



Αθήνα, 17-10-2005

ΑΠ: 3845

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ο Δ Η Γ Ι Α Α Ρ . 1 / 2005

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Έχοντας υπόψη:

1. Ότι σύμφωνα με το άρθρο 10 του Ν. 2472/1997 ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.
2. Ότι τα παραπάνω ισχύουν καθόλη τη διάρκεια της επεξεργασίας, η οποία περατώνεται με την καταστροφή των προσωπικών δεδομένων, σύμφωνα με το άρθρο 4 παρ. 1 δ) του Ν. 2472/1997.
3. Ότι η παραβίαση του άρθρου 10 του Ν.2472/1997 επισύρει τις συνέπειες των άρθρων 21, 22 και 23 του Ν.2472/1997.
4. Ότι σύμφωνα με το άρθρο 19 και 1 α) του Ν. 2472/1997, η Αρχή Προστασίας Προσωπικών Δεδομένων εκδίδει Οδηγίες προς το σκοπό της ενιαίας εφαρμογής των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Αποφασίζει την έκδοση της παρακάτω Οδηγίας:

ΟΔΗΓΙΑ

**για την ασφαλή καταστροφή των προσωπικών δεδομένων
μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού
της επεξεργασίας**

Άρθρο 1. Πεδίο εφαρμογής

1. Η παρούσα Οδηγία αφορά στην καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας ή γενικότερα της περιόδου τήρησης των προσωπικών δεδομένων σύμφωνα με το άρθρο 4 παρ. 1 δ) του Ν. 2472/1997.

2. Η παρούσα Οδηγία δεν εφαρμόζεται στην περίπτωση, που τα δεδομένα καθίστανται ανώνυμα από τον υπεύθυνο επεξεργασίας μετά το πέρας της περιόδου της επεξεργασίας.

Άρθρο 2. Τύποι δεδομένων προς καταστροφή

1. Ανάλογα με το μέσο που χρησιμοποιείται για την τήρηση και την περαιτέρω επεξεργασία τους, διακρίνονται οι παρακάτω τύποι προσωπικών δεδομένων προς καταστροφή:

- Προσωπικά δεδομένα σε έντυπη μορφή (έγγραφα).
- Προσωπικά δεδομένα σε ηλεκτρονική μορφή που τηρούνται σε οποιοδήποτε φυσικό υπόστρωμα (σκληρούς δίσκους υπολογιστών, CD, DVD, δισκέττες, κ.λ.π). Τα δεδομένα αυτά μπορεί να βρίσκονται είτε σε δομημένη μορφή (π.χ. βάση δεδομένων), είτε να αποτελούν ένα σύνολο επιμέρους ηλεκτρονικών αρχείων (π.χ. αρχεία κειμένου, εικόνες, κ.λ.π).
- Προσωπικά δεδομένα σε άλλη μορφή (π.χ. δεδομένα που τηρούνται σε βιντεοκασέτες, μικροφίλμ, κλπ).

2. Οι ανωτέρω τύποι δεδομένων μπορεί να απαντώνται ταυτόχρονα.

Άρθρο 3. Αργές για την ασφαλή καταστροφή δεδομένων

1. Τα προσωπικά δεδομένα πρέπει να καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας αμέσως μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας.

2. Ανάλογα με την περίοδο που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας, διακρίνονται οι παρακάτω περιπτώσεις καταστροφής προσωπικών δεδομένων:

