Ιδιωτικό AI, ΓΚΠΔ (GDPR) και AI Act: τι αλλάζει όταν το AI τρέχει στους δικούς σας διακομιστές

Πρακτικός οδηγός για τη διοίκηση, τους υπευθύνους προστασίας δεδομένων και το IT: πού καταλήγουν τα προσωπικά δεδομένα σε ένα σύστημα AI, πώς αλλάζει η δουλειά της συμμόρφωσης με τον ΓΚΠΔ (GDPR) και τον Κανονισμό για την ΤΝ (AI Act) όταν το AI τρέχει στους δικούς σας διακομιστές, και τι παραμένει δική σας ευθύνη.

10 Νοεμβρίου 2026

empisto.ai · τοπικό · ιδιωτικό · αξιόπιστο

Περιεχόμενα

01 Σύνοψη

02 Πού εμφανίζονται προσωπικά δεδομένα σε ένα σύστημα AI

03 Σύγκριση των δύο δρόμων

04 Ο ΓΚΠΔ, αρχή προς αρχή

05 Ο Κανονισμός για την ΤΝ (AI Act)

06 Εμπιστευτικότητα πέρα από την προστασία δεδομένων

07 AI στο cloud, αν το επιλέξετε

08 Προετοιμασία της αξιολόγησής σας

09 Διαβάστε επίσης

01 Σύνοψη

Κάθε χρήσιμος βοηθός AI θα χειριστεί αργά ή γρήγορα προσωπικά δεδομένα. Οι συμβάσεις περιέχουν ονόματα προσώπων, τα email έχουν υπογραφές, οι φάκελοι προσωπικού και οι σημειώσεις για ασθενείς είναι από τη φύση τους προσωπικά δεδομένα, και οι ερωτήσεις που πληκτρολογούν οι χρήστες συχνά αφορούν συναδέλφους και πελάτες. Για τον ΓΚΠΔ (GDPR), όλα αυτά συνιστούν επεξεργασία. Για τον Κανονισμό για την ΤΝ (AI Act), ο ίδιος ο βοηθός είναι σύστημα AI που συνεπάγεται υποχρεώσεις.

Ο συνηθισμένος δρόμος προς το AI είναι να στέλνονται αυτά τα έγγραφα και οι ερωτήσεις στους διακομιστές ενός παρόχου. Ο δρόμος αυτός λειτουργεί, όμως φέρνει σε κάθε συνομιλία έναν πάροχο, συχνά και τους υπεκτελούντες την επεξεργασία για λογαριασμό του, ενίοτε και μια άλλη χώρα, και κάθε τέτοιος κρίκος προσθέτει συμβάσεις, αξιολογήσεις και κινδύνους. Όταν το AI τρέχει στους δικούς σας διακομιστές, οι περισσότεροι από αυτούς τους κρίκους βγαίνουν από τη μέση. Η συμμόρφωση δεν γίνεται αυτόματη, αλλά η δουλειά γίνεται μικρότερη, σαφέστερη και ευκολότερο να τεκμηριωθεί.

Ο οδηγός αυτός εξηγεί πού εμφανίζονται προσωπικά δεδομένα σε ένα σύστημα AI, πώς εφαρμόζονται οι βασικές αρχές του ΓΚΠΔ και οι υποχρεώσεις του Κανονισμού για την ΤΝ, πώς βοηθά το Empisto σε καθεμία, και τι μένει στη δική σας ευθύνη.

ΠΟΥ ΒΡΙΣΚΟΝΤΑΙ ΤΑ ΔΕΔΟΜΕΝΑ

Στους δικούς σας διακομιστές. Εκεί μένουν τα έγγραφα, οι ερωτήσεις, οι απαντήσεις και οι καταγραφές.

ΤΡΙΤΟΙ

Κανένας πάροχος AI δεν λαμβάνει τα δεδομένα σας στην κανονική χρήση. Δεν στέλνεται τίποτα πίσω στο Empisto.

