| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου | | | | | | | |
| Αριθμός εγγράφου:<br>P16 | | | | | Τίτλος εγγράφου:<br>**Πολιτική απόκρυψης δεδομένων και ψευδωνυμοποίησης P16S** | | | | | | | |
| Έκδοση:<br>1.0 | | Ημερομηνία έναρξης ισχύος:<br>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 | Ρήτρες 6.1 | Γενικές απαιτήσεις για τη διαχείριση κινδύνων και τους επιχειρησιακούς ελέγχους για την απόκρυψη και την ψευδωνυμοποίηση |
| ISO/IEC 27002:2022 | Έλεγχοι 8.11, 8 | Καθοδήγηση ελέγχων για την εφαρμογή της απόκρυψης και της ψευδωνυμοποίησης |
| NIST SP 800-53 Rev.5 | PM-17, PT-2, PT-3, SC-12, SC-28, SC-30 | Έλεγχοι ιδιωτικότητας και εμπιστευτικότητας για την ελαχιστοποίηση δεδομένων, τον μετασχηματισμό και τον περιορισμό πρόσβασης |
| ΓΚΠΔ της ΕΕ | Άρθρα 4(5), 5(1)(c,f), 32 | Νομική βάση και απαιτήσεις για την ψευδωνυμοποίηση και τα μέτρα προστασίας δεδομένων |
| Οδηγία NIS2 της ΕΕ | Άρθρο 21(2)(c) | Υποχρέωση λήψης τεχνικών και οργανωτικών μέτρων, συμπεριλαμβανομένων τεχνολογιών ενίσχυσης της ιδιωτικότητας (PETs) |
| Κανονισμός DORA της ΕΕ | Άρθρα 10(1), 10(2)(e) | Διαχείριση κινδύνων ΤΠΕ και έλεγχοι εμπιστευτικότητας για την απόκρυψη δεδομένων/ψευδωνυμοποίηση |
| COBIT 2019 | DSS05.01, DSS06.06, MEA | Έλεγχοι διακυβέρνησης για την προστασία δεδομένων μέσω απόκρυψης και αξιολόγηση της συμμόρφωσης |

**1. Σκοπός**

1.1 Η παρούσα πολιτική καθορίζει την προσέγγιση του οργανισμού για την εφαρμογή της απόκρυψης δεδομένων και της ψευδωνυμοποίησης ως τεχνολογιών ενίσχυσης της ιδιωτικότητας (PETs), με σκοπό τη μείωση της δυνατότητας ταυτοποίησης και της έκθεσης προσωπικών ή ευαίσθητων δεδομένων.

1.2 Υποστηρίζει την ασφαλή χρήση πληροφοριών σε δοκιμές, αναλύσεις και λειτουργικές δραστηριότητες, διασφαλίζοντας παράλληλα τη συμμόρφωση με νομικές και κανονιστικές απαιτήσεις, τον μετριασμό του αντικτύπου παραβίασης και την εφαρμογή των αρχών της ελαχιστοποίησης δεδομένων και της εμπιστευτικότητας.

1.3 Η πολιτική ευθυγραμμίζεται με το ISO/IEC 27001:2022, υποστηρίζει το Άρθρο 4(5) του ΓΚΠΔ της ΕΕ σχετικά με την ψευδωνυμοποίηση και ενσωματώνει προσέγγιση βάσει κινδύνου, συνεπή με τα πρότυπα NIST, NIS2, DORA και COBIT 2019.

**2. Πεδίο εφαρμογής**

**2.1 Η παρούσα πολιτική εφαρμόζεται στα εξής:**

2.1.1 Σε όλους τους εργαζομένους, αναδόχους, τρίτα μέρη ή προμηθευτές που έχουν πρόσβαση σε συστήματα τα οποία χειρίζονται προσωπικές, εμπιστευτικές ή ευαίσθητες πληροφορίες.

2.1.2 Σε όλα τα περιβάλλοντα δεδομένων, συμπεριλαμβανομένων του περιβάλλοντος παραγωγής, της ανάπτυξης, των δοκιμών και της προπαραγωγής.

2.1.3 Σε όλες τις μορφές απόκρυψης δεδομένων (π.χ. στατική, δυναμική, ντετερμινιστική, tokenization) και στις τεχνικές ψευδωνυμοποίησης που χρησιμοποιούνται για τη μείωση των κινδύνων ιδιωτικότητας.

2.1.4 Σε όλους τους τύπους δεδομένων (δομημένα ή αδόμητα), τα συστήματα (εντός εγκαταστάσεων ή φιλοξενούμενα σε περιβάλλον νέφους) και τις εφαρμογές που περιλαμβάνουν προσωπικά ή ρυθμιζόμενα δεδομένα.

