

Σύμβαση Επεξεργασίας Δεδομένων (DPA)

Anasa (Εκτελών) ⇄ Εταιρεία μεταφορών (Υπεύθυνος) · άρθρο 28 ΓΚΠΔ

Παρέχεται με κάθε συνδρομή Anasa και καταρτίζεται με την αποδοχή σας μέσα στην εφαρμογή — δεν χρειάζεται υπογραφή σε χαρτί (§10). Ο GDPR (άρθρο 28) **απαιτεί** γραπτή σύμβαση μεταξύ της εταιρείας που χρησιμοποιεί την υπηρεσία (Υπεύθυνος επεξεργασίας) και του παρόχου λογισμικού (Εκτελών). Η Anasa σας τη δίνει έτοιμη ώστε να έχετε **τη σύμβαση που απαιτεί το άρθρο 28** από την πρώτη μέρα. Τις υπόλοιπες υποχρεώσεις σας ως Υπεύθυνος επεξεργασίας (αρχείο δραστηριοτήτων, ενημέρωση οδηγών, αντίδραση σε περιστατικό) τις κρατάτε εσείς. **Έκδοση 2026-09-03ap** · Το κείμενο αυτό είναι **ταντόσημο** με το /dpa.html. Αν διαφέρουν, ισχύει η δημοσιευμένη σελίδα και πρόκειται για σφάλμα — ενημερώστε μας στο info@anasaapp.com. *Πρότυπο ευθυγραμμισμένο με το άρθρο 28 GDPR. Συνιστάται τελικός έλεγχος από τον νομικό σας.*

1. Ρόλοι

- **Υπεύθυνος επεξεργασίας:** ο Πελάτης (η εταιρεία μεταφορών). Αποφασίζει **γιατί** και **πώς** επεξεργάζονται τα δεδομένα θέσης/οδηγών/κρατήσεων και κρατά τη νόμιμη βάση απέναντι στους οδηγούς και τους επιβάτες του.
- **Εκτελών την επεξεργασία:** η Anasa (anasaapp.com) — ατομική επιχείρηση **Ελευθερία Τσαπάκη του Πολυδώρου**, 1η Πάροδος Μαλινδρέτου, Κάτω Σταλός, 735 00 Χανιά, Κρήτη, ΑΦΜ 112393497, Γ.Ε.ΜΗ. 152207758000. Επεξεργάζεται προσωπικά δεδομένα **μόνο κατ' εντολή** του Υπευθύνου.

2. Αντικείμενο, διάρκεια, φύση & σκοπός

- **Αντικείμενο:** παροχή της υπηρεσίας διαχείρισης διαδρομών Anasa (κρατήσεις, ανάθεση οδηγών, ζωντανή θέση οχήματος, ειδοποιήσεις).
- **Διάρκεια:** για όσο διαρκεί η συνδρομή του Πελάτη στην Anasa.
- **Επικοινωνία με επιβάτες:** η Anasa στέλνει μηνύματα σε επιβάτες **μόνο κατ' εντολή του Πελάτη** και **με τη διεύθυνση αποστολής του Πελάτη** — το περιεχόμενο και η ενεργοποίηση ορίζονται από τις ρυθμίσεις του. Ορισμένα φεύγουν αυτόματα από χρονοπρογραμματισμένη εργασία, χωρίς ο Πελάτης να είναι συνδεδεμένος. Η Anasa **δεν επικοινωνεί ποτέ με επιβάτες για δικό της σκοπό**.
- **Φύση & σκοπός:** φιλοξενία, μετάδοση, εμφάνιση και βραχυπρόθεσμη αποθήκευση λειτουργικών δεδομένων ώστε ο Πελάτης να συντονίζει **τον δικό του στόλο**.

3. Κατηγορίες δεδομένων & υποκειμένων

- **Υποκείμενα:** οι οδηγοί και το προσωπικό γραφείου του Πελάτη· επιβάτες· επικοινωνούντες από ξενοδοχεία/συνεργάτες που στέλνουν κρατήσεις.
- **Προσωπικά δεδομένα:** - Οδηγός: όνομα, τηλέφωνο, όχημα, ώρες βάρδιας και υπερωρίας, κανόνας αμοιβής, ταμείο βάρδιας, **θέση GPS οχήματος (τελευταία θέση· προσωρινή)**. - Αν ο Υπεύθυνος ορίσει **ζώνες ιδιωτικότητας**, τηρούνται και οι **ίδιες οι ζώνες** *(αναγνώσιμες)*: η **ονομασία** που έδωσε, το **κέντρο** (συντεταγμένες) και η **ακτίνα**. Είναι αναγκαίο να μένουν αναγνώσιμες, γιατί ο διακομιστής τις εφαρμόζει και για συσκευές GPS πάνω στο όχημα, που δεν περνούν από την εφαρμογή του οδηγού — αλλιώς η ζώνη δεν θα ίσχυε καθόλου γι' αυτές. Επειδή μια ζώνη ορίζεται συχνά γύρω από την **κατοικία οδηγού**, ο Υπεύθυνος καλείται να μη γράφει στην ονομασία περισσότερα απ' όσα χρειάζεται. - Επιβάτης/κράτηση: όνομα, τηλέφωνο, email, σημείωση, σημείο παραλαβής/προορισμός και συντεταγμένες, ενδιαμέσες στάσεις, αριθμός επιβατών, αριθμός πτήσης, ώρα, σύνδεσμος παρακολούθησης.
- **Υπεργολαβία διαδρομής σε άλλη εταιρεία μεταφορών — γνωστοποίηση του Υπευθύνου, όχι της Anasa.** Όταν ο Υπεύθυνος στείλει διαδρομή σε συνεργάτη μέσα από την εφαρμογή, η Anasa **διαβιβάζει** με email, **κατ' εντολή του και από τη δική του διεύθυνση**: όνομα και τηλέφωνο επιβάτη, παραλαβή, προορισμό, ημερομηνία/ώρα, αριθμό ατόμων, πτήση, **τα παιδικά καθίσματα που ζητήθηκαν** και τη **σημείωση** της κράτησης. **Δεν** διαβιβάζονται η τιμή του πελάτη, το κόστος προς τον συνεργάτη, ούτε ο σύνδεσμος ζωντανής παρακολούθησης. Η αποδέκτρια εταιρεία είναι **αυτοτελής υπεύθυνη επεξεργασίας· δεν** είναι υπο-εκτελούσα της Anasa και **δεν** καλύπτεται από τον κατάλογο του §7. Ο Υπεύθυνος οφείλει να την έχει προβλέψει στη **δική του** Ενημέρωση Επιβάτη (το παρεχόμενο πρότυπο την ονομάζει ρητά) και να μη διαβιβάζει μέσω της σημείωσης δεδομένα που δεν πρέπει να φύγουν.
- **Δεν ζητούμε ούτε επιδιώκουμε ειδικές κατηγορίες** (άρθρο 9)· κανένα πεδίο δεν τις προβλέπει. Η **σημείωση** της κράτησης είναι ελεύθερο κείμενο και ο Υπεύθυνος οφείλει να μην καταχωρεί εκεί δεδομένα υγείας — αν το κάνει, τηρούνται κρυπτογραφημένα (§6) και σβήνονται με τα υπόλοιπα στοιχεία επιβάτη (§5). Η θέση είναι **λειτουργική, όχι συνεχής καταγραφή ζωής**.

