

AI χωρίς διαρροή: οδηγός για δικηγόρους

Επαγγελματικό απόρρητο, GDPR και τρεις τρόποι εργασίας με ψευδωνυμοποίηση.

Για ποιον: δικηγόρους και δικηγορικές εταιρείες που θέλουν να χρησιμοποιούν ChatGPT, Claude ή αντίστοιχα εργαλεία σε δικόγραφα, συμβάσεις, γνωμοδοτήσεις και αλληλογραφία, χωρίς να παραβιάζουν το επαγγελματικό απόρρητο και τον GDPR. **Τι δεν είναι:** νομική συμβουλή για τη δική σας περίπτωση. Είναι ένας πρακτικός τρόπος εργασίας.

1. Το πρόβλημα με μία πρόταση

Το δικηγορικό απόρρητο δεν έχει εξαίρεση για «το έστειλα σε έναν υπολογιστή». Ό,τι εμπιστεύεται ο εντολέας στον δικηγόρο (Κώδικας Δικηγόρων, ν. 4194/2013, άρθρο 38) καλύπτεται από την υποχρέωση εχεμύθειας ανεξάρτητα από το μέσο. Και ό,τι αφορά φυσικά πρόσωπα (εντολές, αντιδίκους, μάρτυρες, εργαζομένους) είναι προσωπικά δεδομένα με τον GDPR να εφαρμόζεται στο ακέραιο.

Παράλληλα, τα εργαλεία AI είναι πραγματικά χρήσιμα: περίληψη ενός δικογράφου 60 σελίδων, πρώτο σχέδιο εξωδίκου, έλεγχος συνέπειας όρων σε σύμβαση, μετάφραση. Το ερώτημα δεν είναι «AI ή όχι». Είναι «πώς, χωρίς να φύγει από το γραφείο αυτό που δεν πρέπει».

2. Τι φεύγει ακριβώς όταν κάνετε επικόλληση

Πάρτε μια συνηθισμένη αγωγή. Περιέχει:

- ονοματεπώνυμο ενάγοντος, εναγομένου, μαρτύρων, συχνά σε τρεις πτώσεις·
- ΑΦΜ, ΑΔΤ, ΑΜΚΑ, διευθύνσεις κατοικίας·
- IBAN και ποσά·
- αριθμούς υποθέσεων, ημερομηνίες γέννησης, πινακίδες οχημάτων·
- συχνά δεδομένα υγείας (ιατρικές βεβαιώσεις σε αγωγές αποζημίωσης) ή ποινικές καταδίκες, δηλαδή ειδικές κατηγορίες των άρθρων 9 και 10 GDPR.

Όταν αυτό επικολληθεί σε ένα εργαλείο AI:

- 1 **Φεύγει από την ΕΕ**, στις περισσότερες περιπτώσεις. Χρειάζεστε νόμιμο εργαλείο διαβίβασης (Κεφάλαιο V GDPR) και το πρέπει να το αναφέρετε στην ενημέρωση προς τους εντολές.
- 2 **Αποθηκεύεται** για όσο ορίζει ο πάροχος. Στις καταναλωτικές εκδόσεις ενδέχεται να χρησιμοποιηθεί για εκπαίδευση, εκτός αν το απενεργοποιήσετε. Στις επιχειρησιακές κατά κανόνα όχι, αλλά αποθηκεύεται για έλεγχο κατάχρησης.
- 3 **Δεν ελέγχετε ποιος το βλέπει** στην πλευρά του παρόχου. Χωρίς σύμβαση επεξεργασίας (άρθρο 28) δεν έχετε καν το δικαίωμα να ρωτήσετε.
- 4 **Το απόρρητο έχει ήδη αρθεί** ως προς τον πάροχο, ακόμη κι αν δεν συμβεί ποτέ τίποτα.

