής. Τα δεδομένα μεταφέρονται στη συνέχεια σε κρυπτογραφημένη μορφή μέσα στην πλατφόρμα RIO («Ubiquitous encryption» ή «encryption everywhere»). Τα τερματικά ενημερώνονται στην τρέχουσα κατάσταση ασφαλείας μέσω της τακτικής εγκατάστασης ενημερώσεων ασφαλείας (patch management - διαχείριση διορθώσεων).

Ως μέτρα ασφάλειας δικτύων εφαρμόζονται επίσης διάφορα τυπικά μέτρα: Εφαρμόζονται οι κατάλληλες (σύμφωνα με την τρέχουσα τεχνολογία) προδιαγραφές κωδικού πρόσβασης (μήκος, πολυπλοκότητα, διάρκεια ισχύος κωδικού πρόσβασης, κ.λπ.). Η επαναλαμβανόμενη εσφαλμένη εισαγωγή του συνδυασμού ονόματος χρήστη/κωδικού πρόσβασης οδηγεί σε (προσωρινό) κλείδωμα του ονόματος χρήστη. Το εταιρικό δίκτυο προστατεύεται με ένα τείχος προστασίας έναντι μη ασφαλών ανοικτών δικτύων. Δημιουργείται μια διαδικασία που εξασφαλίζει την τακτική παροχή στις κινητές συσκευές με ενημερώσεις ασφαλείας (διαδικασία OTA). Για την αποκάλυψη ή αποφυγή επιθέσεων στο εταιρικό δίκτυο (Intranet), χρησιμοποιούνται οι κατάλληλες τεχνολογίες (π.χ. συστήματα ανίχνευσης εισβολής). Οι εργαζόμενοι ευαισθητοποιούνται τακτικά σχετικά με τους κινδύνους.

Ως μέτρα για την ασφάλεια των εφαρμογών, εφαρμόζονται ορισμένα τυπικά μέτρα:

Οι σχετικές εφαρμογές προστατεύονται από μη εξουσιοδοτημένη πρόσβαση με κατάλληλους μηχανισμούς επαλήθευσης και έγκρισης. Εφαρμόζονται οι κατάλληλες (σύμφωνα με την τρέχουσα τεχνολογία) προδιαγραφές κωδικού πρόσβασης (μήκος, πολυπλοκότητα, διάρκεια ισχύος κωδικού πρόσβασης, κ.λπ.). Για εφαρμογές με ειδικές ανάγκες προστασίας, χρησιμοποιούνται ισχυροί μηχανισμοί επαλήθευσης (π.χ. token, PKI). Η επαναλαμβανόμενη εσφαλμένη εισαγωγή του συνδυασμού ονόματος χρήστη/κωδικού πρόσβασης οδηγεί σε (προσωρινό) κλείδωμα του ονόματος χρήστη. Τα δεδομένα που χρησιμοποιούνται στη σχετική διαδικασία αποθηκεύονται σε κρυπτογραφημένη μορφή σε ένα φορητό μέσο αποθήκευσης δεδομένων. Οι επιτυχείς προσβάσεις και οι προσπάθειες πρόσβασης στις εφαρμογές καταγράφονται. Τα αρχεία καταγραφής που δημιουργούνται διατηρούνται για κατάλληλη χρονική περίοδο (τουλάχιστον 90 ημέρες) και ελέγχονται (δειγματοληπτικά).

Τα δικαιώματα χρήστη (για πρόσβαση) εξασφαλίζονται με διάφορα μέτρα, τα οποία εκχωρούνται ουσιαστικά σε συγκεκριμένο άτομο. Η ανάθεση των δικαιωμάτων αποτελεί ευθύνη του διαχειριστή της πλατφόρμας και ελέγχεται τακτικά. Η χορήγηση των δικαιωμάτων πρόσβασης πραγματοποιείται μόνο μετά από μια καθορισμένη και τεκμηριωμένη διαδικασία. Οι αλλαγές στα δικαιώματα πρόσβασης πραγματοποιούνται σύμφωνα με την αρχή του διπλού ελέγχου και τεκμηριώνονται σε ένα αρχείο καταγραφής με έλεγχο έκδοσης.

