ΜΝΗΜΟΝΙΟ ΣΥΝΕΡΓΑΣΙΑΣ ΜΕΤΑΞΥ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΣΤΑΤΙΣΤΙΚΗΣ ΑΡΧΗΣ (ΕΛΣΤΑΤ), ΤΗΣ ΓΕΝΙΚΗΣ ΓΡΑΜΜΑΤΕΙΑΣ ΔΗΜΟΣΙΩΝ ΕΣΟΔΩΝ (ΓΓΔΕ)

ΤΗΣ ΓΕΝΙΚΗΣ ΓΡΑΜΜΑΤΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ (ΓΓΠΣ)

ΚΑΙ ΤΟΥ ΙΔΡΥΜΑΤΟΣ ΚΟΙΝΩΝΙΚΩΝ ΑΣΦΑΛΙΣΕΩΝ (ΙΚΑ)

σχετικά με τις αρμοδιότητές τους και την ανταλλαγή στατιστικών πληροφοριών για την ενημέρωση του Στατιστικού Μητρώου Επιχειρήσεων, και τις ανάγκες των Διαρθρωτικών Ερευνών στις Επιχειρήσεις και των Εθνικών Λογαριασμών της Χώρας

Λαμβάνοντας υπόψη:

α) το Νόμο αριθ. 3832/2010 (ΦΕΚ 38/Α'/9.3.2010) «*Ελληνικό Στατιστικό Σύστημα (ΕΛΣΣ) - Σύσταση της Ελληνικής Στατιστικής Αρχής (ΕΛΣΤΑΤ) ως Ανεξάρτητης Αρχής*», όπως τροποποιηθείς ισχύει.

β) το άρθρο 51 του Νόμου 4021/2011 (ΦΕΚ 218/Α'/3.10.2011) «*Ενισχυμένα μέτρα εποπτείας και εξυγίανσης των πιστωτικών ιδρυμάτων – Ρύθμιση θεμάτων χρηματοπιστωτικού χαρακτήρα – Κύρωση της Σύμβασης – Πλαίσιο του Ευρωπαϊκού Ταμείου Χρηματοπιστωτικής Σταθερότητας και των τροποποιήσεών της και άλλες διατάξεις*»,

γ) τον Κανονισμό (ΕΚ) αριθ. 177/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ης Φεβρουαρίου 2008, για τη θέσπιση κοινού πλαισίου όσον αφορά τα μητρώα επιχειρήσεων για στατιστικούς σκοπούς, και τον εφαρμοστικό του Κανονισμό (ΕΚ) αριθ. 192/2009 της Επιτροπής,

δ) τον Κανονισμό (ΕΚ) αριθ. 295/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2008, σχετικά με τις στατιστικές διάρθρωσης των επιχειρήσεων,

ε) τον Κανονισμό (ΕΕ) αριθ. 549/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, για το ευρωπαϊκό σύστημα εθνικών και περιφερειακών λογαριασμών της Ευρωπαϊκής Ένωσης

στ) τον Κανονισμό (ΕΚ) αριθ. 223/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2009, σχετικά με τις ευρωπαϊκές στατιστικές,

ζ) την Υπουργική Απόφαση αριθ. 12833/Γ-528/2.7.1996 (ΦΕΚ 581/Β'/ 17.7.1996) με θέμα «*Παροχή στη Γ.Γ. ΕΣΥΕ πρόσθετων στοιχείων από το ΚΕΠΥΟ*», όπως συμπληρώθηκε και τροποποιήθηκε με την Υπουργική Απόφαση αριθ. 5110/Α1-3327/20.4.2006 (ΦΕΚ 581/ Β'/ 9.5.2006),

η) την υπ' αρ.Δ6Α 1117082ΕΞ2013 απόφαση του Υπουργού και του Υφυπουργού Οικονομικών «Μεταφορά αρμοδιοτήτων, προσωπικού και διαθέσιμων πόρων οργανικών μονάδων της Γενικής Διεύθυνσης ΚΕ.ΠΥ.Ο. της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (Γ.Γ.Π.Σ.) στη Γενική Διεύθυνση Δημοσίων Εσόδων και καθορισμός οργανικών θέσεων προσωπικού αυτής (ΦΕΚ Β' 1779), όπως ισχύει.

θ) το άρθρο 89 του ν. 3842/2010 (ΦΕΚ Α' 58) «Γραφείο Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων και Υποδομών στη Γενική Γραμματεία Πληροφοριακών Συστημάτων.

ι) τις διατάξεις του άρθρου 17 ν. 4174/2013 (ΦΕΚ Α' 170/26-7-2013), όπως ισχύει τροποποιηθείς.