- Καθημερινή καταστροφή των δεδομένων. Η περίπτωση αυτή αφορά προσωπικά δεδομένα που παράγονται ή/και χρησιμοποιούνται καθημερινά στο πλαίσιο των εργασιών του υπεύθυνου επεξεργασίας και τα οποία, μετά από την διεκπεραίωση της συγκεκριμένης εργασίας, είναι πλέον άχρηστα (π.χ. αντίγραφα, πρόχειρες εκθέσεις, σημειώσεις των υπαλλήλων, πληροφοριακό υλικό, κ.α. σε έντυπη ή/και ηλεκτρονική μορφή).
- Προγραμματισμένη καταστροφή μέρους ή του συνόλου των δεδομένων. Η περίπτωση αφορά μαζική καταστροφή δεδομένων που πραγματοποιείται είτε επειδή παρήλθε η περίοδος που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας (σύμφωνα με τον εκάστοτε ισχύοντα χρόνο τήρησης των δεδομένων) για τα συγκεκριμένα δεδομένα, είτε για άλλους λόγους, όπως π.χ. παύση ή τροποποίηση εργασιών του υπεύθυνου επεξεργασίας.

3. Τα προσωπικά δεδομένα πρέπει να καταστρέφονται από τον υπεύθυνο επεξεργασίας με ασφαλή τρόπο, ώστε να αποκλειστεί η περαιτέρω μη νόμιμη και αθέμιτη επεξεργασία τους, όπως είναι η κάθε μορφή διάθεσης σε τρίτους.

4. Ως ασφαλής τρόπος καταστροφής των δεδομένων θεωρείται κάθε σύνολο διαδικασιών και μέτρων που μετά από την ολοκλήρωση της εφαρμογής τους δεν είναι δυνατό να αναγνωρισθούν τα υποκείμενα των δεδομένων.

5. Σε κάθε ασφαλή τρόπο καταστροφής δεδομένων η καταστροφή είναι μη αναστρέψιμη, δηλαδή δεν είναι δυνατή η ανάκτηση των δεδομένων μετά την καταστροφή με τεχνικά ή άλλα μέσα.

Άρθρο 4. Υποχρεώσεις του υπεύθυνου επεξεργασίας

1. Διαδικασίες για την ασφαλή καταστροφή δεδομένων

α) Ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει συγκεκριμένη διαδικασία για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Η διαδικασία αυτή θα καλύπτει προσωπικά δεδομένα όλων των αναφερόμενων στο άρθρο 2 της παρούσας τύπων, θα αφορά τόσο την καθημερινή, όσο και την προγραμματισμένη καταστροφή μέρους ή του συνόλου των δεδομένων του υπεύθυνου επεξεργασίας και θα είναι γραπτώς διατυπωμένη, υπογραφόμενη από τον υπεύθυνο επεξεργασίας.

β) Ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει τους κατάλληλους μηχανισμούς ελέγχου της ορθής τήρησης της παραπάνω διαδικασίας. Ο έλεγχος θα ανατίθεται σε εξουσιοδοτημένους για τον σκοπό αυτό υπαλλήλους του υπεύθυνου επεξεργασίας. Η διαδικασία του ελέγχου θα είναι γραπτώς διατυπωμένη και θα υπογράφεται από τον υπεύθυνο επεξεργασίας.

2. Ανάθεση της καταστροφής σε εκτελούντα την επεξεργασία

α) Αν η καταστροφή των δεδομένων εκτελείται για λογαριασμό του υπεύθυνου επεξεργασίας από πρόσωπο μη εξαρτώμενο από αυτόν (εκτελούντα την επεξεργασία), ο υπεύθυνος επεξεργασίας οφείλει να πραγματοποιεί τη σχετική ανάθεση μόνον εγγράφως, σύμφωνα με όσα ορίζονται στο άρθρο 10 παρ. 4 του Ν. 2472/1997. Στην σύμβαση της ανάθεσης θα πρέπει να ορίζονται τα μέτρα που θα εφαρμόσει ο εκτελών την επεξεργασία για την ασφαλή μεταφορά των δεδομένων στον τόπο καταστροφής, ο τόπος καταστροφής, οι τυχόν ενδιάμεσοι τόποι αποθήκευσης των δεδομένων, ο τρόπος καταστροφής, καθώς επίσης και ο μέγιστος επιτρεπόμενος χρόνος από την στιγμή της παράδοσης των δεδομένων από τον