Ως μέτρα για τον έλεγχο/τη ρύθμιση πρόσβασης εφαρμόζονται διάφορα μέτρα: Τα δικαιώματα πρόσβασης ορίζονται και τεκμηριώνονται στο πλαίσιο μιας έννοιας ρόλων/εξουσιοδότησης και εκχωρούνται στους αντίστοιχους ρόλους, σύμφωνα με τις απαιτήσεις που σχετίζονται με την εργασία. Για τεχνικούς διαχειριστές έχουν οριστεί συγκεκριμένοι ρόλοι/δικαιώματα (τα οποία, στο μέτρο που είναι τεχνικά δυνατό, δεν επιτρέπουν την πρόσβαση σε προσωπικά δεδομένα). Ρυθμίζονται συγκεκριμένοι ρόλοι/δικαιώματα για την τεχνική υποστήριξη (τα οποία δεν περιέχουν τεχνικά δικαιώματα διαχείρισης).

Ο ορισμός των ρόλων/δικαιωμάτων και η ανάθεση ρόλων/δικαιωμάτων δεν πραγματοποιείται, στο μέτρο που είναι τεχνικά και οργανωτικά δυνατό, από τα ίδια πρόσωπα, αλλά με διαδικασία ελέγχου (έγκρισης) και περιορίζεται χρονικά. Η άμεση πρόσβαση στη βάση δεδομένων παρακάμπτοντας την έννοια των ρόλων/δικαιωμάτων είναι δυνατή μόνο από εξουσιοδοτημένους διαχειριστές βάσεων δεδομένων. Υπάρχει κανονισμός για τη χρήση ιδιωτικών μέσων αποθήκευσης δεδομένων ή την απαγόρευση της χρήσης ιδιωτικών μέσων αποθήκευσης δεδομένων. Υπάρχουν δεσμευτικοί κανονισμοί σχετικά με την πρόσβαση σε δεδομένα κατά την εξωτερική συντήρηση, την απομακρυσμένη συντήρηση και τηλεργασία. Εκτελείται κατάλληλη καταστροφή/απόρριψη των εγγράφων και των μέσων αποθήκευσης δεδομένων, σύμφωνα με τους κανονισμούς για την προστασία των δεδομένων (όπως καταστροφείς εγγράφων, κάδος προστασίας δεδομένων) από αξιόπιστες εταιρείες διαχείρισης απορριμμάτων.

Η έννοια των ρόλων/δικαιωμάτων προσαρμόζεται τακτικά στις μεταβαλλόμενες δομές οργάνωσης της εργασίας (π.χ., νέοι ρόλοι) και οι εκχωρημένοι ρόλοι / τα δικαιώματα ελέγχονται τακτικά (π.χ., από τον προϊστάμενο) και, εφόσον απαιτηθεί, προσαρμόζονται ή ανακαλούνται. Υπάρχει ένας τακτικός κεντρικός έλεγχος, όσον αφορά τα εκχωρημένα τυπικά προφίλ. Οι αλλαγές πρόσβασης (εγγραφή, διαγραφή) καταγράφονται και τα αρχεία καταγραφής που δημιουργούνται διατηρούνται για κατάλληλη χρονική περίοδο (τουλάχιστον 90 ημερών) και ελέγχονται (δειγματοληπτικά).

Ως γενικά μέτρα για την ασφάλεια της διαβίβασης, εφαρμόζονται διάφορα τυπικά μέτρα:

Τα πρόσωπα στα οποία έχει ανατεθεί η διαβίβαση θα ενημερώνονται εκ των προτέρων για τα μέτρα ασφαλείας που πρέπει να ληφθούν. Ο κύκλος των παραληπτών καθορίζεται εκ των προτέρων, έτσι ώστε να είναι δυνατός ο αντίστοιχος έλεγχος (επαλήθευση ταυτότητας). Η συνολική διαδικασία μεταφοράς δεδομένων έχει καθοριστεί και τεκμηριωθεί και η υλοποίηση της συγκεκριμένης μεταφοράς δεδομένων καταγράφεται ή τεκμηριώνεται (π.χ., επιβεβαίωση παραλαβής, απόδειξη). Τα πρόσωπα στα οποία έχει ανατεθεί η διαβίβαση διενεργούν εκ των προτέρων έναν έλεγχο αξιοπιστίας, πληρότητας και ορθότητας.