- Ποια από αυτά είναι αναγνώσιμα από την Anasa και ποια όχι: **βλ. §6.**

4. Υποχρεώσεις εκτελούντος (άρθρο 28§3)

Η Anasa:

- **(α)** επεξεργάζεται δεδομένα **μόνο κατ' εντολή** του Υπευθύνου — εκτός αν υποχρεούται από το δίκαιο της Ένωσης ή κράτους μέλους (π.χ. δεσμευτικό αίτημα φορολογικής, δικαστικής ή εποπτικής αρχής)· στην περίπτωση αυτή ενημερώνει τον Υπεύθυνο **πριν** από την επεξεργασία, εκτός αν το δίκαιο απαγορεύει την ενημέρωση για **σοβαρούς** λόγους δημοσίου συμφέροντος. Παρέχει **μόνο τα δεδομένα που ρητά ζητούνται**, ελέγχοντας πρώτα, όπου είναι εφικτό, ότι το αίτημα είναι γραπτό και επικαλείται νομική βάση·
- **(β)** εξασφαλίζει ότι **κάθε φυσικό πρόσωπο** που ενεργεί υπό την εποπτεία της και έχει πρόσβαση σε δεδομένα του Υπευθύνου — **περιλαμβανομένων του διαχειριστή συστημάτων και του συντηρητή του λογισμικού** — έχει αναλάβει **έγγραφο δέσμευση εμπιστευτικότητας** που επιβιώνει της λήξης της σχέσης του με την Anasa, και ότι η πρόσβαση περιορίζεται σε ό,τι είναι αναγκαίο για τη συντήρηση, την υποστήριξη και την ασφάλεια. Ο κατάλογος των προσώπων αυτών τηρείται γραπτά και τίθεται στη διάθεση του Υπευθύνου κατά §7β·
- **(γ)** εφαρμόζει κατάλληλα **τεχνικά & οργανωτικά μέτρα ασφάλειας** (άρθρο 32) — βλ. §6·
- **(δ)** χρησιμοποιεί **υπο-εκτελούντες** μόνο κατά §7, με ισοδύναμες υποχρεώσεις·
- **(ε)** συνδράμει τον Υπεύθυνο στην ικανοποίηση **δικαιωμάτων υποκειμένων** (πρόσβαση, διαγραφή, εναντίωση) — με εργαλεία εξαγωγής/διαγραφής ανά οργανισμό. **Με την επιφύλαξη της §6:** για τα πεδία που είναι κρυπτογραφημένα στη συσκευή του Υπευθύνου, η Anasa δεν έχει τεχνική δυνατότητα ανάγνωσης και επομένως δεν μπορεί να συνδράμει σε αιτήματα που προϋποθέτουν ανάγνωση·
- **(στ)** συνδράμει σε **γνωστοποίηση παραβίασης** (άρθρα 33–34), **DPIA** (άρθρο 35) και προηγούμενη διαβούλευση (άρθρο 36)·
- **(ζ)** κατ' επιλογή του Υπευθύνου, **διαγράφει ή επιστρέφει** όλα τα δεδομένα στο τέλος της υπηρεσίας·
- **(η)** διαθέτει τις πληροφορίες που αποδεικνύουν συμμόρφωση, επιτρέπει και **διευκολύνει ελέγχους και επιθεωρήσεις** κατά §7β, και ειδοποιεί άμεσα τον Υπεύθυνο αν μια εντολή φαίνεται να παραβιάζει τον GDPR ή τον N. 4624/2019.