υπεύθυνο επεξεργασίας στον εκτελούντα την επεξεργασία μέχρι την οριστική καταστροφή τους. Επίσης, στη σύμβαση της ανάθεσης πρέπει να αναφέρονται και τυχόν πρόσθετες υποδείξεις του υπεύθυνου επεξεργασίας σχετικά με τεχνικά και οργανωτικά μέτρα καταστροφής, καθώς επίσης και τα ακριβή στοιχεία τυχόν τρίτων (υπεργολάβων) που πρόκειται να πραγματοποιήσουν μέρος ή το σύνολο της καταστροφής των δεδομένων για λογαριασμό του εκτελούντος την επεξεργασία.

β) Σε περίπτωση ανάθεσης της καταστροφής σε εκτελούντα την επεξεργασία:

- Πρέπει να διασφαλίζεται ότι ο υπεύθυνος επεξεργασίας έχει την εξουσία διάθεσης και ελέγχου των δεδομένων μέχρι την οριστική καταστροφή τους. Ως εκ τούτου, ο εκτελών την επεξεργασία πρέπει να διατηρεί ξεχωριστά τα προς καταστροφή δεδομένα του κάθε υπεύθυνου επεξεργασίας με τον οποίο συνάπτει σχετική σύμβαση.
- Ο εκτελών την επεξεργασία πρέπει να είναι σε θέση να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέσα για την ασφαλή καταστροφή των δεδομένων, και να έχει προβλέψει αντίστοιχη διαδικασία καταστροφής και ελέγχου καταστροφής όπως ορίζεται στη παρ. 1 του παρόντος άρθρου για τον υπεύθυνο επεξεργασίας.
- Τα φυσικά πρόσωπα – υπάλληλοι του εκτελούντος την επεξεργασία που θα πραγματοποιήσουν την καταστροφή πρέπει να υποχρεώνονται ειδικώς στο απόρρητο της επεξεργασίας.

γ) Όταν τα δεδομένα διέπονται από ειδικό απόρρητο που προβλέπεται από νόμο (π.χ. ιατρικό απόρρητο), ο υπεύθυνος επεξεργασίας οφείλει καταρχήν να πραγματοποιεί ο ίδιος την καταστροφή (χωρίς δηλαδή να την αναθέτει σε εκτελούντα την επεξεργασία) έτσι ώστε να διασφαλίζεται το απόρρητο από τυχόν αθέμιτη πρόσβαση τρίτων. Σε περίπτωση που αυτό είναι τεχνικά ή/και οργανωτικά ιδιαιτέρως δυσχερές για τον υπεύθυνο επεξεργασίας, η ανάθεση πρέπει να γίνεται κατά τέτοιο τρόπο, ώστε ο υπεύθυνος επεξεργασίας να έχει τη συνολική επίβλεψη της διαδικασίας της καταστροφής (π.χ. η καταστροφή των δεδομένων να γίνεται εντός των εγκαταστάσεων του υπεύθυνου επεξεργασίας ή το πρώτο στάδιο της καταστροφής να γίνεται εντός των εγκαταστάσεων του υπεύθυνου επεξεργασίας π.χ. με χρήση προγραμμάτων αλλοίωσης των δεδομένων που τηρούνται ηλεκτρονικώς (βλ. άρθρο 6 της παρούσας), ή σε περίπτωση που αυτό δεν είναι εφικτό, π.χ. στην περίπτωση που

τα δεδομένα τηρούνται σε έντυπη μορφή, εξουσιοδοτημένος υπάλληλος του υπεύθυνου επεξεργασίας να επιβλέπει την καταστροφή των δεδομένων στις εγκαταστάσεις του εκτελούντος την επεξεργασία).