Πριν από την εκτέλεση της συγκεκριμένης μεταφοράς δεδομένων, πραγματοποιείται έλεγχος της διεύθυνσης του παραλήπτη (π.χ. διεύθυνση ηλεκτρονικού ταχυδρομείου). Η μεταφορά των δεδομένων μέσω του Διαδικτύου πραγματοποιείται σε κρυπτογραφημένη μορφή (π.χ. κρυπτογράφηση αρχείων). Η ακεραιότητα των μεταφερθέντων δεδομένων διασφαλίζεται, στον βαθμό που είναι τεχνικά εφικτό, με τη χρήση διαδικασιών υπογραφής (ψηφιακή υπογραφή). Τα ηλεκτρονικά αποδεικτικά παραλαβής αρχειοθετούνται σε κατάλληλη μορφή. Οι ανεπιθύμητες διαβιβάσεις δεδομένων στο Διαδίκτυο αποτρέπονται με κατάλληλες τεχνολογίες (π.χ. διακομιστής μεσολάβησης, τείχος προστασίας).

Επιπλέον, εφαρμόζονται τα ακόλουθα τυπικά μέτρα ως μέτρα για την εκτέλεση της απαίτησης διαχωρισμού:

Υπάρχουν δεσμευτικοί κανονισμοί σχετικά με τον περιορισμό του σκοπού της επεξεργασίας, για τη συμμόρφωση με την απαίτηση διαχωρισμού. Τα δεδομένα που συλλέγονται για συγκεκριμένους σκοπούς αποθηκεύονται χωριστά από τα δεδομένα που συλλέγονται για άλλους σκοπούς. Τα χρησιμοποιούμενα συστήματα IT επιτρέπουν την ξεχωριστή αποθήκευση δεδομένων (μέσω της δυνατότητας πολλαπλών προγραμμάτων-πελατών ή εννοιών πρόσβασης). Πραγματοποιείται διαχωρισμός των δεδομένων σε δοκιμαστικά και παραγωγικά συστήματα. Για τα ψευδωνυμοποιημένα δεδομένα, η γέφυρα-κλειδί, η οποία

επιτρέπει την επαναπροσδιορισιμότητα, αποθηκεύεται ή διατηρείται χωριστά. Κατά την επεξεργασία προσωπικών δεδομένων ή τη μεταφορά λειτουργιών, διενεργείται ξεχωριστή επεξεργασία των δεδομένων διαφόρων πελατών από τον Ανάδοχο. Οι υπάρχουσες έννοιες ρόλων/δικαιωμάτων επιτρέπουν τον λογικό διαχωρισμό των επεξεργασμένων δεδομένων μέσω της διαμόρφωσής τους.

4. Εξασφάλιση της ακεραιότητας

Ως μέτρα για την εκτέλεση της καταγραφής δεδομένων, εφαρμόζονται διάφορα τυπικά μέτρα:

Καταγραφή των αλλαγών στα δικαιώματα πρόσβασης καθώς και σε όλες τις δραστηριότητες διαχειριστή. Καταγραφή προσβάσεων εγγραφής (εισαγωγή δεδομένων, αλλαγές, διαγραφές) και αλλαγών στα πεδία δεδομένων (π.χ. περιεχόμενο του νέου εισηγμένου ή τροποποιημένου αρχείου). Καταγραφή των διαβιβάσεων (π.χ. λήψη) και καταγραφή σύνδεσης.

Τα χρησιμοποιημένα έγγραφα καταγραφής τεκμηριώνονται και αρχειοθετούνται για την ιχνηλασιμότητα των καταχωρίσεων. Η καταγραφή πραγματοποιείται με την ημερομηνία και ώρα, τον χρήστη, τον τύπο δραστηριότητας, το πρόγραμμα εφαρμογής και τον αριθμό παραγγελίας του συνόλου δεδομένων. Οι ρυθμίσεις καταγραφής τεκμηριώνονται.

Επιτρέπεται αποκλειστικά η πρόσβαση με δυνατότητα ανάγνωσης στα αρχεία καταγραφής. Το εύρος των δικαιούχων πρόσβασης σε αρχεία καταγραφής είναι περιορισμένο (π.χ. στον διαχειριστή, τον υπεύθυνο προστασίας δεδομένων, τον ελεγκτή). Τα αρχεία καταγραφής διατηρούνται για συγκεκριμένο χρονικό διάστημα (π.χ. 1 έτος) και, στη συνέχεια, διαγράφονται σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων. Τα αρχεία καταγραφής αξιολογούνται αυτοματοποιημένα σε τακτική βάση. Οι αξιολογήσεις των αρχείων καταγραφής δημιουργούνται στο μέτρο του δυνατού σε ψευδωνυμοποιημένη μορφή.