ια) την Απόφαση 9843/7.10.2011 (ΦΕΚ 2469/Β'/4.11.2011) του Προέδρου της ΕΛΣΤΑΤ «*Έγκριση Κανονισμού Στατιστικών Υποχρεώσεων των φορέων του Ελληνικού Στατιστικού Συστήματος*»,

ιβ) την ανάγκη ενημέρωσης του στατιστικού μητρώου επιχειρήσεων της ΕΛΣΤΑΤ, με τη μικρότερη δυνατή επιβάρυνση των επιχειρήσεων για την παροχή των στοιχείων, ειδικά για τα στοιχεία που περιλαμβάνονται σε διοικητικά, νομικά και άλλα μητρώα και βάσεις δεδομένων, και προκειμένου η ΕΛΣΤΑΤ να ανταποκριθεί στις υποχρεώσεις της για παροχή έγκαιρων και έγκυρων στατιστικών διάρθρωσης των επιχειρήσεων στα αρμόδια Κοινοτικά και διεθνή όργανα, καθώς και για την παραγωγή των εθνικών λογαριασμών σύμφωνα με το ευρωπαϊκό σύστημα εθνικών και περιφερειακών λογαριασμών της Ευρωπαϊκής Ένωσης, οι ως άνω αναφερόμενοι φορείς αναλαμβάνουν τις ακόλουθες υποχρεώσεις:

Α) ΕΛΣΤΑΤ

Η ΕΛΣΤΑΤ υποχρεούται να διαβιβάζει στη Στατιστική Υπηρεσία της Ευρωπαϊκής Ένωσης (Eurostat), σε συγκεκριμένα χρονικά διαστήματα, όπως προβλέπεται από τον ισχύοντα Κανονισμό (ΕΚ) αριθ. 177/2008, ενημερωμένα αρχεία για τα στοιχεία του μητρώου επιχειρήσεων και των ομίλων επιχειρήσεων, να καταρτίζει ετησίως αντίγραφο της κατάστασης του μητρώου της στο τέλος του χρόνου και να τηρεί το αντίγραφο αυτό τουλάχιστον για 30 χρόνια. Ομοίως, να διαβιβάζει στη Eurostat, ετησίως, κατάλογο μεταβλητών, απαραίτητων για την ανάλυση του πληθυσμού των ενεργών επιχειρήσεων, των γεννήσεων και θανάτων των επιχειρήσεων, των περιπτώσεων επιβίωσης των νέων επιχειρήσεων και των συνεπειών που οι εν λόγω περιπτώσεις έχουν στη διάρθρωση, τη δραστηριότητα και την εξέλιξη του πληθυσμού των επιχειρήσεων και ειδικά των μικρών και μεσαίων επιχειρήσεων. Υποχρεούται ομοίως να διαβιβάζει στη Eurostat έγκυρες στατιστικές διάρθρωσης των επιχειρήσεων σύμφωνα με τα προβλεπόμενα στον Κανονισμό (ΕΚ) αριθ. 295/2008 και να παράγει τους εθνικούς λογαριασμούς της Χώρας σύμφωνα με τον Κανονισμό (ΕΕ) αριθ. 549/2013.

Στο πλαίσιο αυτό, η ΕΛΣΤΑΤ υποχρεούται:

1. Να τηρεί στατιστικό μητρώο επιχειρήσεων και ομίλων επιχειρήσεων που βρίσκονται στην ελληνική επικράτεια.
2. Να ενημερώνει το στατιστικό μητρώο επιχειρήσεων και ομίλων επιχειρήσεων με τις πιο πρόσφατες πληροφορίες που αφορούν σε καθεμία μεταβλητή του Παραρτήματος του Κανονισμού (ΕΚ) αριθ. 192/2009.
3. Να καταρτίζει, ελέγχει και διαβιβάζει ενημερωμένα αντίγραφα του μητρώου στη Eurostat, όπως προβλέπεται στον Κανονισμό (ΕΚ) αριθ. 177/2008.
4. Να καταρτίζει, ελέγχει και διαβιβάζει τα δημογραφικά χαρακτηριστικά των επιχειρήσεων του μητρώου της.
5. Να διασφαλίζει την εσωτερική συνέπεια των στοιχείων που λαμβάνει από τους διάφορους φορείς και να ζητά επεξηγήσεις από αυτούς, όποτε κρίνει απαραίτητο.
6. Να αναθεωρεί, όποτε κρίνει αναγκαίο, ή επιβάλλεται από τη Eurostat, τη μεθοδολογία και τις πηγές κατάρτισης/επικαιροποίησης του στατιστικού μητρώου επιχειρήσεων.

7. Να διασφαλίζει το απόρρητο των στοιχείων που λαμβάνει από τους συνεργαζόμενους φορείς, ΓΓΔΕ, ΓΓΠΣ και ΙΚΑ, και να τηρεί αυτά σε ασφαλή φυσικό και ηλεκτρονικό χώρο.