**2.2 Το πεδίο εφαρμογής περιλαμβάνει χρήση σε:**

2.2.1 Περιβάλλοντα ανάπτυξης εφαρμογών και διασφάλισης ποιότητας/δοκιμών

2.2.2 Πλατφόρμες ανάλυσης ή αναφορών

2.2.3 Ανταλλαγή δεδομένων με τρίτα μέρη ή τρίτους παρόχους υπηρεσιών

2.2.4 Συστήματα αντιγράφων ασφαλείας, αρχειοθέτησης ή ανάκαμψης

**3. Στόχοι**

3.1 Να διασφαλίζεται η συνεπής και αποτελεσματική εφαρμογή της απόκρυψης και της ψευδωνυμοποίησης για τη μείωση των κινδύνων έκθεσης ή κακής χρήσης δεδομένων.

3.2 Να διασφαλίζεται ότι πραγματικά δεδομένα δεν χρησιμοποιούνται ποτέ σε περιβάλλον μη παραγωγικής λειτουργίας, εκτός εάν έχουν μετασχηματιστεί μέσω εγκεκριμένων τεχνικών PET.

3.3 Να διατηρούνται η αναφορική ακεραιότητα, η χρηστικότητα και οι μετασχηματισμοί διατήρησης μορφοτύπου, όταν αυτό απαιτείται για τη λειτουργική συνέπεια.

3.4 Να εφαρμόζονται αυστηροί έλεγχοι πρόσβασης στα αρχικά δεδομένα, στα δεδομένα που έχουν υποστεί απόκρυψη και στα κλειδιά επαναταυτοποίησης.

3.5 Τα σύνολα δεδομένων που έχουν υποστεί απόκρυψη ή ψευδωνυμοποίηση να αντιμετωπίζονται ως ευαίσθητα δεδομένα και να υπόκεινται σε καταγραφή πρόσβασης, ελέγχους διατήρησης και πρωτόκολλα απόκρισης σε περιστατικά.

3.6 Να επικυρώνεται η αποτελεσματικότητα αυτών των ελέγχων μέσω συνεχών δοκιμών, παρακολούθησης και ελεγκτικών διαδικασιών.

**4. Ρόλοι και αρμοδιότητες**

**4.1 Ανώτατη Διοίκηση**

4.1.1 Εγκρίνει την παρούσα πολιτική και διασφαλίζει την εφαρμογή της ως μέρος της ευρύτερης διακυβέρνησης της πληροφορικής και των πρωτοβουλιών προστασίας δεδομένων.

**4.2 Επικεφαλής Ασφάλειας Πληροφοριών (CISO) / Υπεύθυνος ΣΔΑΠ**

4.2.1 Ασκεί εποπτεία της υλοποίησης και της διαρκούς συμμόρφωσης.

4.2.2 Διασφαλίζει την ευθυγράμμιση με το ISO/IEC 27001, Ρήτρα 6.1.3 (αντιμετώπιση κινδύνων) και Ρήτρα 8.1 (επιχειρησιακός έλεγχος).

4.2.3 Ανασκοπεί τα αρχεία ελέγχου και επικυρώνει την αποτελεσματικότητα των ελέγχων.

[ ... 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 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον ετησίως ή νωρίτερα σε περίπτωση:**

9.1.1 Κανονιστικών αλλαγών που επηρεάζουν την απόκρυψη ή την ψευδωνυμοποίηση

9.1.2 Υιοθέτησης νέων πληροφοριακών συστημάτων που χειρίζονται ευαίσθητα δεδομένα

9.1.3 Ουσιωδών αλλαγών στο σχήμα ταξινόμησης δεδομένων του οργανισμού

9.1.4 Ευρημάτων ελέγχου που υποδεικνύουν αδυναμίες ελέγχων

9.1.5 Εμφάνισης νέων απειλών ή τεχνολογιών απόκρυψης

9.2 Ο Υπεύθυνος ΣΔΑΠ οφείλει να ηγείται της ανασκόπησης σε διαβούλευση με τον Υπεύθυνο Προστασίας Δεδομένων, τους Ιδιοκτήτες Δεδομένων, την Ασφάλεια Πληροφοριών και τις λειτουργίες Νομικών Υπηρεσιών και Κανονιστικής Συμμόρφωσης. Οι επικαιροποιήσεις πρέπει να υπόκεινται σε έλεγχο εκδόσεων, να εγκρίνονται από την Εκτελεστική Διοίκηση και να γνωστοποιούνται σε όλα τα επηρεαζόμενα ενδιαφερόμενα μέρη.

**10. Συναφείς πολιτικές και διασυνδέσεις**

10.1 P13 - Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων. Οι αποφάσεις για απόκρυψη και ψευδωνυμοποίηση εξαρτώνται άμεσα από την ταξινόμηση των πεδίων δεδομένων και τα επίπεδα ευαισθησίας που ορίζονται στην P13.

