					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P16S					Τίτλος εγγράφου: **Πολιτική απόκρυψης δεδομένων και ψευδωνυμοποίησης P16S**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρα 6.1.3, Ρήτρα 8	Κίνδυνοι ασφάλειας πληροφοριών και αναγκαίοι έλεγχοι, συμπεριλαμβανομένων της απόκρυψης και της ψευδωνυμοποίησης
ISO/IEC 27002:2022	Έλεγχοι 8.11, 8.12	Καθοδήγηση για απόκρυψη δεδομένων και πρόληψη διαρροής δεδομένων
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Συσκότιση δεδομένων και τεχνολογίες ενίσχυσης της ιδιωτικότητας
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(γ)	Αναλογικά τεχνικά μέτρα, ψευδωνυμοποίηση ως έλεγχος
Κανονισμός DORA της ΕΕ	Άρθρο 10(1)	Έλεγχοι κινδύνων ΤΠΕ, συμπεριλαμβανομένων δικλίδων μετασχηματισμού
COBIT 2019	DSS05.01, DSS06	Προστασία δεδομένων, τεχνικές συσκότισης/ψευδωνυμοποίησης
ΓΚΠΔ της ΕΕ	Άρθρα 4(5), 5(1)(γ), 32	Ελαχιστοποίηση δεδομένων, ψευδωνυμοποίηση ως τεχνικός έλεγχος

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει υποχρεωτικές και εκτελεστές απαιτήσεις για τη χρήση απόκρυψης δεδομένων και ψευδωνυμοποίησης με σκοπό την προστασία ευαίσθητων, προσωπικών και εμπιστευτικών δεδομένων σε μικρές και μεσαίες επιχειρήσεις (ΜΜΕ).

1.2. Οι τεχνικές αυτές είναι υποχρεωτικές όταν δεν απαιτείται η χρήση πραγματικών δεδομένων, όπως σε περιβάλλοντα ανάπτυξης, αναλυτικής επεξεργασίας ή σε σενάρια παροχής υπηρεσιών από τρίτους, συμβάλλοντας στη μείωση του κινδύνου έκθεσης, κακής χρήσης ή παραβίασης δεδομένων.

1.3. Η παρούσα πολιτική υποστηρίζει άμεσα τη συμμόρφωση με το ISO/IEC 27001:2022, καθώς και με ευρωπαϊκές κανονιστικές απαιτήσεις όπως ο ΓΚΠΔ της ΕΕ, η Οδηγία NIS2 της ΕΕ και ο Κανονισμός DORA της ΕΕ.

1.4. Με τον μετασχηματισμό των δεδομένων πριν από τη χρήση τους εκτός του αρχικού επιχειρησιακού τους πλαισίου, ο οργανισμός περιορίζει την έκθεσή του σε ευθύνη και ενισχύει τη δυνατότητά του να αποδεικνύει τη δέουσα επιμέλεια ως προς την ιδιωτικότητα και την ασφάλεια.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλα τα δομημένα ή αδόμητα δεδομένα που έχουν ταξινομηθεί ως προσωπικά, εμπιστευτικά ή ευαίσθητα, είτε αποθηκεύονται είτε υποβάλλονται σε επεξεργασία:

2.1.1. Σε περιβάλλοντα παραγωγής, δοκιμών ή ανάπτυξης

2.1.2. Σε τοπικές συσκευές, διακομιστές ή πλατφόρμες υπολογιστικού νέφους

2.1.3. Από εσωτερικό προσωπικό, αναδόχους ή τρίτους παρόχους

2.2. Καλύπτει επίσης όλα τα εργαλεία μετασχηματισμού δεδομένων (απόκρυψη, δημιουργία διακριτικών, ψευδωνυμοποίηση), είτε πρόκειται για λογισμικό ανοικτού κώδικα, εμπορικό λογισμικό ή λογισμικό που αναπτύσσεται εσωτερικά.

2.3. Οι περιπτώσεις χρήσης που εμπίπτουν στην παρούσα πολιτική περιλαμβάνουν:

2.3.1. Προετοιμασία συνόλων δεδομένων για δοκιμές ή ανάπτυξη

2.3.2. Εξαγωγή δεδομένων σε συστήματα αναλυτικής επεξεργασίας

2.3.3. Πρόσβαση προμηθευτών ή συμβούλων σε επιχειρησιακά συστήματα

2.3.4. Ελαχιστοποίηση δεδομένων υποκειμένων των δεδομένων για τη μείωση του κινδύνου επεξεργασίας

3. Στόχοι

3.1. Να διασφαλίζεται ότι πραγματικά προσωπικά ή ευαίσθητα δεδομένα δεν εκτίθενται ποτέ σε περιβάλλοντα χαμηλότερης ασφάλειας, όπου δεν είναι απολύτως αναγκαία.

3.2. Να καθίσταται υποχρεωτική η απόκρυψη ή η ψευδωνυμοποίηση όταν δεν απαιτούνται αυστηρά πραγματικά αναγνωριστικά για την εκτέλεση της εργασίας.