Η λύση δεν είναι να μη χρησιμοποιήσετε το εργαλείο. Είναι να φεύγει **μόνο ό,τι χρειάζεται το εργαλείο για να δουλέψει**, δηλαδή η δομή, τα γεγονότα και το νομικό ζήτημα, και όχι η ταυτότητα των προσώπων.

3. Η μέθοδος: ψευδωνυμοποίηση με επαναφορά

Η ιδέα είναι απλή. Πριν φύγει το κείμενο, κάθε αναγνωριστικό αντικαθίσταται με ένα σταθερό placeholder. Το AI δουλεύει πάνω στα placeholders. Όταν γυρίσει η απάντηση, τα placeholders γίνονται ξανά τα πραγματικά στοιχεία, στον δικό σας υπολογιστή ή λογαριασμό και ποτέ στον πάροχο.

Παράδειγμα, όπως το βλέπει ο δικηγόρος:

Ο ενάγων Γεώργιος Παπαδόπουλος (ΑΦΜ 123456789, ΑΜΚΑ 01018012345), κάτοικος Αθηνών, οδός Σταδίου 10, κατέβαλε στον εναγόμενο Νικόλαο Ιωάννου το ποσό των 12.000 ευρώ στον λογαριασμό GR1601101250000000012300695 την 3η Μαρτίου 2025.

Όπως το βλέπει το AI:

Ο ενάγων [NAME_1] (ΑΦΜ [AFM_1], ΑΜΚΑ [AMKA_1]), κάτοικος [LOCATION_1], [ADDRESS_1], κατέβαλε στον εναγόμενο [NAME_2] το ποσό των 12.000 ευρώ στον λογαριασμό [IBAN_1] την [DATE_1].

Το AI μπορεί να συντάξει την περίληψη, να εντοπίσει την αντίφαση στις ημερομηνίες, να προτείνει δομή για την απάντηση. Δεν έμαθε ποτέ ποιος είναι ο Παπαδόπουλος. Και όταν η απάντηση επιστρέφει με «[NAME_1]», εσείς τη διαβάζετε με «Γεώργιος Παπαδόπουλος».

Δύο λεπτομέρειες που κρίνουν αν δουλεύει στα ελληνικά:

- **Οι πτώσεις.** «Του Παπαδόπουλου» και «τον Παπαδόπουλο» πρέπει να γίνουν το ίδιο [NAME_1]. Αλλιώς το πρόσωπο διαρρέει από τη δεύτερη παράγραφο. Το filterit χρησιμοποιεί ελληνικό μοντέλο αναγνώρισης ονομάτων και κανονικοποίηση κλιτικών τύπων ακριβώς για αυτό.
- **Το ψηφίο ελέγχου.** Ο ΑΦΜ και ο ΑΜΚΑ έχουν εσωτερικό έλεγχο. Ένα εργαλείο που масκάρει «κάθε 9ψηφίο» θα κρύψει και τον αριθμό πρωτοκόλλου· ένα που ελέγχει το ψηφίο ελέγχου масκάρει τον ΑΦΜ και αφήνει το πρωτόκολλο. Αυτό αλλάζει την ποιότητα της απάντησης.

4. Τρεις τρόποι εργασίας, ανάλογα με το πώς δουλεύετε

4.1 «Ψευδωνυμοποίηση πρώτα»: για έγγραφα

Ανοίγετε τον Anonymizer του filterit, επικολλάτε το κείμενο ή ανεβάζετε το Word/PDF (και σκαναρισμένα, με OCR). Βλέπετε κάθε εύρημα με τον τύπο του, αφαιρείτε ή προσθέτετε ό,τι θέλετε με το χέρι, και παίρνετε την ψευδωνυμοποιημένη έκδοση. Αυτή τη στέλνετε όπου θέλετε: σε οποιοδήποτε AI, σε εξωτερικό συνεργάτη, σε μεταφραστή. Όταν γυρίσει το αποτέλεσμα, το επικολλάτε πίσω και το filterit επαναφέρει τα πραγματικά στοιχεία.