10.2 P14 - Πολιτική Διατήρησης και Διάθεσης Δεδομένων. Τα μετασχηματισμένα σύνολα δεδομένων πρέπει να διατηρούνται και να διατίθενται σύμφωνα με τους κανόνες κύκλου ζωής της P14, διασφαλίζοντας ότι τα δεδομένα που έχουν υποστεί απόκρυψη και ψευδωνυμοποίηση αντιμετωπίζονται ως ευαίσθητα.

10.3 P17 - Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας. Παρέχει τις αρχές ιδιωτικότητας και τα κανονιστικά θεμέλια για την εφαρμογή της ψευδωνυμοποίησης ως δραστηριότητας επεξεργασίας που συμμορφώνεται με τον ΓΚΠΔ της ΕΕ και παρόμοιες νομοθεσίες.

10.4 P22 - Πολιτική Καταγραφής και Παρακολούθησης. Υποστηρίζει τον κεντρικό έλεγχο και τις ειδοποιήσεις για συμβάντα απόκρυψης και ψευδωνυμοποίησης σύμφωνα με δομημένα πρωτόκολλα παρακολούθησης ασφάλειας.

**11. Πρότυπα και πλαίσια αναφοράς**

**11.1 ISO/IEC 27001**

11.1.1 Ρήτρα 6.1.3 - Σχέδιο Αντιμετώπισης Κινδύνων: Καθιερώνει την απόκρυψη και την ψευδωνυμοποίηση ως μηχανισμούς αντιμετώπισης κινδύνων για τη μείωση της δυνατότητας ταυτοποίησης ευαίσθητων δεδομένων σε περιβάλλοντα επεξεργασίας όπου αυτό δεν είναι απολύτως αναγκαίο.

11.1.2 Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος: Επιβάλλει τεχνικούς και διαδικαστικούς ελέγχους για τον ασφαλή μετασχηματισμό δεδομένων κατά την επεξεργασία, αποθήκευση ή μεταφορά.

**11.2 ISO/IEC 27002:2022**

11.2.1 Έλεγχοι 8.11, 8: Καθοδήγηση για την απόκρυψη δεδομένων και την ψευδωνυμοποίηση με στόχο την ελαχιστοποίηση των κινδύνων επαναταυτοποίησης και διαρροής.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 PM-17 - Προστασία PII: Εφαρμογή τεχνολογιών ενίσχυσης της ιδιωτικότητας όπως η απόκρυψη και η ψευδωνυμοποίηση.

11.3.2 PT-2, PT-3: Ελαχιστοποίηση και ασφάλεια επεξεργασίας PII - Μετασχηματισμός για μείωση της δυνατότητας ταυτοποίησης και εφαρμογή ελέγχου πρόσβασης.

11.3.3 SC-12, SC-28, SC-30: Εμπιστευτικότητα και ακεραιότητα δεδομένων - Έλεγχοι εμπιστευτικότητας και απόκρυψης για αποθήκευση, μετάδοση και χρήση.

**11.4 ΓΚΠΔ της ΕΕ (2016/679)**

11.4.1 Άρθρο 4(5): Επίσημος ορισμός της ψευδωνυμοποίησης.

11.4.2 Άρθρο 32: Ασφάλεια της επεξεργασίας - οργανωτικά και τεχνικά μέτρα για την ψευδωνυμοποίηση.

11.4.3 Άρθρο 5(1)(c,f): Ελαχιστοποίηση δεδομένων και εμπιστευτικότητα με χρήση ψευδωνυμοποίησης/απόκρυψης.

**11.5 Οδηγία NIS2 της ΕΕ (2022/2555)**

11.5.1 Άρθρο 21(2)(c): Απαιτεί PETs όπως η απόκρυψη και η ψευδωνυμοποίηση ως μέτρα ασφάλειας.

**11.6 Κανονισμός DORA της ΕΕ (2022/2554)**

11.6.1 Άρθρο 10(1): Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ περιλαμβάνει ελέγχους απόκρυψης/ψευδωνυμοποίησης.

11.6.2 Άρθρο 10(2)(e): Επιβάλλει τη χρήση τεχνολογιών μετασχηματισμού για την προστασία προσωπικών και οικονομικών δεδομένων.

**11.7 COBIT 2019**

11.7.1 DSS05.01: Προστασία πληροφοριακών περιουσιακών στοιχείων - Απαιτήσεις για απόκρυψη και ψευδωνυμοποίηση.

11.7.2 DSS06.06: Ασφαλείς δοκιμές και αναλύσεις - Απόκρυψη σε περιβάλλοντα εκτός παραγωγής.

11.7.3 MEA03: Παρακολούθηση συμμόρφωσης για την αποτελεσματικότητα της απόκρυψης και της ψευδωνυμοποίησης.