5. Εξασφάλιση της διαθεσιμότητας

Η αρχιτεκτονική προστατεύεται καθαυτή από την απώλεια δεδομένων μέσω εσωτερικών μηχανισμών αναπαραγωγής στο εσωτερικό της πλατφόρμας AWS. Επιπλέον, εφαρμόζονται τα ακόλουθα τυπικά μέτρα της AWS ως μέτρα της προστασίας αντικειμένου:

Εφαρμόζονται μέτρα πυροπροστασίας (π.χ. πυροστεγείς θύρες, ανιχνευτές καπνού, πυροφραγμοί, απαγόρευση καπνίσματος). Οι εγκαταστάσεις υπολογιστών προστατεύονται από πλημμύρες (π.χ. αίθουσα υπολογιστών στον 1ο όροφο, ανιχνευτής νερού). Εφαρμόζονται μέτρα για την αποφυγή κραδασμών (π.χ. η αίθουσα υπολογιστών δεν βρίσκεται κοντά σε εθνικές οδούς, σιδηροδρομικές γραμμές, μηχανοστάσια). Οι εγκαταστάσεις υπολογιστών προστατεύονται από ηλεκτρομαγνητικά πεδία (π.χ. χαλύβδινα ελάσματα σε εξωτερικούς τοίχους). Εφαρμόζονται μέτρα κατά των βανδαλισμών και της κλοπής (πρβλ. έλεγχο πρόσβασης). Οι εγκαταστάσεις υπολογιστών βρίσκονται σε κλιματιζόμενους χώρους (η θερμοκρασία και η υγρασία ελέγχονται από σύστημα κλιματισμού). Οι εγκαταστάσεις υπολογιστών προστατεύονται από αιχμές υπέρτασης με προστασία από υπέρταση. Εφαρμόζονται μέτρα για την εξασφάλιση συνεχούς τροφοδοσίας ρεύματος χαμηλού θορύβου (π.χ. UPS, εφεδρικές γεννήτριες).

Οι βάσεις δεδομένων προστατεύονται τακτικά με τη μορφή αντιγράφων ασφαλείας εντός της πλατφόρμας AWS. Η έννοια της δημιουργίας αντιγράφων ασφαλείας τεκμηριώνεται, αναθεωρείται και ενημερώνεται τακτικά. Τα εφεδρικά μέσα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Τα χρησιμοποιούμενα εφεδρικά προγράμματα συμμορφώνονται με τα ισχύοντα πρότυπα ποιότητας και ενημερώνονται τακτικά σχετικά με αυτό το θέμα. Έχει δημιουργηθεί ένα εφεδρικό κέντρο επεξεργασίας δεδομένων (μακριά από τον τόπο επεξεργασίας) και μπορεί να συνεχίσει να επεξεργάζεται δεδομένα σε περίπτωση καταστροφής. Τα διάφορα μέτρα ελέγχου διαθεσιμότητας τεκμηριώνονται σε ένα σχέδιο διαχείρισης έκτακτης ανάγκης της AWS.

Πριν από την ανάθεση εντολής για επεξεργασία δεδομένων, ο Ανάδοχος ελέγχεται προσεκτικά και σύμφωνα με τα καθορισμένα κριτήρια (τεχνικά και οργανωτικά μέτρα). Για αυτό, απαιτείται και ελέγχεται ιδιαίτερα η λεπτομερής περιγραφή των τεχνικών/οργανωτικών μέτρων προστασίας δεδομένων που εφαρμόζει ο Ανάδοχος (απάντηση σε ερωτηματολόγιο ή έννοια της προστασίας δεδομένων). Ανάλογα με την ποσότητα και την ευαισθησία των επεξεργασμένων δεδομένων, αυτός ο έλεγχος πραγματοποιείται επίσης επιτόπου από τον Ανάδοχο. Οι κατάλληλες πιστοποιήσεις (π.χ. ISO 27001) λαμβάνονται υπόψη κατά την επιλογή των Αναδόχων. Ο προσδιορισμός της καταλληλότητας του Αναδόχου τεκμηριώνεται σε κατάλληλη και κατανοητή μορφή.

