GDPR και επαγγελματική ανταλλαγή μηνυμάτων: γιατί οι περισσότεροι παραβιάζουν τους κανόνες χωρίς να το γνωρίζουν

Σχεδόν κάθε γραφείο, ιατρείο ή συμβουλευτική εταιρεία στέλνει έγγραφα πελατών μέσω εφαρμογών των οποίων ο διακομιστής βρίσκεται εκτός του Ευρωπαϊκού Οικονομικού Χώρου. Χωρίς κακή πρόθεση, αλλά σε πολλές περιπτώσεις παραβιάζοντας τον κανονισμό, χωρίς κανείς να τους έχει προειδοποιήσει.

Το έγγραφο που ταξιδεύει περισσότερο απ' όσο νομίζετε

Μια καθημερινή κατάσταση: μια φοροτεχνική σύμβουλος λαμβάνει μέσω μηνυμάτων ένα έγγραφο με δεδομένα πελάτη. Ένας πωλητής προωθεί μέσω chat μια προσφορά σε έναν συνάδελφο. Μια γιατρός μοιράζεται με τον ίδιο τρόπο μια κλινική αναφορά με έναν συνεργάτη. Κανείς δεν το σκέφτεται δεύτερη φορά. Είναι φυσιολογικό. Είναι βολικό. Είναι αυτό που γίνεται κάθε μέρα σε κάθε γραφείο σε κάθε ευρωπαϊκή πόλη.

Αλλά αυτό το έγγραφο, σε πολλές περιπτώσεις, μόλις ταξίδεψε σε έναν διακομιστή στις Ηνωμένες Πολιτείες. Αποθηκεύτηκε –έστω και προσωρινά, έστω και «κρυπτογραφημένο σε ηρεμία»– σε ένα σύννεφο που ούτε ο επαγγελματίας ούτε ο πελάτης του ελέγχουν. Πέρασε από συστήματα που μπορούν τεχνικά να ευρετηριάσουν μεταδεδομένα που σχετίζονται με το περιεχόμενο. Και ο ευρωπαϊκός Γενικός Κανονισμός για την Προστασία Δεδομένων έχει κάτι πολύ σαφές να πει γι' αυτό.

Τι απαιτεί ο κανόνας

Το GDPR –και κατ' επέκταση η νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ιδίως η απόφαση Schrems II, C-311/18, του 2020)– ορίζει ότι τα προσωπικά δεδομένα των Ευρωπαίων πολιτών πρέπει να προστατεύονται κατάλληλα. Εάν αυτά τα δεδομένα εγκαταλείψουν τον Ευρωπαϊκό Οικονομικό Χώρο, ο υπεύθυνος επεξεργασίας πρέπει να εγγυηθεί ότι ο παραλήπτης προσφέρει ένα επίπεδο προστασίας «ουσιωδώς ισοδύναμο» με το ευρωπαϊκό. Στην πράξη, αυτό σημαίνει ότι η αποστολή δεδομένων πελατών μέσω υπηρεσιών των οποίων οι διακομιστές υπάγονται στη δικαιοδοσία των ΗΠΑ, χωρίς να έχει διενεργηθεί εκτίμηση αντικτύπου και χωρίς να έχουν εφαρμοστεί συμπληρωματικές εγγυήσεις –τυποποιημένες συμβατικές ρήτρες, πρόσθετα τεχνικά μέτρα όπως επαληθεύσιμη κρυπτογράφηση κ.λπ.– μπορεί να αποτελεί παραβίαση του κανονισμού. Ακόμα κι αν μέχρι στιγμής κανείς δεν έχει πει τίποτα.

Και δεν είναι μόνο το περιεχόμενο των μηνυμάτων. Τα μεταδεδομένα –ποιος στέλνει τι σε ποιον, πότε, πόσο συχνά, από πού– είναι επίσης προσωπικά δεδομένα σύμφωνα με τους κανονισμούς, σύμφωνα με την επανειλημμένη ερμηνεία του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων. Μια υπηρεσία που συλλέγει μεταδεδομένα από την επαγγελματική επικοινωνία ενός χρήστη επεξεργάζεται προσωπικά δεδομένα των πελατών αυτού του χρήστη, χωρίς αυτοί να το γνωρίζουν ή να έχουν δώσει οποιαδήποτε συγκατάθεση για μια τέτοια επεξεργασία.

Το σύνηθες σχήμα σκέψης –«χρησιμοποιώ την εφαρμογή μόνο για να γράφω· η εφαρμογή δεν είναι πάροχος δεδομένων του πελάτη μου»– είναι νομικά εσφαλμένο. Εάν τα δεδομένα του πελάτη περάσουν από την υποδομή

ενός τρίτου, αυτός ο τρίτος επεξεργάζεται αυτά τα δεδομένα. Και αν τα επεξεργάζεται, πρέπει να υπάρχει νομική βάση, σύμβαση επεξεργασίας δεδομένων και κατάλληλες εγγυήσεις.

