**Πρότυπο για την τεκμηρίωση**

**μιας δραστηριότητας επεξεργασίας**

**σύμφωνα με το άρθρο 30 του ΓΚΠΔ**

|  |  |
| --- | --- |
| **Περιγραφή της δραστηριότητας επεξεργασίας** | *Η ονομασία πρέπει να περιγράφει σύντομα και συνοπτικά την εν λόγω επεξεργασία. Παραδείγματα: Διαχείριση προσωπικού, λογιστική, διαχείριση δεδομένων έργου, χειρισμός δεδομένων εφαρμογών, διαχείριση έργου, οργάνωση μαθημάτων κατάρτισης κ.λπ.* |
| **Σκοπός της επεξεργασίας** | *Για ποιο λόγο επεξεργάζεστε τα δεδομένα; Ποιος είναι ο σκοπός της επεξεργασίας;*  *Παραδείγματα:*   * *Επεξεργασία δεδομένων στο πλαίσιο της απασχόλησης* * *Διασφάλιση της λειτουργίας του οργανισμού ή της εταιρείας* * *Εγυηση γενικών μέτρων ασφαλείας* * *Παροχή υποδομής για τη λειτουργία του οργανισμού ή της εταιρείας* * *Κατάρτιση, εκτέλεση ή καταγγελία συμβάσεων αγοράς ή παροχής υπηρεσιών* * *Παραγωγή προϊόντων και υπηρεσιών* |
| Αρμόδιο τμήμα | *Ποιο τμήμα του οργανισμού ή της εταιρείας σας είναι υπεύθυνο για την επεξεργασία;* |
| Υπεύθυνος επικοινωνίας | *Αναφέρετε έναν εσωτερικό υπέυθυνο επικοινωνίας ή το άτομο που είναι υπέυθυνο για τη διαδικασία (Ιδιοκτήτης Επιχειρησιακών Διαδικασιών.* |
| Περιγραφή διαδικασίας | *Σύντομη περιγραφή της επεξεργασίας. (προαιρετικά)*  *Περιγράφει με σύντομο τρόπο την εσωτερική διαδικασία. Αυτό γίνεται μόνο για λόγους επεξήγησης και καλύτερης κατανόησης.* |
| Ομάδες υποκειμένων δεδομένων | *Αναφέρετε τις κατηγορίες υποκειμένων που υπόκεινται σε επεξεργασία. Πιθανές κατηγορίες είναι π.χ.*   * *Εργαζόμενοι/ες* * *Ενδιαφερόμενοι/ες* * *Προμηθευτές* * *Πελάτες/ισσες* * *…* |
| Κατηγορίες δεδομένων | *Αναφέρετε τις κατηγορίες δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων που υπόκεινται σε επεξεργασία στο πλαίσιο της συγκεκριμένης επεξεργασίας.*  *Θα πρέπει να αφιερώσετε χρόνο σε αυτό το στάδιο και να εξετάσετε προσεκτικά ποια δεδομένα των υποκειμένων των δεδομένων υπόκεινται σε επεξεργασία. Αυτό εξαρτάται σε μεγάλο βαθμό από τη συγκεκριμένη επεξεργασία.*  *π.χ. (Παρακαλούμε να είστε όσο το δυνατόν πιο συγκεκριμένοι/ες)*   * *Προσωπικά κύρια δεδομένα (π.χ. όνομα, ημερομηνία γέννησης, οικογενειακή κατάσταση κ.λπ.)* * *Δεδομένα επικοινωνίας (π.χ. ταχυδρομική διεύθυνση, διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμός τηλεφώνου κ.λπ.)* * *Κύρια δεδομένα εργαζόμενων (π.χ. φορολογική κατηγορία εισοδήματος, αριθμός προσωπικού, κ.λπ.)* * *Δεδομένα χρήσης (π.χ. συμπεριφορά πλοήγησης, αγοραστική συμπεριφορά, δεδομένα πρόσβασης κ.λπ.)