3.3. Να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση ή η κακή χρήση δεδομένων με την εφαρμογή ελέγχων μετασχηματισμού πριν από τη μεταφορά ή την επεξεργασία δεδομένων.

3.4. Να διασφαλίζεται ότι όλες οι διαδικασίες απόκρυψης και ψευδωνυμοποίησης είναι ιχνηλάσιμες, ελέγξιμες και εφαρμόζονται μέσω εγκεκριμένων εργαλείων.

3.5. Να διασφαλίζεται η συμμόρφωση με τις εφαρμοστέες νομικές και κανονιστικές απαιτήσεις που επιβάλλουν ελαχιστοποίηση δεδομένων, εμπιστευτικότητα και δικλίδες μετασχηματισμού.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής

4.1.1. Έχει την κυριότητα της παρούσας πολιτικής και την εγκρίνει.

4.1.2. Διασφαλίζει ότι όλα τα τμήματα και οι πάροχοι συμμορφώνονται με τις απαιτήσεις μετασχηματισμού.

4.1.3. Ανασκοπεί εξαιρέσεις, αξιολογήσεις κινδύνου και αρχεία καταγραφής μετασχηματισμού.

4.1.4. Συντονίζει νομικές, επιχειρησιακές ή σχετιζόμενες με προμηθευτές ενέργειες σε περίπτωση παραβιάσεων.

4.2. Πάροχος Υποστήριξης Πληροφορικής / Εσωτερικό Τμήμα Πληροφορικής

4.2.1. Επιλέγει και διαχειρίζεται εργαλεία απόκρυψης ή ψευδωνυμοποίησης.

4.2.2. Διασφαλίζει ότι εφαρμόζονται κατάλληλες μέθοδοι μετασχηματισμού ανάλογα με τον τύπο των δεδομένων.

4.2.3. Τηρεί αρχεία καταγραφής των μετασχηματισμένων συνόλων δεδομένων και των διαδικασιών διαχείρισης κλειδιών.

4.2.4. Διασφαλίζει ότι η απόκρυψη εφαρμόζεται πριν από τη χρήση για δοκιμές, από προμηθευτές ή για αναλυτική επεξεργασία.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1. Ετήσια ανασκόπηση

9.1.1. Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον Γενικό Διευθυντή, ώστε να διασφαλίζεται ότι αποτυπώνει:

9.1.1.1. Επικαιροποιήσεις στις εφαρμοστέες κανονιστικές απαιτήσεις (π.χ. ΓΚΠΔ της ΕΕ, Κανονισμός DORA της ΕΕ)

9.1.1.2. Νέα επιχειρησιακά συστήματα ή ανταλλαγές δεδομένων με τρίτα μέρη

9.1.1.3. Ανατροφοδότηση από ελέγχους ή περιστατικά που αφορούν χρήση μη καλυμμένων δεδομένων

9.2. Ενδιάμεσες ανασκοπήσεις

9.2.1. Ανασκοπήσεις πρέπει επίσης να διενεργούνται όταν:

9.2.1.1. Εισάγονται νέες εφαρμογές ή πλατφόρμες που χειρίζονται ευαίσθητα δεδομένα

9.2.1.2. Σοβαρό περιστατικό αποκαλύπτει κενά στους ισχύοντες ελέγχους μετασχηματισμού

9.2.1.3. Αλλαγές στα επίπεδα ταξινόμησης επηρεάζουν τις πρακτικές χειρισμού δεδομένων

9.3. Έλεγχος εκδόσεων και διαχείριση αλλαγών

9.3.1. Όλες οι αλλαγές της πολιτικής πρέπει:

9.3.1.1. Να εγκρίνονται από τον Γενικό Διευθυντή και να τεκμηριώνονται σε αρχείο μεταβολών

9.3.1.2. Να κοινοποιούνται με σαφήνεια στους εργαζομένους και στους παρόχους υπηρεσιών που επηρεάζονται

9.3.1.3. Να αρχειοθετούνται με ασφαλή τρόπο, με περιορισμένη πρόσβαση σε παρωχημένες εκδόσεις

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική πρέπει να εφαρμόζεται σε συνδυασμό με τις ακόλουθες πολιτικές SME, ώστε να διασφαλίζεται συνεπής και εκτελεστή προστασία ευαίσθητων δεδομένων:

10.1.1. P13S – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθορίζει τα επίπεδα ταξινόμησης (π.χ. Εμπιστευτικό – Προσωπικά) που προσδιορίζουν πότε πρέπει να εφαρμόζεται απόκρυψη ή ψευδωνυμοποίηση. Η πολιτική αυτή επιβάλλει κανόνες μετασχηματισμού βάσει των επιπέδων ευαισθησίας των δεδομένων.

10.1.2. P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Διασφαλίζει ότι τα μετασχηματισμένα σύνολα δεδομένων, συμπεριλαμβανομένων αντιγράφων ασφαλείας που περιέχουν καλυμμένα ή ψευδωνυμοποιημένα δεδομένα, διατηρούνται και διατίθενται σύμφωνα με τους εφαρμοστέους κανόνες, συμπεριλαμβανομένης της διαγραφής των κλειδιών αντιστοίχισης όταν δεν χρειάζονται πλέον.