ΔΙΑΒΙΒΑΣΕΙΣ

Καμία από προεπιλογή. Κάθε εξωτερική σύνδεση είναι προαιρετική και την ενεργοποιείτε εσείς.

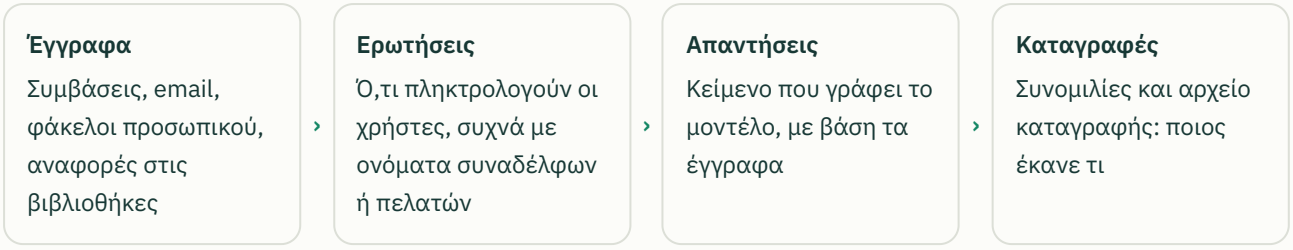
Ο ΡΟΛΟΣ ΣΑΣ

Παραμένετε ο υπεύθυνος επεξεργασίας κατά τον ΓΚΠΔ και ο φορέας εφαρμογής κατά τον Κανονισμό για την ΤΝ.

> **Δεν αποτελεί νομική συμβουλή**
>
> Ο οδηγός αυτός περιγράφει πώς σχετίζεται ο σχεδιασμός του Empisto με τον ΓΚΠΔ και τον Κανονισμό για την ΤΝ. Το αν μια συγκεκριμένη χρήση είναι νόμιμη εξαρτάται από τους σκοπούς σας, τα δεδομένα σας και τον κλάδο σας, και είναι ζήτημα που κρίνετε εσείς και οι σύμβουλοί σας.

02 Πού εμφανίζονται προσωπικά δεδομένα σε ένα σύστημα AI

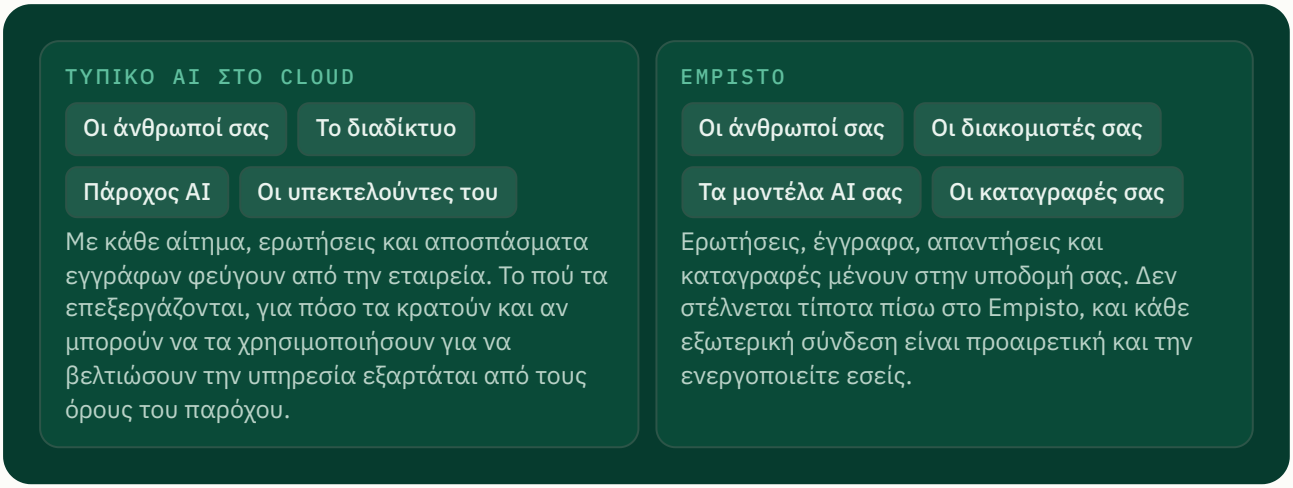
Καλό είναι να ξεκινήσουμε με έναν χάρτη. Σε έναν βοηθό AI που απαντά με βάση εταιρικά έγγραφα, προσωπικά δεδομένα μπορεί να βρεθούν σε τέσσερα σημεία, και για το καθένα πρέπει να απαντηθούν τα ίδια τρία ερωτήματα: πού βρίσκονται, ποιος μπορεί να τα δει και για πόσο διατηρούνται.