8. Να χρησιμοποιεί τα απόρρητα στοιχεία που λαμβάνει από τους συνεργαζόμενους φορείς, ΓΓΔΕ, ΓΓΠΣ και ΙΚΑ, αποκλειστικά για σκοπούς στατιστικής και να παρέχει δικαίωμα πρόσβασης σε αυτά τα στοιχεία, στο πλαίσιο των αρμοδιοτήτων της ΕΛΣΤΑΤ, μόνο στα πρόσωπα που προβλέπονται στην παράγραφο 3 του άρθρου 8 του ν. 3832/2010, όπως ισχύει, των οποίων η πράξη ορισμού θα κοινοποιείται στο Γραφείο Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων και Υποδομών (ΓΑΠΣ ΓΓΠΣ).

9. Να παρέχει, στους συνεργαζόμενους φορείς, ΓΓΔΕ, ΓΓΠΣ και ΙΚΑ, πληροφορίες και διευκρινίσεις σε μεθοδολογικά θέματα, εφόσον ζητηθούν.

10. Να ενημερώνει τους συνεργαζόμενους φορείς για τις ευρωπαϊκές και εθνικές ταξινομήσεις οικονομικών δραστηριοτήτων και των επαγγελμάτων που είναι σε ισχύ.

11. Να παρέχει, στους συνεργαζόμενους φορείς επικαιροποιημένο κατάλογο γεωγραφικών κωδικών.

Β) Γ.Γ.Δ.Ε.

Η Γ.Γ.Δ.Ε. αναλαμβάνει τις ακόλουθες υποχρεώσεις:

1. Να παρέχει στην ΕΛΣΤΑΤ τα ακόλουθα στοιχεία επιχειρήσεων/νομικών μονάδων, φυσικών και μη φυσικών προσώπων και ασκούντων ελεύθερα επαγγέλματα, από το Μητρώο TAXIS που τηρεί:

   α) ΑΦΜ,
   β) ονοματεπώνυμο / επωνυμία / τίτλος επιχείρησης,
   γ) ταχυδρομική διεύθυνση, τηλέφωνο, φαξ και e-mail,
   δ) Κωδικός Αριθμός Δραστηριότητας (ΚΑΔ), κύριας, δευτερευουσών, βοηθητικών και λοιπών οικονομικών δραστηριοτήτων,
   ε) νομική μορφή,
   στ) ημερομηνία έναρξης εργασιών / δραστηριότητας επιχείρησης / εγκατάστασης,
   ζ) ημερομηνία διακοπής εργασιών / δραστηριότητας επιχείρησης / εγκατάστασης,
   η) κατάσταση επιχείρησης και ημερομηνίες μεταβολών επιχείρησης / εγκατάστασης,
   θ) οποιαδήποτε μεταβολή επέρχεται στα ανωτέρω στοιχεία α) έως η).

2. Να παρέχει στην ΕΛΣΤΑΤ στοιχεία υποκαταστημάτων / τοπικών μονάδων των επιχειρήσεων, με την αντίστοιχη πληροφορία, όπως περιλαμβάνεται στα ανωτέρω στοιχεία α) έως και θ), για κάθε υποκατάστημα / τοπική μονάδα.

3. Να παρέχει στην ΕΛΣΤΑΤ στοιχεία έδρας αλλοδαπής επιχείρησης, εγκατάστασης εξωτερικού και εγκατάστασης εσωτερικού, από τις αντίστοιχες δηλώσεις των εντύπων του Μητρώου TAXIS.

4. Να παρέχει στην ΕΛΣΤΑΤ στοιχεία και αρχεία σχέσεων μελών και συμμετοχών επιχειρήσεων και επιτηδευματιών.

5. Να παρέχει στην ΕΛΣΤΑΤ οικονομικά στοιχεία επιχειρήσεων και επιτηδευματιών, ανά ΑΦΜ, από τις Δηλώσεις Φορολογίας Εισοδήματος (Ε1), (Ε3), (Ε5) και τις αντίστοιχες Δηλώσεις Φορολογίας Εισοδήματος όλων των νομικών προσώπων, αναλυτικά, ανά κατηγορία εισοδήματος, καθώς και τους πίνακες ισολογισμών και το ισοζύγιο που υποβάλλουν σε ηλεκτρονική μορφή οι επιχειρήσεις.

6. Να παρέχει στην ΕΛΣΤΑΤ στοιχεία απασχόλησης (μόνιμο και εποχικά απασχολούμενο προσωπικό, πλήρους και μερικής απασχόλησης, ωρομίσθιοι) από τις οριστικές και προσωρινές Δηλώσεις Απόδοσης Φόρου Μισθωτών Υπηρεσιών (Έντυπο Ε7) και υπηρεσιών από ελεύθερα επαγγέλματα, ανά ΑΦΜ.

7. Να παρέχει στην ΕΛΣΤΑΤ όλα τα οικονομικά στοιχεία (κύκλος εργασιών, απασχόληση κλπ.) από τις περιοδικές και εκκαθαριστικές δηλώσεις ΦΠΑ, ανά ΑΦΜ.