Γνωστοποίηση παραβίασης (άρθρο 33§2). Μόλις η Anasa αντιληφθεί παραβίαση δεδομένων που αφορά δεδομένα του Πελάτη, τον ειδοποιεί χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση **εντός 48 ωρών**, στο email του λογαριασμού του. Η ειδοποίηση περιλαμβάνει ό,τι είναι γνωστό τη στιγμή εκείνη: τη φύση του περιστατικού, τις κατηγορίες και τον κατά προσέγγιση αριθμό εγγράφων/υποκειμένων, τις πιθανές συνέπειες και τα μέτρα που λήφθηκαν ή προτείνονται. Αν κάποια στοιχεία λείπουν, δίνονται σταδιακά χωρίς να καθυστερεί η αρχική ειδοποίηση. Οι **72 ώρες** του Πελάτη προς την Αρχή τρέχουν από τη δική του γνώση — γι' αυτό η προθεσμία της Anasa είναι συντομότερη.

5. Ελαχιστοποίηση & διατήρηση δεδομένων

- **Η θέση είναι προσωρινή.** Κρατείται η **τελευταία** θέση για τη ζωντανή λειτουργία, χωρίς μακροχρόνιο ιστορικό κινήσεων. Παύει να ισχύει και να εμφανίζεται **μετά από 30 λεπτά**, και η εγγραφή διαγράφεται αυτόματα **εντός 24 ωρών** από το τελευταίο στίγμα. **Περιορισμός σκοπού:** όχι αυτόνομη κατάρτιση προφίλ συμπεριφοράς.
- **Στοιχεία επιβάτη** (όνομα, τηλέφωνο, email, σημείωση, σύνδεσμος παρακολούθησης, **οι ενδιάμεσες στάσεις** — που κρατούν πλάνωμα και τηλέφωνα επιβατών — **ο συνοδός ή ξεναγός** της διαδρομής (όνομα και τηλέφωνο) και **το επισυναπτόμενο έγγραφο της κράτησης**, π.χ. voucher πρακτορείου, PDF ή φωτογραφία): διαγράφονται αυτόματα **3 μήνες** από τη διαδρομή. Ο Υπεύθυνος μπορεί να το συντομεύσει σε 1 μήνα· **ανώτατο 6 μήνες**, χωρίς δυνατότητα απενεργοποίησης. **Στο ίδιο ρολόι διαγράφεται και το αρχικό εισερχόμενο μήνυμα** από το οποίο προήλθε η κράτηση (email, WhatsApp, φόρμα ιστοσελίδας, πύλη ξενοδοχείου) — **ολόκληρο το κείμενο του μηνύματος**, όχι μόνο τα πεδία που αναγνωρίστηκαν, μετρημένο από την **παραλαβή του μηνύματος**. Τα **συννημμένα των εισερχόμενων email δεν αποθηκεύονται**: από ένα email κρατείται το κείμενό του, ενώ τα επισυναπτόμενα αρχεία **δεν φτάνουν ποτέ στους διακομιστές μας**. Στο μήνυμα που βλέπετε σημειώνεται **πόσα ήταν και πώς λέγονταν**, ώστε να ξέρετε ότι υπήρχαν και να ανοίξετε το αρχικό email αν τα χρειάζεστε.
- **Μηνύματα εσωτερικής συνομιλίας** (κείμενο, όνομα αποστολέα, ώρα) — **δύο παράθυρα**: το νήμα **γραφείου ↔ οδηγού δεν διαγράφεται αυτόματα** και τηρείται όσο ζει ο λογαριασμός του Υπευθύνου (εργασιακή τεκμηρίωση της επιχείρησής του)· τα μηνύματα **οδηγού ↔ οδηγού διαγράφονται αυτόματα μετά από τρεις (3) μήνες**, ολόκληρα. Ο λόγος του χωρισμού είναι ο σκοπός (άρθρο 5§1ε): το δεύτερο νήμα δεν είναι προσβάσιμο ούτε στον Υπεύθυνο ούτε στο γραφείο του, επομένως δεν εξυπηρετεί σκοπό της επιχείρησης πέρα από τη στιγμή του.
- **Ιστορικό πύλης ξενοδοχείου/πρακτορείου** (αντίγραφο κάθε κράτησης και μηνύματος που υποβλήθηκε από τη συγκεκριμένη πύλη): **δύο επίπεδα**. Ως **έξι (6) μήνες** τηρείται πλήρες, ώστε η ρεσεψιόν να βλέπει τι έχει στείλει. Στη συνέχεια, και **έως δώδεκα (12) μήνες**, η γραμμή επιβιώνει **χωρίς κανένα στοιχείο επιβάτη**: διαγράφονται **όνομα, διεύθυνση email και σημείωση**, και τα μηνύματα ελεύθερου κειμένου **διαγράφονται ολόκληρα**.

μένουν μόνο διαδρομή, αριθμός ατόμων, ημερομηνία και ώρα, αριθμός πτήσης, παιδικά καθίσματα και κατάσταση — όσα χρειάζεται η ρεσεψιόν για να αποδείξει **τι υπέβαλε και πότε**, σε ξενοδοχείο ή πρακτορείο που συνεργάζεται όλο τον χρόνο. Στους **δώδεκα (12) μήνες** η εγγραφή διαγράφεται ολόκληρη. Η **πλήρης** περίοδος των έξι μηνών είναι **ανεξάρτητη** από τη ρύθμιση του Υπευθύνου για τα στοιχεία επιβάτη και **μπορεί να την υπερβαίνει** όταν εκείνος έχει επιλέξει 1 ή 3 μήνες· **ποτέ όμως δεν υπερβαίνει το ανώτατο των έξι μηνών** που ισχύει για τα στοιχεία επιβάτη. Με την **ανάκληση της πύλης** διαγράφεται αμέσως ολόκληρο. Πρόκειται για **δεύτερο, χωριστό αντίγραφο**: το αρχικό εισερχόμενο μήνυμα της πύλης, που φτάνει στα εισερχόμενα του Υπευθύνου, εξακολουθεί να ακολουθεί το ρολόι των **στοιχείων επιβάτη** παραπάνω.