Ποιος είναι υπεύθυνος

Το ερώτημα ποιος φέρει τη νομική ευθύνη δεν είναι ακαδημαϊκό. Το GDPR διακρίνει μεταξύ του *υπευθύνου επεξεργασίας* (ποιος αποφασίζει ποια δεδομένα επεξεργάζονται και για ποιο σκοπό) και του *εκτελούντος την επεξεργασία* (ποιος το κάνει υλικά για λογαριασμό του υπευθύνου). Ο επαγγελματίας που στέλνει έγγραφα πελατών είναι ο υπεύθυνος επεξεργασίας. Ο πάροχος της εφαρμογής μηνυμάτων είναι σε πολλές περιπτώσεις de facto εκτελών την επεξεργασία. Χωρίς σύμβαση επεξεργασίας –και χωρίς τις περισσότερες από τις ρήτρες που θα έπρεπε να περιλαμβάνει μια τέτοια σύμβαση– ο υπεύθυνος δεν έχει εκπληρώσει την υποχρέωσή του.

Η επιεικής ερμηνεία λέει: «οι περισσότεροι επαγγελματίες δεν το γνωρίζουν». Η αυστηρή ερμηνεία λέει: «η άγνοια του νόμου δεν δικαιολογεί την παραβίασή του». Και η ερμηνεία οποιουδήποτε εξειδικευμένου δικηγόρου προστασίας δεδομένων που ερωτάται σχετικά είναι συνήθως η αυστηρή.

Για ποιον είναι αυτό σημαντικό στην πράξη

Για κάθε επαγγελματία ή επιχείρηση που έστω και περιστασιακά διαχειρίζεται προσωπικές πληροφορίες τρίτων:

- Δικηγόροι που λαμβάνουν τεκμηρίωση πελατών (συμβόλαια, αγωγές, δηλώσεις, αναφορές περιουσιακών στοιχείων).
- Γιατροί και άλλοι επαγγελματίες υγείας που μοιράζονται δεδομένα υγείας –τα οποία θεωρούνται *ειδικές κατηγορίες* βάσει του άρθρου 9 του GDPR με ενισχυμένο καθεστώς προστασίας–.
- Φοροτεχνικοί και διοικητικοί διαχειριστές που διαχειρίζονται δεδομένα ταυτοποίησης, φορολογικά και τραπεζικά δεδομένα.
- Τμήματα Ανθρώπινου Δυναμικού που διαχειρίζονται την εργασιακή και προσωπική τεκμηρίωση των εργαζομένων.
- Εμπορικοί αντιπρόσωποι που λαμβάνουν στοιχεία επικοινωνίας και συχνά ευαίσθητες επιχειρηματικές πληροφορίες από υποψήφιους και υπάρχοντες πελάτες.

Σε όλες τις περιπτώσεις, οι πληροφορίες προστατεύονται από το GDPR. Σε όλες τις περιπτώσεις, στη συνήθη πρακτική, οι πληροφορίες αυτές ρέουν μέσω καναλιών των οποίων η δικαιοδοσία δεν επιτρέπει τη δήλωσή τους ως «ουσιωδώς ισοδύναμων» με το ευρωπαϊκό πλαίσιο χωρίς πρόσθετες εγγυήσεις. Όχι από κακή πρόθεση. Από συνήθεια. Και λόγω μιας τεχνολογικής υποδομής που για δεκαπέντε χρόνια έθετε την ευκολία πάνω από τη συμμόρφωση.

Το επιχείρημα «όλοι το κάνουν»

Είναι σκόπιμο να προβλέψουμε την πιο συνηθισμένη αντίρρηση: «εάν όλοι το κάνουν, δεν μπορεί να είναι πραγματικό πρόβλημα». Είναι ένα απολύτως κατανοητό επιχείρημα και νομικά δεν έχει καμία ισχύ. Το γεγονός ότι μια πρακτική είναι διαδεδομένη δεν την καθιστά σύμφωνη με τον κανονισμό. Οι αρχές προστασίας δεδομένων (όπως η ΑΠΔΠΧ στην Ελλάδα) έχουν επιβάλει κυρώσεις τα τελευταία χρόνια σε αρκετές εταιρείες ακριβώς για τρόπους χρήσης των μηνυμάτων που φαινόταν ακίνδυνοι μέχρι τη στιγμή του ελέγχου.