8. Να παρέχει στην ΕΛΣΤΑΤ στοιχεία από τις Συγκεντρωτικές Καταστάσεις Πελατών – Προμηθευτών ανά ΚΑΔ, πελάτη – προμηθευτή, Δ.Ο.Υ. και Ταχυδρομικό Κώδικα..

9. Να διαβιβάζει στην ΕΛΣΤΑΤ τα ανωτέρω αναφερόμενα στοιχεία, ως εξής:

   α) τα στοιχεία των παραγράφων 1 έως και 4, κάθε μήνα,

   β) τα στοιχεία των παραγράφων 5 και 6, αμέσως μετά την υποβολή τους από τις επιχειρήσεις και τον έλεγχό τους από τη Γ.Γ.Δ.Ε., και, οπωσδήποτε, πριν την παρέλευση ενός έτους από τη λήξη του έτους αναφοράς των στοιχείων (ημερολογιακό έτος),

   γ) τα στοιχεία της παραγράφου 7, αμέσως μετά την υποβολή τους από τις επιχειρήσεις και τον έλεγχό τους από τη Γ.Γ.Δ.Ε., και, όσον αφορά τα στοιχεία των εκκαθαριστικών δηλώσεων ΦΠΑ, οπωσδήποτε, πριν την παρέλευση δύο ετών από τη λήξη του έτους αναφοράς των στοιχείων (ημερολογιακό έτος),

   δ) τα στοιχεία της παραγράφου 8, αμέσως μετά την υποβολή τους από τις επιχειρήσεις και τον έλεγχό τους από τη Γ.Γ.Δ.Ε..

10. Να διασφαλίζει την ακρίβεια, αξιοπιστία και εγκυρότητα των ανωτέρω στοιχείων που θα διαβιβάζει στην ΕΛΣΤΑΤ.

11. Να διαβιβάζει, σε πρώτη φάση, τα ανωτέρω στοιχεία σε ηλεκτρονική μορφή, ώστε να είναι επεξεργάσιμα από την ΕΛΣΤΑΤ και να συνεργαστεί άμεσα με την ΕΛΣΤΑΤ στην εφαρμογή άμεσης (on line) διαβίβασης των προαναφερομένων στοιχείων μέσω της ΓΓΠΣ, προκειμένου αυτά να αντλούνται αυτομάτως και να ελαχιστοποιηθεί η διοικητική επιβάρυνση της Γ.Γ.Δ.Ε.

    Για τη διαβίβαση των στοιχείων σε ηλεκτρονική μορφή και την άμεση (on line) διαβίβαση των στοιχείων, θα πρέπει να ακολουθούνται οι οδηγίες του Γραφείου Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων και Υποδομών της Γ.Γ.Π.Σ (ΓΑΠΣ ΓΓΠΣ), σύμφωνα με τον Κανονισμό Ανταλλαγής Στοιχείων μεταξύ Γ.Γ.Π.Σ., Γ.Γ.Δ.Ε., ΕΛ.ΣΤΑΤ και Ι.Κ.Α, ο οποίος αποτελεί παράρτημα του παρόντος.

12. Να διαβιβάζει στο ΙΚΑ, σε ετήσια βάση, τα ακόλουθα στοιχεία επιχειρήσεων/νομικών μονάδων, φυσικών και μη φυσικών προσώπων και ασκούντων ελεύθερα επαγγέλματα, από το Μητρώο TAXIS που τηρεί:

α) ΑΦΜ,

β) ονοματεπώνυμο / επωνυμία / τίτλος επιχείρησης,

γ) ταχυδρομική διεύθυνση, τηλέφωνο, φαξ και e-mail,

δ) Κωδικός Αριθμός Δραστηριότητας (ΚΑΔ), κύριας δραστηριότητας.

Γ) Γ.Γ.Π.Σ.

Η Γ.Γ.Π.Σ., δια του Γραφείου Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων και Υποδομών (ΓΑΠΣ Γ.Γ.Π.Σ.), αναλαμβάνει τις ακόλουθες υποχρεώσεις:

1. Την παροχή οδηγιών και λοιπών διευκρινήσεων στους λοιπούς εμπλεκόμενους φορείς για την ορθή εφαρμογή του Κανονισμού Ανταλλαγής Στοιχείων μεταξύ ΓΓΠΣ, ΓΓΔΕ, ΕΛΣΤΑΤ και ΙΚΑ.

2. Την εισήγηση επικαιροποιημένου σχεδίου του Κανονισμού Ανταλλαγής Στοιχείων μεταξύ Γ.Γ.Π.Σ.,Γ.Γ.Δ.Ε., ΕΛ.ΣΤΑΤ και Ι.Κ.Α., οσάκις αυτό απαιτηθεί, μετά από αμοιβαία απόφαση των διοικήσεων των εμπλεκόμενων φορέων.

Δ) Ι.Κ.Α.