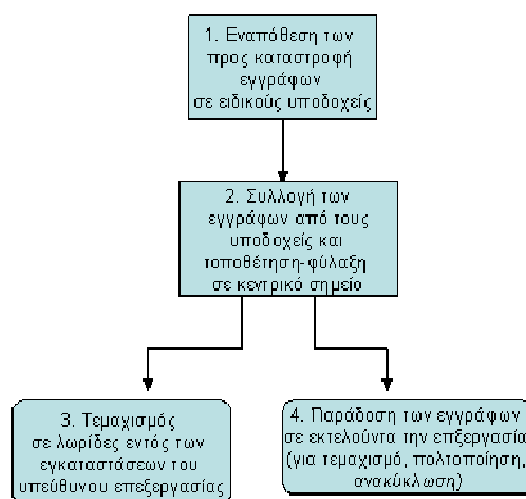
3. Τρόπος καταστροφής των δεδομένων

Ο υπεύθυνος επεξεργασίας μπορεί να εφαρμόζει οποιοδήποτε ασφαλή τρόπο καταστροφής των δεδομένων, όπως αυτός ορίζεται στο άρθρο 2 της παρούσας. Οι διαδικασίες και τα μέτρα καταστροφής δεδομένων που περιγράφονται στα άρθρα 5 και 6 της παρούσας Οδηγίας είναι ενδεικτικά.

Άρθρο 5. Ασφαλής καταστροφή δεδομένων σε έντυπη μορφή

1. Καθημερινή καταστροφή δεδομένων που τηρούνται σε έντυπη μορφή

Μία ασφαλής διαδικασία για την καθημερινή καταστροφή προσωπικών δεδομένων που τηρούνται σε έντυπη μορφή (εγγράφων) περιλαμβάνει ενδεικτικώς τα παρακάτω βήματα (βλ. Σχήμα 1):



Σχήμα 1: Διαδικασία για την καθημερινή καταστροφή μη χρησιμοποιούμενων εγγράφων με προσωπικά δεδομένα

α) Εναπόθεση των προς καταστροφή εγγράφων από τους υπαλλήλους του υπεύθυνου επεξεργασίας σε ειδικούς υποδοχείς, που είναι τοποθετημένοι σε συγκεκριμένα σημεία εντός των εγκαταστάσεων του υπεύθυνου επεξεργασίας.

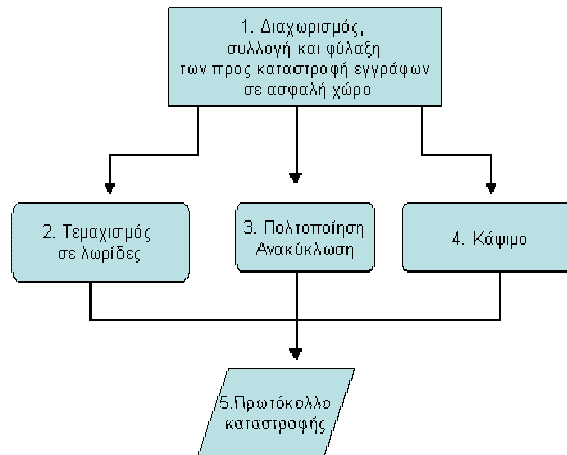
β) Συλλογή των προς καταστροφή εγγράφων από τους υποδοχείς και εναπόθεση τους σε κεντρικό υποδοχέα σε ειδικό χώρο εντός των εγκαταστάσεων του υπεύθυνου επεξεργασίας και από εξουσιοδοτημένο προς το σκοπό αυτό υπάλληλο του υπεύθυνου επεξεργασίας.

γ) Τεμαχισμός των εγγράφων σε λωρίδες με χρήση ειδικών μηχανημάτων τεμαχισμού εγγράφων εντός των εγκαταστάσεων και από εξουσιοδοτημένους υπαλλήλους του υπεύθυνου επεξεργασίας.