Για την αιτιολόγηση της σχέσης συνεργασίας, συνάπτεται μια Σύμβαση επεξεργασίας δεδομένων μεταξύ του Πελάτη και του Αναδόχου. Αυτή διευκρινίζει λεπτομερώς και εγγράφως τις αρμοδιότητες και τις ευθύνες καθώς και τα καθήκοντα και των δύο συμβαλλόμενων μερών. Σε περίπτωση που ένας εντεταλμένος πάροχος υπηρεσιών εδρεύει εκτός της ΕΕ ή του ΕΟΧ, εφαρμόζονται οι τυποποιημένες συμβατικές ρήτρες της ΕΕ. Σύμφωνα με τη σύμβαση, η επεξεργασία δεδομένων από τον Ανάδοχο μπορεί να πραγματοποιηθεί μόνο σύμφωνα με τις οδηγίες του Πελάτη. Ο Ανάδοχος υποχρεούται να ενημερώσει τον Πελάτη αμέσως εάν μία από τις οδηγίες του, κατά τη γνώμη του Αναδόχου, παραβιάζει τους κανονισμούς προστασίας δεδομένων. Προκειμένου να τηρηθούν τα δικαιώματα των ενδιαφερόμενων, συμφωνείται στη Σύμβαση επεξεργασίας δεδομένων ότι ο Ανάδοχος πρέπει να υποστηρίζει επαρκώς τον Πελάτη, εφόσον απαιτείται, π.χ. για την παροχή πληροφοριών στους εμπλεκόμενους.

Στην περαιτέρω πορεία της επεξεργασίας των προσωπικών δεδομένων, ο Πελάτης ελέγχει τα αποτελέσματα της εργασίας του Αναδόχου, όσον αφορά τη μορφή και το περιεχόμενο. Η τήρηση των τεχνικών και οργανωτικών μέτρων που λαμβάνει ο Ανάδοχος εξετάζεται τακτικά. Για τον σκοπό αυτό, χρησιμοποιείται κυρίως η υποβολή των υφιστάμενων βεβαιώσεων ελέγχου ή των κατάλληλων πιστοποιήσεων ή τα αποδεικτικά στοιχεία σχετικά με τη διεξαγωγή ελέγχων ασφάλειας IT ή της προστασίας των προσωπικών δεδομένων. Στο μέτρο που απασχολούνται υπεργολάβοι, ορίζεται συμβατικά να ελέγχονται αναλόγως.

6. Εξασφάλιση της αντοχής των συστημάτων

Η υποδομή του cloud της AWS δημιουργήθηκε ως ένα από τα πιο ευέλικτα και ασφαλή περιβάλλοντα υπολογιστικού νέφους (Cloud Computing). Έχει σχεδιαστεί για βέλτιστη διαθεσιμότητα με πλήρη διαχωρισμό των πελατών. Παρέχει μια εξαιρετικά κλιμακούμενη και αξιόπιστη πλατφόρμα, που επιτρέπει στους πελάτες να αναπτύσσουν εφαρμογές και περιεχόμενο γρήγορα και με ασφάλεια σε όλο τον κόσμο, όπως απαιτείται. Οι υπηρεσίες της AWS είναι ανεξάρτητες όσον αφορά το περιεχόμενο, δεδομένου ότι

παρέχουν σε όλους τους πελάτες το ίδιο υψηλό επίπεδο ασφάλειας, ανεξάρτητα από το είδος του περιεχομένου ή τη γεωγραφική περιοχή στην οποία αποθηκεύεται το περιεχόμενο.

Τα κέντρα επεξεργασίας δεδομένων υψηλής ασφάλειας της AWS σε παγκόσμιο επίπεδο χρησιμοποιούν σύγχρονα μέτρα ηλεκτρονικής παρακολούθησης και πολυεπίπεδα συστήματα ελέγχου πρόσβασης. Τα κέντρα επεξεργασίας δεδομένων στελεχώνονται όλο το εικοσιτετράωρο με εκπαιδευμένο προσωπικό ασφαλείας και η πρόσβαση εξασφαλίζεται αυστηρά σύμφωνα με την αρχή των ελάχιστων δικαιωμάτων και αποκλειστικά για τον σκοπό της διαχείρισης του συστήματος.