Το ΙΚΑ - Γενική Διεύθυνση Πληροφορικής και Δ/νση Αναλογιστικών Μελετών και Στατιστικής - αναλαμβάνει τις ακόλουθες υποχρεώσεις:

1. Να παρέχει στην ΕΛΣΤΑΤ μηνιαία στοιχεία ασφαλισμένων κοινών επιχειρήσεων και ασφαλισμένων οικοδομοτεχνικών έργων, ανά έργο, τα οποία θα περιλαμβάνουν:

α) ΑΦΜ εργοδότη-επιχείρησης,

β) ονοματεπώνυμο εργοδότη / επωνυμία / τίτλο επιχείρησης,

γ) ταχυδρομική διεύθυνση, τηλέφωνο και φαξ,

δ) Κωδικό Αριθμό Δραστηριότητας (ΚΑΔ) της επιχείρησης,

ε) α/α παραρτήματος εργοδότη,

στ) αριθμό εργαζομένων (με διάκριση σε εργαζόμενους με πλήρες ωράριο και μη)

2. Να διαβιβάζει στην ΕΛΣΤΑΤ τα ανωτέρω στοιχεία της παραγράφου 1 για το σύνολο ενός συγκεκριμένου ημερολογιακού έτους, με μηνιαία ανάλυση, εντός του πρώτου εξαμήνου από τη λήξη του έτους αναφοράς τους, καθώς και όποτε αυτά ζητηθούν από την ΕΛΣΤΑΤ, με την πλέον πρόσφατη επικαιροποίησή τους.

3. Να παρέχει στην ΕΛΣΤΑΤ το σύνολο των ετήσιων αποδοχών, όλων των τύπων αθροιστικά και το σύνολο των αντίστοιχων ετήσιων εισφορών ασφαλισμένων και εργοδοτών που δηλώνονται στις Α.Π.Δ. από τους εργοδότες, ανά αριθμό παραρτήματος, Κ.Α.Δ. και Νομό της Χώρας.

4. Να διαβιβάζει στην ΕΛΣΤΑΤ τα ανωτέρω στοιχεία της παραγράφου 3 για το σύνολο ενός συγκεκριμένου ημερολογιακού έτους, εντός του πρώτου εξαμήνου από τη λήξη του έτους αναφοράς τους.

5. Να διασφαλίζει την ακρίβεια, αξιοπιστία και εγκυρότητα των στοιχείων που θα διαβιβάζει στην ΕΛΣΤΑΤ.

6. Να διαβιβάζει τα ανωτέρω στοιχεία σε ηλεκτρονική μορφή, ώστε να είναι επεξεργάσιμα από την ΕΛΣΤΑΤ.

Η ανταπόκριση της ΕΛΣΤΑΤ, της ΓΓΔΕ, της ΓΓΠΣ και του ΙΚΑ στις ανωτέρω υποχρεώσεις προϋποθέτει τη σύσταση Ομάδας Εργασίας, η οποία θα έχει ως αντικείμενο θέματα εφαρμογής των υποχρεώσεων του παρόντος μνημονίου.

Τόσο η ΕΛΣΤΑΤ όσο και οι ανωτέρω φορείς (ΓΓΔΕ, ΓΓΠΣ και ΙΚΑ) δεσμεύονται ότι θα τηρήσουν τις υποχρεώσεις που περιγράφονται στο παρόν μνημόνιο, σε συνδυασμό με τις σχετικές υποχρεώσεις τους που απορρέουν από την εφαρμογή του Κανονισμού Στατιστικών Υποχρεώσεων των φορέων του ΕΛΣΣ, όπως αυτός προβλέπεται στο άρθρο 2 παρ. 2 του Νόμου 3832/2010. Η παράβαση των εν λόγω υποχρεώσεων επισύρει την επιβολή των σχετικών κυρώσεων που προβλέπονται στα άρθρα 2 και 8 του ανωτέρω Νόμου και στα άρθρα 9, 10 και 11 του Κανονισμού Στατιστικών Υποχρεώσεων των φορέων του ΕΛΣΣ.

Τα εξουσιοδοτημένα από κάθε ένα από τους ανωτέρω φορείς άτομα, τα οποία μετέχουν άμεσα ή έμμεσα στην επεξεργασία, διακίνηση ή αποθήκευση των πληροφοριών πρέπει να ακολουθούν όσα ορίζονται στον Κανονισμό Ανταλλαγής Στοιχείων μεταξύ ΓΓΠΣ, ΓΓΔΕ, ΕΛΣΤΑΤ και ΙΚΑ, ο οποίος αποτελεί παράρτημα του παρόντος.

Το παρόν συντάχθηκε σε τέσσερα αντίτυπα, ένα εκ των οποίων παραλαμβάνει ο κάθε υπογράφων.