- **Επιχειρησιακά αρχεία** (διαδρομή, ώρα, ποσό, οδηγός): τη διάρκεια την ορίζει ο Υπεύθυνος (**3/6/12/24 μήνες ή χωρίς όριο· προεπιλογή 12**) και η Anasa την εκτελεί — με ειδοποίηση 14 ημερών, τελευταία υπενθύμιση 2 ημερών και δυνατότητα εξαγωγής πριν από την πρώτη διαγραφή.
- **Αντίγραφα ασφαλείας — εξαίρεση από τα ανωτέρω παράθυρα**. Τα παραπάνω αφορούν τα **ζωντανά** δεδομένα. Αντίγραφο που λήφθηκε **πριν** από τη διαγραφή εξακολουθεί να περιέχει τα δεδομένα μέχρι να λήξει το ίδιο. Η Anasa τηρεί αντίγραφα **έως τριάντα πέντε (35) ημέρες**, τα οποία: (α) υπόκεινται σε αυστηρό έλεγχο πρόσβασης· (β) **δεν χρησιμοποιούνται στην κανονική λειτουργία**, παρά μόνο για αποκατάσταση μετά από απώλεια ή αλλοίωση· (γ) μετά από **κάθε** επαναφορά, η διαγραφή του παρόντος άρθρου **ξανατρέχει αμέσως**, ώστε να μην ανασταίνονται δεδομένα που είχαν διαγραφεί νόμιμα. Πρακτική συνέπεια: η μέγιστη πραγματική ζωή ενός δεδομένου είναι ο χρόνος διατήρησής του **συν έως 35 ημέρες**.
- **Υπηρεσία αποστολής email — δικό της, ανεξάρτητο παράθυρο**. Κάθε email που φεύγει προς επιβάτη, οδηγό ή τον ίδιο τον Υπεύθυνο περνά από την υπηρεσία αποστολής (Resend, §7). Εκείνη κρατά **αντίγραφο του μηνύματος και το ιστορικό παράδοσης έως τριάντα (30) ημέρες** από την αποστολή, ώστε να είναι δυνατός ο έλεγχος παράδοσης, και τα διαγράφει στη συνέχεια. Το παράθυρο αυτό είναι **της υπηρεσίας** και τρέχει ανεξάρτητα από τους χρόνους διατήρησης της παρούσας παραγράφου: δεν αναιρεί τη διαγραφή στα ζωντανά δεδομένα, ούτε επιμηκύνεται από αυτήν. Το περιεχόμενο που φτάνει εκεί είναι μόνο ό,τι μπαίνει στο ίδιο το μήνυμα (π.χ. όνομα επιβάτη, σημείο παραλαβής, στοιχεία οχήματος), ποτέ το αρχείο κρατήσεων.
- **Λήξη ή καταγγελία της συνδρομής**. Ο λογαριασμός τίθεται σε κατάσταση **μόνο-ανάγνωσης**: δεν προστίθενται νέες κρατήσεις, αλλά ο Υπεύθυνος **διατηρεί πλήρη πρόσβαση ανάγνωσης και εξαγωγής** του αρχείου του (κρατήσεις, βάρδιες, ταμείο) σε Excel/CSV. **Δεν διαγράφουμε τα δεδομένα επειδή έληξε η συνδρομή**. Οι χρόνοι διατήρησης της παρούσας παραγράφου **εξακολουθούν να τρέχουν** και μετά τη λήξη.
- Η **οριστική διαγραφή ή επιστροφή του συνόλου** γίνεται **κατ' επιλογή του Υπευθύνου (§4ζ)**, με γραπτό αίτημα στο info@anasaapp.com· την εκτελούμε **εντός τριάντα (30) ημερών** και χορηγούμε **έγγραφο βεβαίωσης διαγραφής** κατόπιν αιτήματος. Η επιστροφή γίνεται από τα **ζωντανά** δεδομένα — τα αντίγραφα ασφαλείας είναι μηχανισμός αποκατάστασης, **όχι αρχείο**, και λήγουν μόνα τους (έως 35 ημέρες).

6. Ασφάλεια (άρθρο 32)

- Απομόνωση δεδομένων **ανά εταιρεία** (καμία πρόσβαση μεταξύ εταιρειών).
- Εγγραφές κατάστασης/κράτησης μόνο αφού επαληθευτεί η ταυτότητα και η ιδιότητα μέλους του καλούντος.
- **Κρυπτογράφηση μεταφοράς (TLS)**.
- Τα κλειδιά GPS του παρόχου, **όταν** ο Πελάτης επιλέξει 24/7 server-side, αποθηκεύονται **κρυπτογραφημένα** και χρησιμοποιούνται **μόνο για ανάγνωση**· ο Πελάτης μπορεί να τα ανακαλέσει οποτεδήποτε.
- Υπογεγραμμένα webhooks / tokens ανά οργανισμό· πρόσβαση μόνο σε εξουσιοδοτημένους ρόλους.

Ανθεκτικότητα & αποκατάσταση (άρθρο 32§1 β, γ). Η βάση τηρεί δυνατότητα **επαναφοράς σε συγκεκριμένη χρονική στιγμή (PITR) επτά (7) ημερών**, **ημερήσιο αντίγραφο ασφαλείας με διατήρηση πέντε εβδομάδων (§5)** και **προστασία κατά της διαγραφής της ίδιας της βάσης**. Η διαδικασία αντίδρασης σε περιστατικό είναι γραπτή και επανεξετάζεται ετησίως.