Πότε: γνωμοδοτήσεις, μεγάλα δικόγραφα, οτιδήποτε θέλετε να ελέγξετε πριν φύγει.

4.2 «Chat με επαναφορά»: για καθημερινή δουλειά

Μέσα στην εφαρμογή του filterit υπάρχει chat. Γράφετε κανονικά, με τα πραγματικά ονόματα. Η μάσκα μπαίνει αυτόματα πριν φύγει η ερώτηση, και η απάντηση έρχεται με τα ονόματα επαναφερμένα. Στο πλάι βλέπετε τι ακριβώς масκαρίστηκε. Αυτό είναι και το αρχείο σας.

Πότε: σύνταξη email, πρώτα σχέδια, ερωτήσεις πάνω σε ένα έγγραφο που ανεβάσατε.

4.3 «Το εργαλείο που ήδη χρησιμοποιώ»: ChatGPT, Claude, Copilot

Αν το γραφείο έχει ήδη συνδρομές, δεν χρειάζεται να αλλάξετε συνήθειες. Η επέκταση browser του filterit масκάρει το κείμενο στο πεδίο του ChatGPT ή του Claude τη στιγμή που πατάτε Enter, και επαναφέρει τα

ονόματα στην απάντηση όπως εμφανίζεται στην οθόνη σας. Για Windows, ο desktop agent κάνει το ίδιο για όλες τις εφαρμογές, όχι μόνο τον browser, και ο διαχειριστής του γραφείου ορίζει κεντρικά τι μασκάρεται.

Πότε: γραφεία που θέλουν την προστασία «από προεπιλογή» χωρίς να εκπαιδεύσουν κάθε συνεργάτη σε νέα ροή.

5. Τι δεν κάνει καμία τεχνολογία, και τι κάνετε εσείς

- **Δεν είναι 100%.** Ένα σπάνιο επώνυμο, ένα παρατσούκλι, «ο γιος του ιδιοκτήτη του φούρνου στη γωνία» μπορεί να μην αναγνωριστούν. Το filterit δημοσιεύει τους αριθμούς ακρίβειας στη σελίδα /accuracy· διαβάστε τους, και **ελέγχετε την προεπισκόπηση** πριν στείλετε κάτι κρίσιμο. Η επαναφορά τιμών δουλεύει μόνο εκεί όπου φυλάσσεται ο πίνακας αντιστοίχισης.
- **Το πλαίσιο ταυτοποιεί.** «Ο μοναδικός συμβολαιογράφος του νησιού» είναι ταυτοποιήσιμος και χωρίς όνομα. Για υποθέσεις με λίγα πρόσωπα σε μικρή κοινότητα, μασκάρετε και τις τοποθεσίες ή αφαιρέστε τα περιγραφικά.
- **Το AI δεν είναι πηγή δικαίου.** Επινοεί αριθμούς αποφάσεων και άρθρα με αυτοπεποίθηση. Ελέγχετε κάθε παραπομπή. Αυτό δεν είναι θέμα διαρροής, αλλά είναι θέμα ευθύνης.
- **Ο πίνακας αντιστοίχισης είναι το κλειδί του απορρήτου.** Πρέπει να είναι κρυπτογραφημένος, με πρόσβαση μόνο από το γραφείο, με διαγραφή όταν κλείσει η υπόθεση. Στο filterit φυλάσσεται κρυπτογραφημένος (AES-256-GCM) σε υποδομή εντός ΕΕ, ανά λογαριασμό, με επιλογή δικού σας κλειδιού για οργανισμούς.