δ) Εναλλακτικά, ο τεμαχισμός των εγγράφων μπορεί να γίνει εκτός των εγκαταστάσεων του υπεύθυνου επεξεργασίας μέσω ανάθεσης της καταστροφής σε εκτελούντα την επεξεργασία, σύμφωνα με τα οριζόμενα στο άρθρο 4, παρ. 2 της παρούσας. Στην περίπτωση αυτή πρέπει να τηρείται πρωτόκολλο παράδοσης των δεδομένων από τον υπεύθυνο στον εκτελούντα την επεξεργασία, καθώς και πρωτόκολλο καταστροφής των δεδομένων από τον εκτελούντα την επεξεργασία, σύμφωνα με τα οριζόμενα στην παρ. 3 β) του παρόντος άρθρου. Ο τεμαχισμός των εγγράφων μπορεί να ακολουθείται από πολτοποίηση ή/και ανακύκλωση των εγγράφων.

2. Προγραμματισμένη καταστροφή μέρους ή του συνόλου των δεδομένων που τηρούνται σε έντυπη μορφή

Μία ασφαλής διαδικασία για την καταστροφή μέρους ή του συνόλου των δεδομένων που τηρούνται σε έντυπη μορφή περιλαμβάνει ενδεικτικώς τα παρακάτω βήματα (βλ. Σχήμα 2):



Σχήμα 2: Διαδικασία για την ασφαλή καταστροφή μέρους ή του συνόλου των δεδομένων του υπεύθυνου επεξεργασίας

α) Διαχωρισμός των προς καταστροφή δεδομένων από τον αρμόδιο υπάλληλο του υπεύθυνου επεξεργασίας.

β) Συλλογή και φύλαξη των προς καταστροφή δεδομένων σε ειδικά διαμορφωμένο ασφαλή χώρο εντός των εγκαταστάσεων του υπεύθυνου επεξεργασίας. Στο χώρο αυτό θα έχουν πρόσβαση μόνο εξουσιοδοτημένοι υπάλληλοι του υπεύθυνου επεξεργασίας.

γ) Μαζική καταστροφή των δεδομένων με τεμαχισμό τους σε λωρίδες και πολυτοποίηση/ανακύκλωσή τους, σύμφωνα με τα αναφερόμενα στην παρ1. γ) και δ) του παρόντος άρθρου. Μία εναλλακτική μέθοδος καταστροφής είναι η αποτέφρωση του υλικού υποστρώματος των δεδομένων.

δ) Σύνταξη πρωτοκόλλου καταστροφής, σύμφωνα με τα αναφερόμενα στη παρ. 3 του παρόντος άρθρου.

3. Πρωτόκολλο καταστροφής δεδομένων

α) Το πρωτόκολλο καταστροφής πρέπει να περιλαμβάνει τουλάχιστον τα παρακάτω στοιχεία (βλ. Παράρτημα 2 της παρούσας):

- Ημερομηνία καταστροφής των δεδομένων.

- Περιγραφή των δεδομένων που καταστράφηκαν.
- Μέθοδος καταστροφής.
- Ονοματεπώνυμο αρμόδιου υπαλλήλου του υπεύθυνου επεξεργασίας που είναι υπεύθυνος για την καταστροφή.
- Εκτελών την καταστροφή (στη περίπτωση που η καταστροφή ανατίθεται σε εκτελούντα την επεξεργασία).

β) Όταν τα δεδομένα καταστρέφονται από εκτελούντα την επεξεργασία, το πρωτόκολλο καταστροφής πρέπει να συμπληρώνεται από τον ίδιο. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας θα πρέπει να συμπληρώνει πρωτόκολλο παράδοσης των δεδομένων προς καταστροφή και να λαμβάνει το πρωτόκολλο καταστροφής από τον εκτελούντα την επεξεργασία.