10.1.3. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Ευθυγραμμίζει τις πρακτικές μετασχηματισμού με τις ευρύτερες υποχρεώσεις ιδιωτικότητας, συμπεριλαμβανομένων των απαιτήσεων του ΓΚΠΔ της ΕΕ για ελαχιστοποίηση δεδομένων και χρήση της ψευδωνυμοποίησης ως δικλίδας προστασίας κατά την επεξεργασία προσωπικών δεδομένων.

10.1.4. P30S – Πολιτική Αντιμετώπισης Περιστατικών: Καλύπτει διαδικασίες αναφοράς και κλιμάκωσης σε περίπτωση μη εξουσιοδοτημένης γνωστοποίησης δεδομένων, συμπεριλαμβανομένης της ακατάλληλης χρήσης ή αντιστροφής καλυμμένων ή ψευδωνυμοποιημένων δεδομένων.

10.1.5. P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Κατανέμει τη συνολική λογοδοσία για την εφαρμογή της πολιτικής, την αποδοχή κινδύνου και την έγκριση εξαιρέσεων, κυρίως στον Γενικό Διευθυντή.

10.2. Οι πολιτικές αυτές συγκροτούν ένα ολοκληρωμένο πλαίσιο προστασίας δεδομένων, διασφαλίζοντας ότι οι ενέργειες απόκρυψης και ψευδωνυμοποίησης υποστηρίζουν την πιστοποίηση ISO/IEC 27001 και τη συμμόρφωση με το εφαρμοστέο κανονιστικό πλαίσιο.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 6.1.3: Απαιτεί την αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών, η οποία περιλαμβάνει τον μετριασμό της έκθεσης μέσω τεχνικών μετασχηματισμού δεδομένων.

11.1.2. Ρήτρα 8.1: Επιβάλλει την εφαρμογή των αναγκαίων ελέγχων για την επίτευξη των στόχων ασφάλειας, συμπεριλαμβανομένων της ψευδωνυμοποίησης και της απόκρυψης.

11.2. ISO/IEC 27002

11.2.1. Έλεγχος 8.11: Παρέχει καθοδήγηση για την απόκρυψη ευαίσθητων δεδομένων σε συστήματα δοκιμών και ανάπτυξης.

11.2.2. Έλεγχος 8.12: Παρέχει στρατηγικές για την πρόληψη διαρροής δεδομένων μέσω ελεγχόμενου μετασχηματισμού και πρακτικών πρόσβασης.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Διασφαλίζει την εμπιστευτικότητα των πληροφοριών μέσω συσκότισης δεδομένων.

11.3.2. SC-28: Προστατεύει πληροφορίες σε αποθήκευση και κατά τη χρήση.

11.3.3. PT-2/PT-3: Προάγουν τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας, συμπεριλαμβανομένης της ψευδωνυμοποίησης, κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα (PII).

11.4. ΓΚΠΔ της ΕΕ

11.4.1. Άρθρο 4(5): Ορίζει νομικά την ψευδωνυμοποίηση και απαιτεί ελέγχους επί των κλειδιών αντιστοίχισης και των αναγνωριστικών.

11.4.2. Άρθρο 5(1)(γ): Υποστηρίζει τις αρχές ελαχιστοποίησης δεδομένων μέσω της απόκρυψης.

11.4.3. Άρθρο 32: Αναγνωρίζει την ψευδωνυμοποίηση ως τεχνικό έλεγχο που μειώνει τους κινδύνους ιδιωτικότητας.

11.5. Οδηγία NIS2 της ΕΕ

11.5.1. Άρθρο 21(2)(γ): Απαιτεί αναλογικά τεχνικά μέτρα για την ελαχιστοποίηση του κινδύνου ασφάλειας δεδομένων, συμπεριλαμβανομένης της ψευδωνυμοποίησης ως μέρους του ελέγχου κινδύνου.

11.6. Κανονισμός DORA της ΕΕ

11.6.1. Άρθρο 10(1): Επιβάλλει ελέγχους κινδύνων σχετικών με τις ΤΠΕ που περιλαμβάνουν δικλίδες μετασχηματισμού δεδομένων για επιχειρησιακή συνέχεια και εμπιστευτικότητα κατά την εξωτερική ανάθεση και την ανάπτυξη συστημάτων.

11.7. COBIT 2019

11.7.1. DSS05.01: Απαιτεί την προστασία των πληροφοριακών περιουσιακών στοιχείων, συμπεριλαμβανομένου του μετασχηματισμού όπου είναι εφικτό.

11.7.2. DSS06.06: Απαιτεί κατάλληλες τεχνικές συσκότισης και ψευδωνυμοποίησης για τον περιορισμό της έκθεσης δεδομένων σε περιβάλλοντα χαμηλότερης εμπιστοσύνης.