6. Checklist για το δικηγορικό γραφείο

- ☐ Έχουμε γραπτή απόφαση ποια εργαλεία AI επιτρέπονται και με ποιους λογαριασμούς (όχι προσωπικοί δωρεάν).
- ☐ Έχουμε σύμβαση επεξεργασίας με κάθε πάροχο AI που λαμβάνει κείμενο (άρθρο 28 GDPR), ή στέλνουμε μόνο ψευδωνυμοποιημένο κείμενο.
- ☐ Η ψευδωνυμοποίηση είναι η προεπιλογή στη ροή εργασίας, όχι επιλογή του κάθε συνεργάτη.
- ☐ Δεδομένα υγείας και ποινικών καταδικών δεν φεύγουν, ούτε ψευδωνυμοποιημένα, χωρίς έγκριση εταίρου.
- ☐ Κάθε αποτέλεσμα AI ελέγχεται από δικηγόρο πριν χρησιμοποιηθεί.
- ☐ Ενημερώνουμε τους εντολείς στην ενημέρωση απορρήτου ότι χρησιμοποιούμε εργαλεία AI με ψευδωνυμοποίηση (άρθρο 13 GDPR).
- ☐ Έχουμε αρχείο του τι μασκαρίστηκε και πότε, για περίπτωση ερωτήματος εντολέα ή της Αρχής.
- ☐ Έχουμε πει στους συνεργάτες τι να κάνουν αν κάτι έφυγε χωρίς μάσκα (άρθρο 33: 72 ώρες).
- ☐ Οι συνεργάτες έχουν περάσει βασική ενημέρωση για τα εργαλεία AI (Κανονισμός 2024/1689, άρθρο 4).

7. Συχνές ερωτήσεις

Μπορώ να ανεβάσω σκαναρισμένη απόφαση; Ναι. Το filterit κάνει OCR σε ελληνικά και αγγλικά και, για PDF και εικόνες, προσφέρει και οπτική απαλοιφή: μαύρα ορθογώνια πάνω στα στοιχεία, στις

υπογραφές και στις σφραγίδες, με προεπισκόπηση πριν την εφαρμογή.

Τα placeholders μπερδεύουν το AI; Όχι στην πράξη. Τα μοντέλα χειρίζονται το «[NAME_1] κατέβαλε στον [NAME_2]» όπως θα χειρίζονταν «ο Α κατέβαλε στον Β». Η συνέπεια των placeholders μέσα στο ίδιο έγγραφο είναι αυτό που μετρά, και είναι εγγυημένη.

Τι γίνεται με τα ονόματα εταιρειών; Δεν είναι προσωπικά δεδομένα, αλλά συχνά είναι εμπιστευτικά. Μπορείτε να τα προσθέσετε στη μάσκα με το χέρι ή μέσω κανόνων του γραφείου.

Πού φυλάσσεται η υπόθεση; Στο filterit φυλάσσονται μόνο ψευδωνυμοποιημένα κείμενα και ο κρυπτογραφημένος πίνακας αντιστοίχισης. Τα αρχεία που ανεβάζετε δεν αποθηκεύονται μόνιμα. Για γραφεία που δεν θέλουν καμία εξάρτηση από υποδομή τρίτου, υπάρχουν εκδόσεις αποκλειστικού διακομιστή και εγκατάστασης στο γραφείο.

Είναι αρκετό για να πω στον εντολέα ότι «δεν φεύγουν τα στοιχεία του»; Μπορείτε να πείτε ότι τα στοιχεία ταυτοποίησής του ψευδωνυμοποιούνται πριν από κάθε χρήση εργαλείου AI και ότι ο πάροχος του AI δεν τα λαμβάνει. Μην πείτε «ανωνυμοποιούνται». Δεν είναι το ίδιο, και ο εντολέας σας ίσως το ξέρει.

Το παρόν είναι γενική ενημέρωση και όχι νομική συμβουλή. Αναφορές: Κώδικας Δικηγόρων (ν. 4194/2013), Κανονισμός (ΕΕ) 2016/679 (GDPR), ν. 4624/2019, Κανονισμός (ΕΕ) 2024/1689 (AI Act). Τα παραδείγματα προσώπων και αριθμών είναι επινοημένα. Έκδοση Σεπτεμβρίου 2026 · filterit.app