Ο Πρόεδρος της ΕΛΣΤΑΤ	Ο Γεν. Γραμματέας της ΓΓΔΕ	Ο Διοικητής του ΙΚΑ	Ο Γεν. Γραμματέας της ΓΓΠΣ
Ανδρέας Β. Γεωργίου	Θεοχάρης Θεοχάρης	Ροβέρτος Σπυρόπουλος	Χαράλαμπος Τσαβδάρης

ΠΑΡΑΡΤΗΜΑ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ - ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΚΩΝ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Γραφείο Ασφάλειας Πληροφοριακών Συστημάτων
και Προστασίας Δεδομένων και Υποδομών ΓΓΠΣ

ΚΑΝΟΝΙΣΜΟΣ ΑΝΤΑΛΛΑΓΗΣ ΣΤΟΙΧΕΙΩΝ ΜΕΤΑΞΥ Γ.Γ.Π.Σ.,Γ.Γ.Δ.Ε., ΕΛ.ΣΤΑΤ και Ι.Κ.Α.

Εισηγητής: Κεφαλληνός Διονύσιος, 2131332392, d.kefallinos@gsis.gr

1. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ - ΣΤΟΧΟΙ

Η παρούσα πολιτική εφαρμόζεται κατά την ανταλλαγή ευαίσθητων δεδομένων σε ηλεκτρονική μορφή μεταξύ της Γ.Γ.Π.Σ,Γ.Γ.Δ.Ε. και της ΕΛ.ΣΤΑΤ και του Ι.Κ.Α., στο πλαίσιο του παρόντος μνημονίου συνεργασίας.

Ως ευαίσθητα χαρακτηρίζονται τα ακόλουθα στοιχεία:

α) Δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων, όπως αυτά ορίζονται από την από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και την κείμενη νομοθεσία.

β) Δεδομένα τα οποία περιέχουν οικονομικά/φορολογικά στοιχεία του Δημοσίου Τομέα ή ιδιωτικών οργανισμών και επιχειρήσεων.

γ) Δεδομένα που έχουν χαρακτηριστεί ως διαβαθμισμένα από αρμόδια Κρατική Αρχή.

Το πεδίο εφαρμογής της πολιτικής είναι τα πληροφοριακά συστήματα (ΠΣ), οι διαδικασίες και οι διοικητικές δομές των εμπλεκομένων οργανισμών που διακινούν δεδομένα σε ηλεκτρονική μορφή, με ένα από τα ακόλουθα σχήματα:

α) Χειροκίνητη διακίνηση (σχήμα 1). Τα δεδομένα παράγονται, διακινούνται και καταναλώνονται με την πρωτοβουλία και το χειρισμό φυσικών προσώπων και όχι μέσω αυτοματισμών που ενεργοποιούνται περιοδικά ή σε απόκριση συγκεκριμένων συνθηκών. Η απόδοση ευθύνης για την διακίνηση των δεδομένων γίνεται με τεχνικά μέσα άμεσα στα άτομα που τα διακινούν.

β) Μερικώς αυτοματοποιημένη διακίνηση (σχήμα 2). Η παραγωγή και η κατανάλωση των δεδομένων γίνεται χειροκίνητα, υπάρχει όμως αυτοματοποιημένο σύστημα διακίνησης και παρακολούθησης δεδομένων, στο οποίο εισάγονται αυτά μετά την παραγωγή τους και από το οποίο εξάγονται προς κατανάλωση. Το σύστημα διακίνησης αποτελείται από εξυπηρετητές και σταθμούς εργασίας με ειδικευμένο λογισμικό ασφαλούς διακίνησης δεδομένων, με διαπροσωπία (user interface) είτε ειδικού τύπου, είτε βασισμένης σε ασφαλείς ιστοσελίδες (HTTPS). Η απόδοση προσωπικής ευθύνης γίνεται βάση

των διαπιστευτηρίων των χρηστών του συστήματος διακίνησης, σε συνδυασμό με πλήρεις καταγραφές συμβάντων εισαγωγής, μετάδοσης και εξαγωγής δεδομένων.

γ) Πλήρως αυτοματοποιημένη διακίνηση (σχήμα 3). Στην περίπτωση αυτή τα ΠΣ των εμπλεκομένων οργανισμών είναι συνδεδεμένα μεταξύ τους (backend-to-backend). Δίδεται η δυνατότητα στον ένα οργανισμό, είτε αυτόματα είτε με χειροκίνητη πρωτοβουλία να θέτει ερωτήματα στην αποθήκη δεδομένων του οργανισμού-κατόχου, με αποτέλεσμα την αυτόματη παραγωγή, τη διακίνηση και την εισαγωγή των δεδομένων στο ΠΣ του οργανισμού-αποδέκτη. Στο σύστημα αυτό καθορίζεται σαφώς πιο υποσύνολο δεδομένων του οργανισμού-κατόχου είναι προσβάσιμο (τυπικά με τη δημιουργία ενδιάμεσης αποθήκης δεδομένων – staging data store), τι μετασχηματισμοί γίνονται στα δεδομένα πριν διακινηθούν, καθώς και η ενδιάμεση αποθήκη δεδομένων του ΠΣ του οργανισμού-παραλήπτη στην οποία τοποθετούνται τα δεδομένα. Η διακίνηση των δεδομένων γίνεται μεταξύ των εξυπηρετητών που υλοποιούν τη διασύνδεση και η επικοινωνία μεταξύ αυτών γίνεται με ασφαλή κανάλια επικοινωνίας. Η απόδοση προσωπικής ευθύνης γίνεται βάση των διαπιστευτηρίων που χρησιμοποιούν οι χρήστες του συστήματος διακίνησης, σε συνδυασμό με πλήρεις καταγραφές συμβάντων εισαγωγής, μετάδοσης και εξαγωγής δεδομένων.