Σχήμα 1. Τα τέσσερα σημεία όπου εμφανίζονται προσωπικά δεδομένα σε έναν βοηθό AI. Με το Empisto, μένουν και τα τέσσερα στους διακομιστές σας.

Σε μια τυπική υπηρεσία AI στο cloud, από τον πάροχο περνούν τουλάχιστον οι ερωτήσεις, τα αποσπάσματα που στέλνονται μαζί τους και οι απαντήσεις. Ανάλογα με την υπηρεσία, εκεί μπορεί να αποθηκεύονται και έγγραφα και καταγραφές. Με το Empisto, και τα τέσσερα μένουν στη δική σας υποδομή, με τους κανόνες πρόσβασης που ορίζετε εσείς.

03 Σύγκριση των δύο δρόμων



Σχήμα 2. Οι δύο δρόμοι. Η διαφορά δεν είναι μόνο το πού τρέχει το μοντέλο, αλλά και πόσοι βλέπουν τα δεδομένα σας.

Η διαφορά φαίνεται στα ερωτήματα που καλείται να απαντήσει ένας υπεύθυνος προστασίας δεδομένων.

Ερώτημα	Τυπικό AI στο cloud	Το Empisto στους διακομιστές σας
Ποιος επεξεργάζεται τα δεδομένα;	Εσείς, ο πάροχος AI και συνήθως οι υπεκτελούντες του	Εσείς, στη δική σας υποδομή

Ερώτημα	Τυπικό AI στο cloud	Το Empisto στους διακομιστές σας
Γίνεται διεθνής διαβίβαση;	Συχνά, ανάλογα με τον πάροχο και τους υπεκτελούντες του	Όχι στην κανονική χρήση
Μπορούν τα δεδομένα να χρησιμοποιηθούν για την εκπαίδευση ή τη βελτίωση των μοντέλων του παρόχου;	Εξαρτάται από τον πάροχο, το συνδρομητικό πακέτο και τις ρυθμίσεις	Όχι. Το Empisto δεν έχει πρόσβαση στα δεδομένα σας
Πού φυλάσσονται οι ερωτήσεις και οι απαντήσεις;	Στα συστήματα του παρόχου, με τους δικούς του όρους	Στη δική σας βάση δεδομένων, υπό τον έλεγχό σας
Ποιος μπορεί να αλλάξει τους όρους;	Ο πάροχος	Εσείς και οι δικές σας πολιτικές

04 Ο ΓΚΠΔ, αρχή προς αρχή

Ο ΓΚΠΔ ζητά από ένα σύστημα AI ό,τι ζητά και από κάθε άλλη επεξεργασία. Αυτό που αλλάζει όταν το σύστημα τρέχει στους δικούς σας διακομιστές είναι πόσο μέρος της απάντησης βρίσκεται στα χέρια σας.