Έλεγχος πρόσβασης. Η πρόσβαση διέπεται από κανόνες **default-deny** ανά οργανισμό και ρόλο: κάθε ανάγνωση και εγγραφή περνά από επαλήθευση ιδιότητας μέλους στον διακομιστή, ποτέ από πεδίο που στέλνει ο πελάτης. Στους λογαριασμούς με κωδικό διατίθεται **δεύτερος παράγοντας ταυτοποίησης (TOTP)** και επιβάλλεται **πολιτική ελάχιστου κωδικού** (10 χαρακτήρες με τουλάχιστον έναν αριθμό)· είναι ενεργή η **προστασία κατά της απαρίθμησης διευθύνσεων email**. Οι λογαριασμοί Google φέρουν τον δεύτερο παράγοντα της Google.

Καταγραφή πρόσβασης (άρθρο 32§1 β). Οι προσβάσεις σε δεδομένα στη βάση και στην υπηρεσία ταυτοποίησης **καταγράφονται** (ανάγνωση, εγγραφή και διαχειριστική ενέργεια), με καταγραφή του ποιος, πότε και σε ποια διαδρομή εγγράφου. Η καταγραφή επιτρέπει τον **προσδιορισμό του εύρους ενός περιστατικού** — δηλαδή τον κατά προσέγγιση αριθμό εγγράφων και υποκειμένων που απαιτεί το άρθρο 33§3(β) — και εξίσου την **απόδειξη ότι δεν υπήρξε πρόσβαση**. Τα αρχεία καταγραφής διατηρούνται **τριάντα (30) ημέρες**.

Τακτική δοκιμή & αξιολόγηση (άρθρο 32§1 δ). Τα τεχνικά και οργανωτικά μέτρα, ο κατάλογος υπο-εκτελούντων (§7) και οι χρόνοι διατήρησης (§5) **επανεξετάζονται τουλάχιστον μία φορά ετησίως** και μετά από κάθε ουσιώδη μεταβολή της υπηρεσίας ή περιστατικό ασφάλειας. Πριν από κάθε δημοσίευση κώδικα εκτελείται **αυτοματοποιημένη δέσμη ελέγχων** που, μεταξύ άλλων, αντιπαραβάλλει τους παρόχους που καλεί ο κώδικας με τον κατάλογο της §7 και τις ρυθμίσεις ασφαλείας της υποδομής με το παρόν κείμενο. Η ημερομηνία της τελευταίας επανεξέτασης γνωστοποιείται στον Υπεύθυνο κατόπιν αιτήματος.

Κρυπτογράφηση στη συσκευή του Υπευθύνου — εξ ορισμού ενεργή. Ο Υπεύθυνος ορίζει μυστική φράση κατά την έναρξη χρήσης. Από εκείνο το σημείο κρυπτογραφούνται τα χρηματικά ποσά, τα στοιχεία παραλαβής/προορισμού και επιβάτη, οι συντεταγμένες, ο κατάλογος συνεργαζόμενων ξενοδοχείων και συνεργατών, ο στόλος, το μητρώο οδηγών, ο τιμοκατάλογος και το ταμείο κάθε οδηγού. Ως συνέπεια, **η Anasa δεν υπολογίζει κανένα ποσό:** στους διακομιστές της καταγράφονται μόνο ποσότητες (λεπτά αναμονής, αριθμός στάσεων), όχι αξίες.

Το κλειδί παράγεται **τοπικά** (PBKDF2-SHA256, 600.000 επαναλήψεων · AES-256-GCM) και δεν μεταδίδεται ούτε τηρείται από την Anasa: για τα πεδία αυτά η Anasa τηρεί **μόνο κρυπτογράφημα**, το οποίο δεν έχει τεχνική δυνατότητα να αποκρυπτογραφηθεί.

Εξαίρεση — ο σύνδεσμος παρακολούθησης της διαδρομής. Όταν ο Υπεύθυνος αναθέτει όχημα και ενεργοποιείται ο προσωπικός σύνδεσμος του επιβάτη, ο διακομιστής τηρεί για τη διάρκεια ζωής του συνδέσμου (**έως 30 ημέρες**) το **ονοματεπώνυμο του επιβάτη και το σημείο παραλαβής** σε **αναγνώσιμη** μορφή. Ο σκοπός είναι αποκλειστικά η ειδοποίηση προς τον οδηγό όταν ο επιβάτης δηλώσει ότι είναι έτοιμος, η οποία πρέπει να προσδιορίζει ποιον επιβάτη και ποιο σημείο αφορά. **Δεν** τηρούνται προορισμός, τηλέφωνο, email ή σημείωση. Η εγγραφή διαγράφεται με τη λήξη του συνδέσμου. Η διαβεβαίωση της προηγούμενης παραγράφου περί κρυπτογραφήματος **δεν καλύπτει τα δύο αυτά πεδία** για όσο ζει ο σύνδεσμος.

Χωριστή περίπτωση — η ΑΠΟΣΤΟΛΗ email, όχι η τήρηση. Όταν ο Υπεύθυνος στέλνει στον επιβάτη το email του συνδέσμου (ή της αλλαγής οχήματος, ή την απόδειξη), η συσκευή του διαβιβάζει στον διακομιστή σε **αναγνώσιμη** μορφή τη **διεύθυνση email**, το **όνομα**, την **παραλαβή**, τον **προορισμό** και τα στοιχεία οχήματος, ώστε να συνταχθεί το μήνυμα και να παραδοθεί μέσω της υπηρεσίας αποστολής email (§7). **Δεν αποθηκεύονται:** το σχετικό endpoint συντάσσει και στέλνει, δεν γράφει πουθενά. Αναγνώσιμο **τηρείται** μόνο ό,τι περιγράφει η προηγούμενη εξαίρεση.