Στις δύο τελευταίες περιπτώσεις διακίνησης μπορεί να μετέχει τρίτος ιδιωτικός ή δημόσιος φορέας, ο οποίος έχει το ρόλο του Επιχειρηματικού Διαύλου Υπηρεσιών (Enterprise Service Bus) και ο οποίος αναλαμβάνει όλες τις λεπτομέρειες της διακίνησης και του μετασχηματισμού. Ο φορέας αυτός μετέχει έχοντας υπογράψει σύμβαση ποιότητας υπηρεσίας (Service Level Agreement), εμπιστευτικότητας (Confidentiality Agreement) και απόδοσης ευθύνης (Non-Repudiation Agreement). Αυτού του είδους η διακίνηση είναι δυνατό να προσφέρεται σαν έτοιμη λύση (turn-key solution) από έναν από τους μετέχοντες οργανισμούς.

Στόχοι της πολιτικής αυτής είναι να διασφαλίσει με ισχυρά τεχνικά μέσα σε όλες τις περιπτώσεις και σε όλες τις φάσεις της διακίνησης των δεδομένων, από την παραγωγή μέχρι την κατανάλωση τα ακόλουθα:

α) Την εμπιστευτικότητα, έτσι ώστε τα δεδομένα να είναι προσβάσιμα μόνο από τα εξουσιοδοτημένα άτομα των εμπλεκομένων οργανισμών.
β) Την ακεραιότητα, έτσι ώστε να είναι δυνατή η επαλήθευση της μη αλλοίωσης των διακινούμενων δεδομένων σε σχέση με τη μορφή που είχαν όταν παράχθηκαν.
γ) Την προσωπική απόδοση ευθύνης / αποφυγή αποποίησης ευθύνης σε / από φυσικά πρόσωπα των εμπλεκομένων οργανισμών για την μεταβίβαση και την απελευθέρωση των δεδομένων προς τρίτους, έτσι ώστε να αποφεύγεται η διάχυση της ευθύνης εντός των οργανισμών.

2. ΠΟΛΙΤΙΚΗ ΡΟΗΣ ΔΕΔΟΜΕΝΩΝ

Η πολιτική ροής των δεδομένων από τον οργανισμό που τα κατέχει στον οργανισμό που τα παραλαμβάνει χωρίζεται σε τρεις κύριες φάσεις:

α) Φάση παραγωγής.

β) Φάση μετάδοσης.

γ) Φάση κατανάλωσης.

2.1 Φάση παραγωγής

Η φάση της παραγωγής λαμβάνει χώρα εξ' ολοκλήρου εντός του οργανισμού που κατέχει αρχικά τα δεδομένα και διακρίνεται στις ακόλουθες υποφάσεις:

α) Πηγής δεδομένων.

β) Πρόσβασης στα δεδομένα.

γ) Μετασχηματισμού των δεδομένων στην απαιτούμενη από τον αποδέκτη μορφή.

δ) Τοποθέτησης των δεδομένων στο υποσύστημα εκπομπής/διακίνησης αυτών.

2.1.1 Υποφάση πηγής δεδομένων

Αρχικά τα δεδομένα φυλάσσονται σε ασφαλείς διατάξεις βάσεων δεδομένων του οργανισμού που τα κατέχει και τα διαφυλάσσει. Τα μέτρα ασφαλείας που υλοποιούνται περιγράφονται στην ενότητα Μέτρα Ασφαλείας Δεδομένων.

2.1.2 Υποφάση πρόσβασης

Στη φάση αυτή γίνεται πρόσβαση στα δεδομένα έτσι ώστε να διακινηθούν. Η πρόσβαση γίνεται είτε κατευθείαν από φυσικά πρόσωπα, είτε από εφαρμογές που χειρίζονται φυσικά πρόσωπα, είτε από εξυπηρετητές που μετέχουν στο υποσύστημα διακίνησης. Σε κάθε περίπτωση υπάρχει έλεγχος πρόσβασης ο οποίος ενέχει επαλήθευση ταυτότητας, καταγραφή πρόσβασης και διακίνησης δεδομένων και μηχανισμούς αποφυγής κακόβουλης/αθέμιτης ανακατεύθυνσης (υποκλοπής) των δεδομένων κατά την εκπομπή τους διαμέσου του τοπικού δικτύου του οργανισμού, όπως περιγράφεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων.