Αρχή ή άρθρο του ΓΚΠΔ	Τι ζητά	Πώς βοηθά το Empisto	Τι μένει σε εσάς
Νομιμότητα και περιορισμός του σκοπού (άρθρα 5 και 6)	Νομική βάση για κάθε σκοπό, και καμία χρήση για άλλους σκοπούς	Τα δεδομένα χρησιμοποιούνται μόνο για να απαντηθούν οι ερωτήσεις των χρηστών σας. Κανένας πάροχος δεν τα επαναχρησιμοποιεί για δικούς του σκοπούς	Η επιλογή της νομικής βάσης και ο καθορισμός των σκοπών
Ελαχιστοποίηση των δεδομένων (άρθρο 5)	Μόνο τα δεδομένα που χρειάζονται για τον σκοπό	Οι βιβλιοθήκες και οι χώροι εργασίας περιορίζουν, ομάδα προς ομάδα, από ποια έγγραφα μπορεί να αντλήσει ο βοηθός	Η απόφαση ποιες πηγές θα συνδεθούν και για ποιους
Περιορισμός της περιόδου αποθήκευσης (άρθρο 5)	Τα δεδομένα δεν διατηρούνται περισσότερο απ’ όσο χρειάζεται	Όλα αποθηκεύονται στους διακομιστές σας. Για κάθε είδος δεδομένων μπορεί να οριστεί περίοδος διατήρησης, την οποία εφαρμόζει η πλατφόρμα	Ο ορισμός των περιόδων διατήρησης και η εφαρμογή τους
Ακεραιότητα και εμπιστευτικότητα (άρθρα 5 και 32)	Κατάλληλη ασφάλεια, ανάλογη με τον κίνδυνο	Πρόσβαση ανά βιβλιοθήκη και ρόλο, που κρίνεται πριν από κάθε αναζήτηση· σύνδεση μέσω του παρόχου ταυτότητάς σας· αρχείο καταγραφής που δεν μπορεί να αλλοιωθεί μέσα από το Empisto· κωδικοί σε ειδικό χώρο φύλαξης	Η ασφάλεια των διακομιστών, η κρυπτογράφηση δίσκων, ο σχεδιασμός του δικτύου

Αρχή ή άρθρο του ΓΚΠΔ	Τι ζητά	Πώς βοηθά το Empisto	Τι μένει σε εσάς
Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (άρθρο 25)	Ενσωματωμένη προστασία και, ως προεπιλογή, οι πιο προστατευτικές ρυθμίσεις	AI στο cloud ανενεργό από προεπιλογή· εξωτερικές συνδέσεις ανενεργές μέχρι να ενεργοποιηθούν· προσωπικοί χώροι εργασίας που κανένας διαχειριστής δεν μπορεί να διαβάσει	Η διαμόρφωση των χώρων εργασίας και της πρόσβασης σύμφωνα με τις ανάγκες σας
Εκτελών την επεξεργασία (άρθρο 28)	Σύμβαση με όποιον επεξεργάζεται δεδομένα για λογαριασμό σας	Στην κανονική χρήση, κανένας πάροχος AI δεν επεξεργάζεται τα δεδομένα σας. Οι μηχανικοί του Empisto αποκτούν πρόσβαση σε μια εγκατάσταση μόνο όπως το κανονίσετε εσείς	Η συμφωνία όρων για κάθε πρόσβαση προμηθευτή, μαζί με σύμβαση επεξεργασίας δεδομένων όπου χρειάζεται
Αρχεία δραστηριοτήτων επεξεργασίας (άρθρο 30)	Αρχείο για το τι υφίσταται επεξεργασία και για ποιο λόγο	Σαφής εικόνα του τι αποθηκεύεται πού, και αρχείο καταγραφής της δραστηριότητας	Η τήρηση του αρχείου δραστηριοτήτων επεξεργασίας σας
Εκτίμηση αντικτύπου (άρθρο 35)	Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (DPIA) όταν η επεξεργασία ενδέχεται να ενέχει υψηλό κίνδυνο	Λιγότεροι εμπλεκόμενοι και λιγότερες ροές δεδομένων προς αξιολόγηση, και τεκμηρίωση της αρχιτεκτονικής	Η απόφαση αν χρειάζεται DPIA και η διενέργειά της
Διεθνείς διαβιβάσεις (κεφάλαιο V)	Εγγυήσεις για δεδομένα που φεύγουν από την ΕΕ	Καμία διαβίβαση στην κανονική χρήση, αφού τα δεδομένα μένουν στους διακομιστές σας	Η επιλογή της τοποθεσίας των διακομιστών σας
Δικαιώματα του υποκειμένου των δεδομένων (άρθρα 15 έως 22)	Πρόσβαση, διόρθωση, διαγραφή και φορητότητα, όταν ζητηθούν	Οι χρήστες μπορούν να εξαγάγουν τις συνομιλίες τους, και τα δεδομένα ενός προσώπου μπορούν, κατόπιν αιτήματος, να εξαχθούν ή να διαγραφούν από όλη την πλατφόρμα	Ο χειρισμός των αιτημάτων και η επαλήθευση της ταυτότητας