Εξαίρεση — η πύλη ξενοδοχείου/πρακτορείου. Για κάθε πύλη που εκδίδει ο Υπεύθυνος, ο διακομιστής τηρεί σε **αναγνώσιμη** μορφή την **επωνυμία του συνεργάτη** όπως την καταχώρισε ο Υπεύθυνος, χωρίς προκαθορισμένη λήξη και για όσο ισχύει ο σύνδεσμος: η σελίδα ανοίγεται από υπάλληλο του συνεργάτη, ο οποίος δεν διαθέτει το κλειδί του Υπευθύνου. Ο τυχόν **κωδικός PIN δεν τηρείται** — τηρείται μόνο κρυπτογραφικό του αποτύπωμα, δεμένο στον συγκεκριμένο σύνδεσμο. Η ανάκληση του συνδέσμου από τον Υπεύθυνο διαγράφει την εγγραφή.

Εξαίρεση — τα εισερχόμενα μηνύματα κρυπτογραφούνται με κλειδί της Anasa, όχι του Υπευθύνου. Ό,τι φτάνει από **τρίτον** (email στη διεύθυνση κρατήσεων, WhatsApp, φόρμα ιστοσελίδας, πύλη ξενοδοχείου/πρακτορείου, αίτημα επιστροφής οδηγού, μήνυμα υποστήριξης) το γράφει ο **διακομιστής** τη στιγμή της παραλαβής: ο αποστολέας δεν διαθέτει —και δεν πρέπει να διαθέτει— τη μυστική φράση του Υπευθύνου. Το περιεχόμενο τηρείται **κρυπτογραφημένο at-rest με κλειδί που κατέχει η Anasa** (AES-256-GCM) και **αποκρυπτογραφείται από τον διακομιστή** σε κάθε ανάγνωση των Μηνυμάτων, ώστε να εμφανιστεί στον Υπεύθυνο. **Κατά συνέπεια η Anasa έχει τεχνική δυνατότητα ανάγνωσης του περιεχομένου αυτού** — σε αντίθεση με τα πεδία της κράτησης (§6) — και η διαβεβαίωση περί μη δυνατότητας ανάγνωσης **δεν καλύπτει τη ροή αυτή**. Η πρόσβαση περιορίζεται κατά §4(β) και υπόκειται στην ίδια δέσμευση εμπιστευτικότητας. Τα μηνύματα διαγράφονται στο ρολόι της §5.

Συνέπεια που ο Υπεύθυνος αποδέχεται ορίζοντας τη μυστική φράση: για τα κρυπτογραφημένα πεδία η Anasa **δεν μπορεί να συνδράμει σε αιτήματα υποκειμένων** (§4ε) ούτε να ανακτήσει δεδομένα σε περίπτωση απώλειας της φράσης και του κωδικού ανάκτησης· **δεν τηρείται εφεδρικό κλειδί**. Η διαγραφή (§5) εκτελείται κανονικά, καθώς δεν προϋποθέτει ανάγνωση. Η κρυπτογράφηση πάνει **μόνο ό,τι γράφεται μετά** την ενεργοποίησή της.

Τι παραμένει αναγνώσιμο σε κάθε περίπτωση: ημερομηνία, ώρα, κατάσταση διαδρομής, ανάθεση οδηγού, ένδειξη αεροδρομίου, οι ώρες εργασίας κάθε οδηγού και η ένδειξη ότι παραδόθηκε ταμείο — χωρίς κανένα ποσό. Τα στοιχεία αυτά παραμένουν αναγνώσιμα επειδή τα διαβάζει το προσωπικό γραφείου του Πελάτη και επειδή επ' αυτών εκτελούνται τα ερωτήματα και ο έλεγχος πρόσβασης.

Μηνύματα ομάδας. Στην ίδια κατηγορία ανήκει και το **κείμενο των μηνυμάτων** της εσωτερικής συνομιλίας (γραφείο ↔ οδηγός και οδηγός ↔ οδηγός), μαζί με το **όνομα του αποστολέα** και την ώρα. Τα μηνύματα τα γράφει ο **διακομιστής** και όχι ο browser — ώστε να μην μπορεί κανείς να στείλει μήνυμα στο όνομα άλλου — και επομένως τηρούνται σε αναγνώσιμη μορφή. Εφόσον είναι ενεργές οι ειδοποίηση push, τα πρώτα **120 σημεία** του μηνύματος αποστέλλονται και ως προεπισκόπηση. Ο έλεγχος πρόσβασης επιβάλλεται τεχνικά: το νήμα **γραφείου ↔ οδηγού** το διαβάζουν ο Υπεύθυνος, το γραφείο του και ο συγκεκριμένος οδηγός· τα μηνύματα **οδηγού ↔ οδηγού** τα διαβάζουν **μόνο οι δύο οδηγοί** — ούτε ο Υπεύθυνος ούτε το γραφείο, και το νήμα δεν εμφανίζεται καν στον κατάλόγό τους. Ο

Υπεύθυνος οφείλει να ενημερώνει το προσωπικό του ότι το πεδίο αυτό δεν είναι κρυπτογραφημένο και να μην το χρησιμοποιεί για στοιχεία που δεν πρέπει να τηρούνται αναγνώσιμα.

7. Υπο-εκτελούντες

Ο Πελάτης εξουσιοδοτεί τους εξής υπο-εκτελούντες, κατά άρθρο 28§2/§4:

Υποδομή: **Cloudflare** (φιλοξενία, Pages Functions, εγγραφές διακομιστή σε KV και **ημερήσιο αντίγραφο ασφαλείας της βάσης έως 35 ημέρες σε αποθηκευτικό χώρο R2**) · **Google Firebase/Firestore** (ταυτοποίηση, βάση δεδομένων) · **Firebase Cloud Messaging** (ειδοποιήσεις push) · **Resend** (εξερχόμενο email).