Άρθρο 6. Ασφαλής καταστροφή δεδομένων που τηρούνται σε ηλεκτρονική ή άλλη μορφή

1. Για την ασφαλή καταστροφή δεδομένων σε ηλεκτρονική μορφή δεν επαρκεί η απλή διαγραφή τους (π.χ. με την εντολή «DELETE»), καθώς κατά τον τρόπο αυτό διαγράφεται μόνο η αναφορά στα δεδομένα, ενώ τα ίδια τα δεδομένα ενδέχεται να είναι ανακτήσιμα με χρήση ειδικών προγραμμάτων λογισμικού.

2. Ο ενδεικνυόμενος τρόπος για την ασφαλή καταστροφή των δεδομένων που είναι αποθηκευμένα σε επανεγγράψιμα μέσα (π.χ. σκληροί δίσκοι, δισκέττες, επανεγγράψιμα DVD και CD) είναι η αλλοίωση των δεδομένων μέσω της αντικατάστασης τους με τυχαίους χαρακτήρες (overwrite). Η αλλοίωση μπορεί να γίνει με τη χρήση ειδικών προγραμμάτων (file erasers, file shredders, file pulveritizers). Στην περίπτωση της καθημερινής καταστροφής δεδομένων, ένας εναλλακτικός τρόπος καταστροφής είναι η μορφοποίηση του υλικού υποστρώματος (format).

3. Στην περίπτωση της προγραμματισμένης καταστροφής του συνόλου των δεδομένων, ένας εναλλακτικός τρόπος καταστροφής (για ιδιαίτερα κρίσιμα δεδομένα) είναι και η φυσική καταστροφή του ίδιου του υλικού υποστρώματος (π.χ. με θρυματισμό, κονιορτοποίηση, αποτέφρωση, με την επιφύλαξη ειδικών διατάξεων σχετικά με τη διαχείριση ειδικών αποβλήτων / προστασία του περιβάλλοντος).

4. Η καταστροφή των δεδομένων περιλαμβάνει και την καταστροφή όλων των αντιγράφων ασφαλείας (back up) που τηρεί ο υπεύθυνος επεξεργασίας.

5. Η προγραμματισμένη καταστροφή των δεδομένων πρέπει να συνοδεύεται από πρωτόκολλο καταστροφής, σύμφωνα το άρθρο 5, παρ. 3 της παρούσας.

Ο Πρόεδρος

Η Γραμματέας

Δημήτριος Γουργουράκης

Γεωργία Παλαιολόγου

Παράρτημα 1 – Μέσα επεξεργασίας και ενδεικνύόμενοι τρόποι καταστροφής

Μέσο επεξεργασίας	Ενδεικνύόμενοι τρόποι καταστροφής
Δεδομένα σε έντυπη μορφή	<ul style="list-style-type: none">• Τεμαχισμός• Πολτοποίηση-Ανακύκλωση• Αποτέφρωση
Δεδομένα σε ηλεκτρονική ή άλλη μορφή	<ul style="list-style-type: none">• Αλλοίωση δεδομένων (overwrite)• Μορφοποίηση (format)• Φυσική καταστροφή

Παράρτημα 2 – Πρότυπο πρωτοκόλλου καταστροφής

ΠΡΩΤΟΚΟΛΛΟ ΚΑΤΑΣΤΡΟΦΗΣ

Τα κάτωθι προσωπικά δεδομένα καταστράφηκαν σύμφωνα με τις σχετικές πολιτικές και διαδικασίες καταστροφής δεδομένων του οργανισμού μας.

Υπεύθυνος επεξεργασίας	
Ημερομηνία καταστροφής	Αρμόδιος υπάλληλος
Περιγραφή των στοιχείων που καταστράφηκαν	
Μέθοδος καταστροφής:	
Αποτέφρωση	
Τεμαχισμός	
Πολτοποίηση	
Αλλοίωση (overwrite)	
Μορφοποίηση (format)	
Φυσική καταστροφή εξοπλισμού	
Άλλο: -----	
Σε περίπτωση ανάθεσης, η καταστροφή έγινε από :	