05 Ο Κανονισμός για την ΤΝ (AI Act)

Ο Κανονισμός για την ΤΝ ρυθμίζει τα συστήματα AI ανάλογα με τον κίνδυνο που ενέχουν, και αναθέτει διαφορετικές υποχρεώσεις στην εταιρεία που διαθέτει ένα σύστημα (τον πάροχο) και σε εκείνη που το χρησιμοποιεί (τον φορέα εφαρμογής). Όταν χρησιμοποιείτε το Empisto, το Empisto είναι ο πάροχος της πλατφόρμας και εσείς ο φορέας εφαρμογής.

Οι υποχρεώσεις του εφαρμόζονται σταδιακά, σε διάστημα αρκετών ετών, και ο Κανονισμός (ΕΕ) 2026/1744 (ψηφιακό Omnibus για την ΤΝ), σε ισχύ από τις 27 Ιουλίου 2026, μετέθεσε αρκετές ημερομηνίες. Η απαγόρευση ορισμένων πρακτικών και η υποχρέωση γραμματισμού στον τομέα της ΤΝ ισχύουν από τον Φεβρουάριο του 2025· το Omnibus διατύπωσε τη δεύτερη ως υποχρέωση στήριξης του προσωπικού και πρόσθεσε νέες απαγορεύσεις από τις 2 Δεκεμβρίου 2026. Οι υποχρεώσεις διαφάνειας εφαρμόζονται από τον Αύγουστο του 2026, και οι πάροχοι συστημάτων παραγωγής περιεχομένου που κυκλοφορούσαν ήδη πριν από τότε έχουν προθεσμία έως τις 2 Δεκεμβρίου 2026 για να επισημαίνουν το περιεχόμενο που παράγουν. Οι κανόνες για τις χρήσεις υψηλού κινδύνου εφαρμόζονται από τις 2 Δεκεμβρίου 2027 για όσες περιλαμβάνονται στο παράρτημα III και από τις 2 Αυγούστου 2028 για το AI που ενσωματώνεται σε προϊόντα του παραρτήματος I. Οι σύμβουλοί σας μπορούν να επιβεβαιώσουν ποιες ημερομηνίες σας αφορούν.

Τι ισχύει συνήθως για έναν εσωτερικό βοηθό AI

Ένας βοηθός που διευκολύνει τους εργαζόμενους να βρίσκουν πληροφορίες σε εταιρικά έγγραφα δεν είναι, κατά κανόνα, σύστημα υψηλού κινδύνου. Οι υποχρεώσεις που συνήθως έχουν σημασία είναι οι εξής.