* * *Δεδομένα σύμβασης (π.χ. αριθμός σύμβασης, περιεχόμενο σύμβασης, τρόποι μισθοδοσίας κ.λπ.)* * *Χαρακτηριστικά αναγνώρισης και αριθμοί αναγνώρισης (π.χ. αριθμός δελτίου ταυτότητας, αριθμός διαβατηρίου, αριθμός φορολογικού μητρώου κ.λπ.)* * *Δεδομένα μισθοδοσίας προσωπικού (π.χ. ημερομίσθιο/μισθός, μπόνους, εισφορές ασφάλισης υγείας, λοιπές κρατήσεις κ.λπ.)* * *Δεδομένα πελατών (π.χ. όροι, ιστορικό παραγγελιών, συμπεριφορά πληρωμών κ.λπ.)* * *Δεδομένα πληρωμών (π.χ. τραπεζικός λογαριασμός, στοιχεία πιστωτικών καρτών κ.λπ.)* * *Δεδομένα σχετικά με την αίτηση (π.χ. συστάσεις, έγγραφα αίτησης κ.λπ.)* * *Δεδομένα προμηθευτών (Υπεύθυνοι επικοινωνίας και στοιχεία επικοινωνίας τους, κ.λπ.)* * *Επιβαλλόμενα δεδομένα (δεδομένα που το υποκείμενο των δεδομένων διαβιβάζει οικειοθελώς)* * *….* |
| Ειδικά προσωπικά δεδομένα | **Γίνεται επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 9;**  *Ναι / όχι*  *Ο ΓΚΠΔ ορίζει τα ιδιαίτερα ευαίσθητα δεδομένα στο άρθρο 9. Σε περίπτωση επεξεργασίας τέτοιων δεδομένων σας συνιστούμε ανεπιφύλακτα να διενεργήσετε εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων (DPIA). Θα πρέπει επίσης να συμβουλευτείτε έναν εμπειρογνώμονα προστασίας δεδομένων ή νομικό σύμβουλο.*  *Σημείωση: Πρόκειται για «δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.» (δεδομένα σύμφωνα με το άρθρο 9 παράγραφος 1 του ΓΚΠΔ)* |
| **Κατηγορίες αποδεκτών στους οποίους κοινοποιήθηκαν ή θα κοινοποιηθούν τα δεδομένα προσωπικού χαρακτήρα (σύμφωνα με το άρθρο 30 παράγραφος 1 στοιχείο δ) ΓΚΠΔ)** | |
| Εσωτερικοί αποδέκτες | *Λίστα εσωτερικών αποδεκτών (π.χ. μεμονωμένα τμήματα ή ομάδες ανθρώπων)*  *π.χ.*   * *λογιστική* * *διοίκηση* * *τμήμα πληροφοριακών συστημάτων* * *άλλοι αποδέκτες σε περίπτωση ανάγκης* * *…* |
| Εξωτερικοί αποδέκτες | *Οι εξωτερικοί αποδέκτες είναι κυρίως πάροχοι υπηρεσιών ή αρχές, οι οποίοι είτε έχουν πρόσβαση στα δεδομένα είτε στους οποίους διαβιβάζονται τα δεδομένα. Εδώ αναφέρονται και οι πάροχοι λύσεων λογισμικού που θεωρητικά έχουν πρόσβαση στα αποθηκευμένα δεδομένα.*  *π.χ.*   * *φοροτεχνικός σύμβουλος* * *Πάροχος υπηρεσιών XYZ (δώστε όνομα κι τύπο)* * *…* |