Λειτουργίες: **OpenAI** (αυτόματη ανάγνωση κράτησης — λαμβάνει το περιεχόμενο του εισερχόμενου μηνύματος/εικόνας) · **TomTom** (αναζήτηση διεύθυνσης, διαδρομή, κίνηση) · **Photon/Komoot** (γεωκωδικοποίηση — στην **αναζήτηση** λαμβάνει το κείμενο της διεύθυνσης που πληκτρολογείται, δηλαδή σημείο παραλαβής/προορισμού· ποτέ όνομα ή τηλέφωνο επιβάτη) · **OSRM** (οδικός χρόνος — μόνο συντεταγμένες· **δύο ανεξάρτητοι δημόσιοι διακομιστές**, `router.project-osrm.org` και, ως εφεδρεία όταν ο πρώτος δεν απαντά, `routing.openstreetmap.de`).

Πτήσεις & χάρτης: **AeroDataBox μέσω RapidAPI** (πρόγραμμα πτήσεων — αριθμός πτήσης & αεροδρόμιο, ποτέ δεδομένα επιβάτη) · **airplanes.live** και **adsbdb** (θέση/διαδρομή αεροσκάφους — μόνο κωδικός αναμεταδότη) · **Esri** (πλακίδια χάρτη) · **OpenFreeMap** (διανυσματικές πλακίδες χάρτη) · **Open-Meteo** (καιρός — μόνο συντεταγμένες) · **unpkg** (βιβλιοθήκη χάρτη). Οι πάροχοι πλακιδίων/αρχείων βλέπουν τη διεύθυνση IP του επισκέπτη, όχι δεδομένα κρατήσεων.

Ενεργοποιούμενα από τον ίδιο τον Πελάτη: **Meta/WhatsApp Business** · **Epsilon Net** (αποδείξεις) · ο **πάροχος GPS** που επιλέγει (π.χ. Mapon, Navixy) — ο τελευταίος παραμένει δικός του πάροχος.

Για κάθε προσθήκη ή αντικατάσταση υπο-εκτελούντα η Anasa ειδοποιεί τον Υπεύθυνο **τουλάχιστον 30 ημέρες πριν**, στο email του λογαριασμού του. Ο Υπεύθυνος μπορεί να εναντιωθεί εγγράφως εντός **14 ημερών**, για βάσιμο λόγο σχετικό με την προστασία δεδομένων. Αν δεν βρεθεί λύση, δικαιούται να καταγγείλει τη σύμβαση **χωρίς ποινή**, με επιστροφή του τιμήματος που αναλογεί στον χρόνο που δεν χρησιμοποιήσε. Η Anasa παραμένει **πλήρως υπόλογη** έναντι του Υπευθύνου για τις πράξεις κάθε υπο-εκτελούντα (άρθρο 28§4).

7α. Η συνδρομή του Πελάτη — άλλη σχέση, όχι υπο-εκτελών

Τα παραπάνω αφορούν τα δεδομένα **επιβατών και οδηγών**, όπου Υπεύθυνος Επεξεργασίας είναι ο Πελάτης. Για τη **συνδρομή του Πελάτη** στην Anasa ισχύει το αντίστροφο: Υπεύθυνος Επεξεργασίας είναι η **Anasa**, και η σχέση περιγράφεται στην Πολιτική Απορρήτου, όχι εδώ. Με πληρωμή **κάρτας** μεσολαβεί το **Stripe** (Stripe Payments Europe, Ltd.) ως πάροχος πληρωμών — λαμβάνει επωνυμία/ονοματεπώνυμο, διεύθυνση χρέωσης, ΑΦΜ και email· τα στοιχεία της κάρτας δίνονται απευθείας στο Stripe και δεν περνούν ποτέ από την Anasa. Το Stripe ενεργεί **και ως αυτοτελής υπεύθυνος επεξεργασίας** για δικούς του σκοπούς (πρόληψη απάτης, κανονιστική συμμόρφωση), όχι κατ' εντολή της Anasa. Με **τραπεζικό έμβασμα** δεν μεσολαβεί πάροχος πληρωμών. **Δεδομένα επιβατών δεν φτάνουν ποτέ στο Stripe**.

7β. Έλεγχοι & επιθεωρήσεις (άρθρο 28§3η)

Ο Υπεύθυνος δικαιούται να ελέγχει τη συμμόρφωση της Anasa. Η Anasa θέτει στη διάθεσή του κάθε απαραίτητη πληροφορία και **επιτρέπει και διευκολύνει επιθεωρήσεις** που διενεργεί ο ίδιος ή ελεγκτής που εξουσιοδοτεί, με προηγούμενη γραπτή ειδοποίηση **30 ημερών**, εντός εργάσιμων ωρών, **μία φορά ανά ημερολογιακό έτος** — και επιπλέον όποτε έχει προηγηθεί περιστατικό παραβίασης ή το ζητήσει εποπτική αρχή, χωρίς περιορισμό συχνότητας. Ο ελεγκτής δεσμεύεται με εμπιστευτικότητα και ο έλεγχος δεν επεκτείνεται σε δεδομένα άλλων πελατών.