Υποχρέωση του AI Act	Τι ζητά	Πώς βοηθά το Empisto	Τι μένει σε εσάς
Γραμματισμός στον τομέα της ΤΝ (άρθρο 4)	Μέτρα που στηρίζουν το προσωπικό που χρησιμοποιεί AI να αποκτήσει γραμματισμό στον τομέα της ΤΝ· δεν απαιτείται συγκεκριμένο επίπεδο	Οι απαντήσεις δείχνουν τις πηγές τους, έτσι οι χρήστες μαθαίνουν να τις ελέγχουν	Η εκπαίδευση του προσωπικού σας
Διαφάνεια (άρθρο 50)	Οι άνθρωποι ξέρουν πότε έχουν να κάνουν με AI, και το παραγόμενο περιεχόμενο φέρει σήμανση	Οι απαντήσεις, τα έγγραφα που εξάγονται και ο ήχος που παράγεται επισημαίνονται ως προϊόν AI	Η ενημέρωση του προσωπικού και τρίτων για τον τρόπο που χρησιμοποιείται το AI
Απαγορευμένες πρακτικές (άρθρο 5)	Καμία απαγορευμένη χρήση, όπως η χειραγώγηση ή η κοινωνική βαθμολόγηση	Η πλατφόρμα είναι σχεδιασμένη για απαντήσεις από έγγραφα και για εργασία με επιχειρησιακά συστήματα	Να μην τη χρησιμοποιείτε για απαγορευμένους σκοπούς

Αν τον χρησιμοποιήσετε για σκοπό υψηλού κινδύνου

Ορισμένες χρήσεις χαρακτηρίζονται από τον κανονισμό ως υψηλού κινδύνου, για παράδειγμα στις προσλήψεις και στη διαχείριση προσωπικού, στην αξιολόγηση της πιστοληπτικής ικανότητας ή στην πρόσβαση στην εκπαίδευση και σε βασικές υπηρεσίες. Αν χρησιμοποιείτε σύστημα AI για τέτοιο σκοπό, ισχύουν από τις 2 Δεκεμβρίου 2027 οι υποχρεώσεις του φορέα εφαρμογής (άρθρο 26 του AI Act), μεταξύ άλλων η ανθρώπινη εποπτεία, η παρακολούθηση και η τήρηση αρχείων καταγραφής. Το Empisto στηρίζει αυτή τη δουλειά με απαντήσεις που παραθέτουν τις πηγές τους ώστε να τις ελέγχει

άνθρωπος, με επιβεβαίωση πριν ένα εργαλείο αλλάξει οτιδήποτε, με χώρους εργασίας που κρατούν χωριστά τις ευαίσθητες χρήσεις και με αρχείο καταγραφής που τηρείτε στους δικούς σας διακομιστές. Η απόφαση να χρησιμοποιήσετε AI για τέτοιο σκοπό, καθώς και η αξιολόγηση που τη συνοδεύει, παραμένουν δικές σας.

06 Εμπιστευτικότητα πέρα από την προστασία δεδομένων

Πολλά από όσα θέλουν οι εταιρείες να ρωτήσουν έναν βοηθό AI είναι εμπιστευτικά χωρίς να είναι προσωπικά δεδομένα: όροι συμβάσεων, τιμές, σχέδια, νομικές συμβουλές, υλικό πελατών που καλύπτεται από συμφωνία εμπιστευτικότητας, πληροφορίες που προστατεύει το επαγγελματικό απόρρητο. Αν τα στείλετε σε μια εξωτερική υπηρεσία AI, μπορεί να παραβιάσετε μια δέσμευση που έχετε ήδη αναλάβει, ό,τι κι αν ισχύει από την πλευρά της προστασίας δεδομένων. Όταν το AI τρέχει στους δικούς σας διακομιστές, το υλικό αυτό μένει μέσα στα όρια της εμπιστευτικότητας που έχετε ήδη υποσχεθεί.