7. Διαδικασία για την αποκατάσταση της διαθεσιμότητας προσωπικών δεδομένων μετά από φυσικό ή τεχνικό περιστατικό

Τα κέντρα επεξεργασίας δεδομένων της AWS οικοδομούνται σε ομάδες σε διάφορες περιοχές του κόσμου. Όλα τα κέντρα επεξεργασίας δεδομένων είναι online και εξυπηρετούν πελάτες. Κανένα κέντρο επεξεργασίας δεδομένων δεν τίθεται εκτός λειτουργίας. Σε περίπτωση βλάβης, οι αυτοματοποιημένες διαδικασίες μετακινούν την κυκλοφορία δεδομένων των πελατών μακριά από τις πληγείσες περιοχές. Οι βασικές εφαρμογές αναπτύσσονται σε διαμόρφωση N+1, έτσι ώστε σε περίπτωση βλάβης του κέντρου επεξεργασίας δεδομένων, να υπάρχει επαρκής χωρητικότητα για την ισορροπημένη διανομή φορτίου της κυκλοφορίας δεδομένων στις υπόλοιπες τοποθεσίες.

Η AWS παρέχει την ευελιξία τοποθέτησης οντοτήτων και αποθήκευσης των δεδομένων σε πολλές γεωγραφικές περιοχές, καθώς και σε πολλές ζώνες διαθεσιμότητας εντός των μεμονωμένων περιοχών. Κάθε ζώνη διαθεσιμότητας σχεδιάστηκε ως ανεξάρτητη ζώνη βλάβης. Αυτό σημαίνει ότι οι ζώνες διαθεσιμότητας κατανέμονται φυσικά εντός μιας τυπικής αστικής περιοχής και βρίσκονται π.χ. σε περιοχές με χαμηλότερο κίνδυνο πλημμύρας (ανάλογα με την περιοχή, υπάρχουν διάφορες κατηγορίες πλημμυρικών ζωνών). Εκτός από μια αυτόνομη τροφοδοσία ρεύματος αδιάλειπτης παροχής και τις επιτόπιες γεννήτριες έκτακτης ανάγκης, όλες οι ζώνες διαθεσιμότητας τροφοδοτούνται από ανεξάρτητους παρόχους ηλεκτρικής ενέργειας μέσω διαφορετικών ηλεκτρικών δικτύων, για την ελαχιστοποίηση των σημείων μεμονωμένων αστοχιών. Όλες οι ζώνες διαθεσιμότητας συνδέονται πλεονασματικά με πολλούς παρόχους διαμετακόμισης Tier 1.

Η ομάδα διαχείρισης συμβάντων του Amazon εφαρμόζει διαγνωστικές διαδικασίες που αποτελούν κοινό χαρακτηριστικό στον κλάδο, για να προωθήσει την αντιμετώπιση κρίσιμων επιχειρηματικών συμβάντων. Το προσωπικό εκμετάλλευσης παρέχει συνεχή κάλυψη εικοσιτέσσερις ώρες το εικοσιτετράωρο, επτά ημέρες την εβδομάδα και 365 ημέρες τον χρόνο, για την ανίχνευση βλαβών και τη διαχείριση των επιπτώσεών τους καθώς τη λήψη διορθωτικών μέτρων.

8. Διαδικασίες για τακτικό έλεγχο, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων

Οι οδηγίες και οι εντολές της επιχείρησης και/ή τα εφαρμοζόμενα πρότυπα για την ασφάλεια των πληροφοριών εφαρμόζονται, επίσης, και όσον αφορά την υλοποίηση και τη λειτουργία της πλατφόρμας RIO. Υπάρχουν επιχειρησιακές λειτουργίες για την προστασία των δεδομένων και την ασφάλεια των πληροφοριών (Υπεύθυνος προστασίας δεδομένων και Υπεύθυνος ασφαλείας πληροφοριών). Οι

υπάλληλοι δεσμεύονται για το απόρρητο των δεδομένων και ενημερώνονται σχετικά με την ασφάλεια των δεδομένων ή τα μέτρα ασφάλειας IT μέσω φυλλαδίων, διαφημιστικών, υποδείξεων Intranet κ.λπ.

Οι εσωτερικές διαδικασίες ελέγχονται για τη συμμόρφωση με τα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των δεδομένων μέσω του ελέγχου, της ασφάλειας των πληροφοριών και της προστασίας των δεδομένων.

Οι διαδικασίες επεξεργασίας και τα μέτρα ασφάλειας δεδομένων τεκμηριώνονται σε έναν κατάλογο δραστηριοτήτων επεξεργασίας. Διενεργείται τακτικός έλεγχος (εσωτερικός και εξωτερικός) σχετικά με την αποτελεσματικότητα των μέτρων.