Η τρέχουσα λειτουργική πραγματικότητα είναι ότι ο κίνδυνος ως προς την πιθανότητα είναι χαμηλός –είναι πολύ σπάνιο ένας έλεγχος της Αρχής να ελέγξει τα συγκεκριμένα εργαλεία μηνυμάτων ενός μεσαίου μεγέθους γραφείου– αλλά υψηλός ως προς τον αντίκτυπο εάν υλοποιηθεί. Είναι ένας κίνδυνος που οι περισσότεροι αναλαμβάνουν χωρίς να γνωρίζουν ότι τον αναλαμβάνουν. Δηλαδή, χωρίς να έχουν αξιολογήσει εάν το εργαλείο που χρησιμοποιείται είναι σύμφωνο με τη νομική ευθύνη του υπευθύνου επεξεργασίας.

Το ψηφιακό αποτύπωμα είναι αναδρομικό

Υπάρχει ένα δεύτερο επιχείρημα, σχεδόν συμμετρικό με το προηγούμενο, που αξίζει να προβλέψουμε: *«εάν αυτό ήταν σοβαρό πρόβλημα, η διοίκηση θα είχε ήδη αρχίσει να το ελέγχει»*. Η τρέχουσα παρατηρούμενη πραγματικότητα του δίνει επιφανειακά δίκιο. Οι έλεγχοι για ακατάλληλη χρήση μηνυμάτων σε μικρές επιχειρήσεις και ειδικά σε ελεύθερους επαγγελματίες είναι σήμερα σχεδόν ανύπαρκτοι –όχι επειδή η συμπεριφορά επιτρέπεται, αλλά επειδή η διοίκηση στην Ελλάδα και σε μεγάλο μέρος της ΕΕ στερείται των ανθρώπινων πόρων που απαιτούνται για τον έλεγχο εκατομμυρίων υπόχρεων.

Αυτό υποδηλώνει η σημερινή παρατηρούμενη πρακτική. Αλλά δεν είναι αυτό που υποδηλώνει η επόμενη δεκαετία. Δύο φορείς συγκλίνουν για να αλλάξουν την ισορροπία σε σχετικά σύντομα χρονικά διαστήματα.

Πρώτον: το ψηφιακό αποτύπωμα είναι αναδρομικό. Κάθε μήνυμα που αποστέλλεται μέσω μιας εφαρμογής με κεντρικό διακομιστή παραμένει καταγεγραμμένο –τουλάχιστον στα μεταδεδομένα– σε μια υποδομή που παραμένει. Αυτό που στάλθηκε πριν από έξι μήνες είναι τεχνικά ακόμα ελέγξιμο σήμερα. Αυτό που στέλνεται σήμερα θα είναι ελέγξιμο σε πέντε χρόνια. Η απουσία ενός τρέχοντος ελέγχου δεν αποτελεί εγγύηση για την απουσία ενός μελλοντικού ελέγχου. Είναι μια αναβολή της αξιολόγησης, όχι μια απαλλαγή.

Δεύτερον: η ικανότητα διοικητικού ελέγχου θα αυξηθεί επιταχυνόμενα. Η εισαγωγή εργαλείων τεχνητής νοημοσύνης στις διαδικασίες ελέγχου εξαλείφει το ανθρώπινο εμπόδιο που μέχρι τώρα προστάτευε –de facto, όχι de jure– τις μικρές επιχειρήσεις και τους ελεύθερους επαγγελματίες. Ένα σύστημα ικανό να διασταυρώνει μαζικά μεταδεδομένα, φορολογικές δηλώσεις, εμπορικά μητρώα και υποχρεώσεις κοινοποίησης παραβιάσεων ασφάλειας δεν χρειάζεται επιθεωρητές: χρειάζεται πρόσβαση. Και η πρόσβαση μέσω αιτημάτων προς παρόχους με νομική παρουσία στην ΕΕ εντός του τρέχοντος κανονιστικού πλαισίου είναι απόλυτα εφικτή.

Σε αυτό προστίθεται ένας λιγότερο τεχνικός αλλά εξίσου καθοριστικός παράγοντας: τα ευρωπαϊκά κράτη βρίσκονται σε μια διαδικασία συνεχώς αυξανόμενης χρέωσης και πρέπει, σχεδόν χωρίς εξαίρεση, να διευρύνουν τη φορολογική τους βάση. Η διοικητική κύρωση που απορρέει από τη μη συμμόρφωση με το GDPR είναι σε καθαρά δημοσιονομικούς όρους μια αυξανόμενη και πολιτικά βολική πηγή εσόδων. Αυτό δεν είναι υπόθεση: είναι μια παρατηρήσιμη τάση στις ετήσιες εκθέσεις των ευρωπαϊκών αρχών προστασίας δεδομένων, όπου ο συνολικός όγκος των κυρώσεων αυξάνεται για αρκετά συνεχόμενα οικονομικά έτη.