Το ίδιο ισχύει για τους κλαδικούς κανόνες που περιορίζουν την εξωτερική ανάθεση ή απαιτούν έλεγχο του πού γίνεται η επεξεργασία των δεδομένων, κανόνες συνηθισμένους στον χρηματοπιστωτικό τομέα, στην υγεία, στις νομικές υπηρεσίες και στον δημόσιο τομέα. Όσο λιγότεροι είναι οι τρίτοι, τόσο λιγότεροι είναι και οι προμηθευτές που πρέπει να εγκριθούν, να καταχωριστούν και να παρακολουθούνται.

07 AI στο cloud, αν το επιλέξετε

Ορισμένες ομάδες ίσως θέλουν ένα μοντέλο στο cloud για εργασίες που δεν είναι ευαίσθητες, όπως η σύνταξη κειμένων προς δημοσίευση. Το Empisto το προσφέρει ανά χώρο εργασίας και ανενεργό από προεπιλογή, κρατά μέσα τα ευαίσθητα έγγραφα, αφαιρεί τα προσωπικά στοιχεία πριν σταλεί οτιδήποτε και καταγράφει κάθε αίτημα. Όταν ένας χώρος εργασίας χρησιμοποιεί μοντέλο στο cloud, τα ερωτήματα του ΓΚΠΔ από τον παραπάνω πίνακα τίθενται ξανά για τον συγκεκριμένο χώρο εργασίας, και ο πάροχος μπαίνει στην αξιολόγησή σας.

08 Προετοιμασία της αξιολόγησής σας

Ο υπεύθυνος προστασίας δεδομένων ή ο υπεύθυνος κανονιστικής συμμόρφωσης μπορεί να περάσει μαζί μας τα παρακάτω σημεία. Το καθένα είναι συνήθως μέρος μιας εκτίμησης αντικτύπου (DPIA) ή του ελέγχου ενός προμηθευτή.

1. **Οι ροές δεδομένων.** Ποιες βιβλιοθήκες και ποια συστήματα συνδέονται, ποιες ομάδες τα χρησιμοποιούν, και επιβεβαίωση ότι καμία εξωτερική σύνδεση δεν είναι ενεργή αν δεν το αποφασίσετε εσείς.
2. **Ο σχεδιασμός της πρόσβασης.** Χώροι εργασίας, βιβλιοθήκες και ρόλοι, αντιστοιχισμένοι στις ομάδες σας και στις ομάδες του εταιρικού καταλόγου σας.
3. **Αρχεία.** Το αρχείο δραστηριοτήτων επεξεργασίας σας, το αρχείο καταγραφής, και για πόσο θα διατηρείτε κάθε είδος δεδομένων.

4. **Άνθρωποι.** Πώς ενημερώνετε το προσωπικό, πώς χειρίζεστε τα αιτήματα των υποκειμένων των δεδομένων και πώς καλλιεργείτε τον γραμματισμό στον τομέα της ΤΝ.
5. **Όροι προμηθευτή.** Η άδεια χρήσης, η υποστήριξη και κάθε πρόσβαση που χρειάζονται οι μηχανικοί μας, με σύμβαση επεξεργασίας δεδομένων όπου οι σύμβουλοί σας την κρίνουν απαραίτητη.

Το τεχνικό κείμενο για την αρχιτεκτονική περιγράφει πού αποθηκεύονται τα δεδομένα και κάθε εξωτερική σύνδεση, και είναι χρήσιμο παράρτημα σε μια τέτοια αξιολόγηση.

09 Διαβάστε επίσης

Το τεχνικό κείμενο για την αρχιτεκτονική εξηγεί πώς είναι φτιαγμένη η πλατφόρμα και πού αποθηκεύονται τα δεδομένα. Η σελίδα «Ασφάλεια» απαντά στις έξι ερωτήσεις που θέτουν πρώτα απ’ όλα οι ομάδες ασφαλείας. Για να συζητήσετε την αξιολόγησή σας με τους ιδρυτές, ξεκινήστε εδώ.