8. Διεθνείς διαβιβάσεις

Πού κάθονται τα δεδομένα. Η βάση (Firestore) βρίσκεται στην πολυπεριοχή **eur3** της Google — κέντρα δεδομένων σε **Βέλγιο και Ολλανδία**. Τα δεδομένα των κρατήσεων, των οδηγιών και των πελατών του Υπευθύνου παραμένουν αποθηκευμένα **εντός ΕΕ**. Εξαιρέσεις: η **ταυτοποίηση** (Firebase Authentication — email και αναγνωριστικό χρήστη), το δίκτυο της **Cloudflare** (φιλοξενία, προσωρινή αποθήκευση συνημμένων) και οι υπηρεσίες τρίτων του §7 λειτουργούν σε παγκόσμια υποδομή και ενδέχεται να επεξεργάζονται δεδομένα εκτός ΕΟΧ· για αυτές ισχύει το επόμενο εδάφιο. Τα συνημμένα και τα λοιπά κρυπτογραφημένα πεδία φεύγουν από τη συσκευή **ήδη κρυπτογραφημένα**, οπότε ο αποδέκτης εκτός ΕΟΧ διακινεί κρυπτογράφημα.

Εξαιρέση — αυτόματη ανάγνωση εισερχόμενης κράτησης. Όταν κράτηση φτάνει από κανάλι που χειρίζεται ο διακομιστής (email, ιστοσελίδα, πύλη ξενοδοχείου, WhatsApp), ο διακομιστής **δεν διαθέτει το κλειδί του Υπευθύνου**· επομένως το περιεχόμενο του μηνύματος διαβιβάζεται στην **OpenAI (ΗΠΑ) σε αναγνώσιμη μορφή** και μπορεί να περιλαμβάνει ονοματεπώνυμο και τηλέφωνο επιβάτη, σημείο παραλαβής και προορισμό και αριθμό πτήσης. Η κράτηση κρυπτογραφείται από την **πρώτη συσκευή του Υπευθύνου που την ανακτά**. Η διαβεβαίωση της προηγούμενης παραγράφου περί κρυπτογραφήματος **δεν καλύπτει τη ροή αυτή**. Η υπηρεσία αυτόματης ανάγνωσης τηρεί το

διαβιβασθέν περιεχόμενο **έως τριάντα (30) ημέρες** για δικό της έλεγχο κατάχρησης και **δεν το χρησιμοποιεί για εκπαίδευση μοντέλων**, σύμφωνα με τη δημοσιευμένη πολιτική του παρόχου για το API.

Όπου ο αποδέκτης εκτός ΕΟΧ καλύπτεται από **απόφαση επάρκειας** της Ευρωπαϊκής Επιτροπής (περιλαμβανομένου του **EU-US Data Privacy Framework** για πιστοποιημένους παρόχους στις ΗΠΑ), η διαβίβαση στηρίζεται σε αυτήν (άρθρο 45). Σε κάθε άλλη περίπτωση στηρίζεται στις **Τυποποιημένες Συμβατικές Ρήτρες (SCC)** της Ευρωπαϊκής Επιτροπής (άρθρο 46), με τα πρόσθετα μέτρα που αυτές απαιτούν. Ο Υπεύθυνος λαμβάνει αντίγραφο των εγγυήσεων που ισχύουν για συγκεκριμένο υπο-εκτελούντα κατόπιν αιτήματος.

9. Ευθύνη & εφαρμοστέο δίκαιο

Διέπεται από το ελληνικό δίκαιο· εποπτική αρχή η **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)**. Η ευθύνη κάθε μέρους **έναντι των υποκειμένων των δεδομένων** διέπεται από το **άρθρο 82 GDPR** και **δεν περιορίζεται από τη βασική σύμβαση**. Στη μεταξύ των μερών σχέση, κάθε μέρος βαρύνεται με το τμήμα της ζημίας που αναλογεί στη δική του παράβαση (άρθρο 82§5). Ο περιορισμός ευθύνης της §9 των Όρων Χρήσης ισχύει για την παρούσα σύμβαση **μόνο κατά το μέτρο που εκείνη ρητά την αναφέρει** — και ρητά εξαιρεί τον δόλο, τη βαριά αμέλεια και το άρθρο 82.

10. Κατάρτιση της σύμβασης

Η παρούσα καταρτίζεται **ηλεκτρονικά**: με την αποδοχή της από τον ιδιοκτήτη του λογαριασμού μέσα στην εφαρμογή Anasa. Το άρθρο 28§9 GDPR απαιτεί η σύμβαση να είναι «εγγράφως, **περιλαμβανομένης της ηλεκτρονικής μορφής**» — η αποδοχή αυτή **αρκεί**, και δεν χρειάζεται να μας στείλετε κανένα χαρτί.

Αποδεικτικό είναι η εγγραφή αποδοχής που τηρεί η Anasa: **ποιος** λογαριασμός αποδέχθηκε, **ποια έκδοση** του κειμένου, **πότε** (ώρα διακομιστή) και το **αποτύπωμα SHA-256** των εγγράφων όπως σερβιρίστηκαν εκείνη τη στιγμή — δηλαδή αποδεικνύεται και **τι έλεγε** το κείμενο, όχι μόνο ότι το αποδεχθήκατε. Τηρείται **μία εγγραφή ανά έκδοση**, ώστε να προκύπτει ποιο κείμενο δέσμευε τα μέρη σε κάθε χρονικό σημείο. Αντίγραφο της δικής σας εγγραφής χορηγείται κατόπιν αιτήματος στο **info@anasaapp.com**.

Όταν το κείμενο αλλάξει ουσιαδώς, ζητείται **νέα αποδοχή** στο επόμενο άνοιγμα της εφαρμογής· ως τότε ισχύει η έκδοση που αποδεχθήκατε.

Το παρόν αρχείο είναι **αντίγραφο του κειμένου για το αρχείο σας**. Αν η δική σας διαδικασία απαιτεί υπογεγραμμένο αντίτυπο, ζητήστε το στο **info@anasaapp.com** και το υπογράψουμε.