Το λειτουργικό συμπέρασμα για τον υπεύθυνο επεξεργασίας δεν είναι κινδυνολογικό αλλά νηφάλιο: **η απόφαση για το πώς διαχειρίζεται σήμερα η επικοινωνία με τους πελάτες αξιολογείται έναντι της ικανότητας ελέγχου του έτους κατά το οποίο έρχεται ο έλεγχος, όχι έναντι της τρέχουσας.** Και αυτή η ικανότητα θα είναι, σε εύλογο χρονικό διάστημα, ουσιαστικά διαφορετική από τη σημερινή. Όποιος αρχίσει να κάνει τα πράγματα σωστά σήμερα δεν θα είναι εντάξει μόνο από σήμερα: το αποτύπωμα που δημιουργείται από αυτή τη στιγμή και μετά θα είναι σύμφωνο με τον κανόνα, και αυτό προστατεύει αναδρομικά την επερχόμενη περίοδο. Όποιος συνεχίσει όπως μέχρι τώρα θα συσσωρεύει ένα ελέγξιμο αποτύπωμα του οποίου η συμμόρφωση θα αξιολογηθεί σύμφωνα με τα πρότυπα –και τους πόρους– των επόμενων ετών.

Τι αλλάζει με μια διαφορετική αρχιτεκτονική

Υπάρχουν τεχνικές εναλλακτικές λύσεις όπου τα δεδομένα δεν αποθηκεύονται σε υποδομές τρίτων, αλλά ταξιδεύουν απευθείας από τη συσκευή του αποστολέα σε αυτήν του παραλήπτη. Σε αυτήν την αρχιτεκτονική, η συμμόρφωση με το GDPR όσον αφορά τις διεθνείς διαβιβάσεις δεν εξαρτάται από τυποποιημένες συμβατικές ρήτρες, ούτε από την καλή θέληση του παρόχου ή από μελλοντικούς ελέγχους. Εξαρτάται από το γεγονός ότι *δεν υπάρχει διαβίβαση*. Και ό,τι δεν υπάρχει δεν μπορεί να παραβιαστεί.

Αυτή δεν είναι η μόνη λύση ούτε η μόνη δυνατή. Αλλά είναι δομικά διαφορετική και η κανονιστική συμμόρφωση παύει να είναι ένα διαδικαστικό παράρτημα και γίνεται άμεση συνέπεια του σχεδιασμού. Για έναν επαγγελματία που παίρνει σοβαρά την ευθύνη του ως υπεύθυνος επεξεργασίας, αυτή η διαφορά έχει σημασία.

Το επόμενο τεύχος του Cuadernos θα αναλύσει λεπτομερώς την απόφαση Schrems II και τις πρακτικές επιπτώσεις της για τις μικρές και μεσαίες επιχειρήσεις που εξαρτώνται από υπηρεσίες cloud των ΗΠΑ, πέντε χρόνια μετά τη

δημοσίευσή της.

Πηγές και κανονιστικό πλαίσιο

- Κανονισμός (ΕΕ) 2016/679 (GDPR), ιδίως το Κεφάλαιο V σχετικά με τις διεθνείς διαβιβάσεις.
- ΔΕΕ C-311/18 («Schrems II»), 16 Ιουλίου 2020.
- ΕΣΠΔ – Συστάσεις 01/2020 σχετικά με μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης.
- Αρχές Προστασίας Δεδομένων (συμπεριλαμβανομένης της ΑΠΔΠΧ) – Ετήσιες εκθέσεις με περιπτώσεις κυρώσεων για ακατάλληλη χρήση άμεσων μηνυμάτων σε επαγγελματικά περιβάλλοντα.

← ΠροηγούμενοΤο επαγγελματικό απόρρητο στην ψηφιακή εποχήΕπόμενο →Όταν δεν υπάρχει κανείς στη μέση

Πρόσφατα αναγνώσματα

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Πάρτε αυτό το άρθρο μαζί σας όπου το χρειάζεστε.

↓ Markdown ↓ Απλό κείμενο ↓ PDF

Το αρχείο θα ληφθεί στη συσκευή σας. Από εκεί μπορείτε να το αποθηκεύσετε, να το εισαγάγετε στο Solo2 ή να το μοιραστείτε όπου θέλετε. Το Cuadernos δεν αποφασίζει τον προορισμό για εσάς.

Σφραγίδα από βουλοκέρι · SHA-256
5c4e54d91f521bb13a9e190dd566c783b83bb284b0593fad1e49854bf01aa359

Cuadernos Lacre · Μια έκδοση της Menzuri Gestión S.L. ·
γραμμένη από τον R.Eugenio · επιμελημένη από την ομάδα του Solo2.