| Μεταφορά δεδομένων (σύμφωνα με το άρθρο 30 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ) | *Προσέξτε σε αυτό το σημείο εάν τα δεδομένα μεταφέρονται σε τρίτη χώρα. Αυτό συμβαίνει συχνά όταν χρησιμοποιείτε παρόχους υπηρεσιών (ιδίως παρόχους υπηρεσιών διαδικτύου και λύσεις λογισμικού από το Cloud).*  *Για το σημείο αυτό προσέξτε είτε ότι «η μεταφορά δεδομένων δεν πραγματοποιείται και δεν προβλέπεται», είτε ότι «τα δεδομένα μεταφέρονται σε τρίτη χώρα» και στη συνέχεια περιγράψτε ποια μεταφορά πραγματοποιείται.*  *Σημείωση: Η τρίτη χώρα θα πρέπει πάντα να προσδιορίζεται, εφόσον δεν είναι η χώρα στην οποία έχετε την έδρα σας. Μπορείτε επίσης να προσδιορίσετε τον τόπο επεξεργασίας των δεδομένων και την έδρα του παρόχου υπηρεσιών (εάν είναι διαφορετικός).*  *Πρέπει επίσης να διενεργείται εκτίμηση κινδύνου της τρίτης χώρας.*  *Όλες οι χώρες της ΕΕ και οι χώρες που η ΕΕ έχει αναγνωρίσει ότι διαθέτουν επαρκές επίπεδο προστασίας δεδομένων μέσω απόφασης περί επάρκειας δεν είναι κρίσιμες. Για όλες τις άλλες χώρες θα πρέπει να εφαρμοστούν περαιτέρω μέτρα.*  *Οι απαραίτητες εγγυήσεις θα πρέπει επίσης να αναφέρονται. Τουλάχιστον, θα πρέπει να συναφθεί σύμβαση για την επεξεργασία δεδομένων κατ' εντολή με τον αντίστοιχο πάροχο υπηρεσιών.* |
| Προθεσμίες για διαγραφή των δεδομένων | *Προσέξτε όταν διαγράφετε τα καταγεγραμμένα δεδομένα. Εδώ μπορείτε να αναφερθείτε σε μια εξωτερική έννοια διαγραφής, η οποία πρέπει να δημιουργηθεί ξεχωριστά.* |
| **Έλεγχος συμμόρφωσης προστασίας δεδομένων για τους υπευθύνους επεξεργασίας δεδομένων** | |
| Νομική βάση της δραστηριότητας επεξεργασίας | *Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι νόμιμη μόνο εάν ισχύει μία από τις νομικές βάσεις που απαριθμούνται στον ΓΚΠΔ:*   * *Η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων (ΓΚΠΔ άρθρο 6 παράγραφος 1 α)* * *Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης ή για τη λήψη μέτρων πριν από τη σύναψη σύμβασης (ΓΚΠΔ άρθρο 6 παρ. 1 β)* * *Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με νομική υποχρέωση. (ΓΚΠΔ άρθρο 6 παρ. 1 γ)* * *Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου (ΓΚΠΔ άρθρο 6 παρ. 1 δ)* * *Η επεξργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον (ΓΚΠΔ άρθρο 6 παρ. 1 ε)* * *Η επεξεργασία βασίζεται στο έννομο συμφέρον που επιδιώκει ο υπέυθυνος επεξεργασίας. (ΓΚΠΔ άρθρο 6 παρ. 1 στ)* |
| Περαιτέρω νομοθεσία | *Εάν υπάρχει άλλη νομοθεσία στη χώρα σας βάσει των οποίων πραγματοποιείτε την επεξεργασία που περιγράφεται, μπορείτε να τους τεκμηριώσετε εδώ.* |
| **Περιγραφή των τεχνικών και οργανωτικών μέτρων**  **σύμφωνα με το άρθρο 30 παράγραφος 1 ζ) σε συνδυασμό με το άρθρο 32 παρ. 1 του ΓΚΠΔ**  *Για να διασφαλίσετε την προστασία των προσωπικών δεδομένων, πρέπει να ορίσετε τεχνικά και οργανωτικά μέτρα στην εταιρεία σας. Αυτά μπορούν επίσης να τεκμηριωθούν ξεχωριστά.* | |