2.1.3 Υποφάση μετασχηματισμού

Προκειμένου τα δεδομένα να διακινηθούν στον οργανισμό αποδέκτη, από την αρχική τους μορφή εντός της βάσης δεδομένων που φυλάσσονται, μετασχηματίζονται ώστε να αποκαλύπτονται τα λιγότερα δυνατά στοιχεία, αλλά να ικανοποιούνται και οι απαιτήσεις του οργανισμού αποδέκτη, με τους περιορισμούς που θέτει η κείμενη νομοθεσία.

Ο μετασχηματισμός γίνεται με λογισμικό για το οποίο ισχύουν οι κανόνες για την πρόσβαση και διακίνηση των δεδομένων που περιγράφονται στην ενότητα Μέτρα Ασφαλείας Δεδομένων.

Τα δεδομένα είναι δυνατόν να διακινηθούν εντός του οργανισμού που τα παράγει σε ενδιάμεση μορφή πριν μετασχηματιστούν, οπότε ισχύουν και πάλι οι κανόνες που περιγράφονται στην ενότητα Μέτρα Ασφαλείας Δεδομένων.

2.1.4 Υποφάση τοποθέτησης

Μετά το μετασχηματισμό τους στη μορφή που απαιτείται από τον αποδέκτη, τα δεδομένα αποθηκεύονται στο υποσύστημα που θα χρησιμοποιηθεί για τη διακίνησή

τους. Σε αυτό το σημείο τα δεδομένα έχουν μία από τις ακόλουθες δύο μορφές, ανάλογα με το σχήμα διακίνησης που υλοποιείται:

α) Ένα ή περισσότερα ηλεκτρονικά αρχεία (files), τα οποία αποτελούν ένα ενιαίο πακέτο προς αποστολή. Το πακέτο αρχείων είτε θα διακινηθεί από τον/τους υπεύθυνους διακίνησης, στο σχήμα χειροκίνητης διακίνησης, είτε θα εισαχθεί στο ειδικό λογισμικό διακίνησης, στο σχήμα μερικώς αυτοματοποιημένης διακίνησης.

β) Μια ενδιάμεση αποθήκη δεδομένων (staging data store). Τα δεδομένα παραμένουν εκεί προς κατά βούληση κατανάλωση με πρωτοβουλία του οργανισμού αποδέκτη. Σε αυτή την περίπτωση ισχύουν όλοι οι προαναφερθέντες κανόνες ασφαλείας που εφαρμόζονται και για την πρωτεύουσα αποθήκη δεδομένων του οργανισμού-κατόχου, όπως περιγράφεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων.

Για την περαιτέρω διαδικασία διακρίνονται τρεις περιπτώσεις, ανάλογα με το σχήμα διακίνησης:

α) Χειροκίνητη διακίνηση. Κάθε αρχείο υπογράφεται ψηφιακά από το φυσικό πρόσωπο που είναι τελικά υπεύθυνο για την αποστολή τους στον οργανισμό αποδέκτη. Τα μέτρα ασφαλείας που υλοποιούνται περιγράφονται στην ενότητα Μέτρα Ασφαλείας Δεδομένων.

β) Μερικώς αυτοματοποιημένη διακίνηση. Τα πακέτο δεδομένων προς διακίνηση εισάγεται σε ειδικό λογισμικό ασφαλούς διακίνησης, είτε μέσω λογισμικού-πελάτη εγκατεστημένου στο σταθμό εργασίας των υπευθύνων διακίνησης, είτε μέσω ιστοσελίδας που βρίσκεται στους εξυπηρετητές αυτού. Σε κάθε περίπτωση, για τους σταθμούς εργασίας και τους εξυπηρετητές που χρησιμοποιούνται ισχύουν αυτά που προβλέπονται στην ενότητα Μέτρα Ασφαλείας Δεδομένων. Η είσοδος στο λογισμικό διακίνησης γίνεται με τα προσωπικά διαπιστευτήρια των υπευθύνων διακίνησης για τα οποία ισχύουν οι κανόνες που προβλέπονται στην ενότητα Μέτρα Ασφαλείας Δεδομένων.

Το ειδικό λογισμικό διακίνησης αποθηκεύει τα προς διακίνηση δεδομένα σε εσωτερική σε αυτό αποθήκη δεδομένων, η οποία διασφαλίζει την εμπιστευτικότητα εν ακινησία (privacy in situ), όμως ορίζεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων. Το λογισμικό διακίνησης διασφαλίζει επίσης την ακεραιότητα των δεδομένων με αλγόριθμο κατάτμησης. Διασφαλίζει επίσης την απόδοση ευθύνης για την αποστολή των δεδομένων είτε με προσωπικό ψηφιακό πιστοποιητικό του/των φυσικών προσώπων υπευθύνων για την αποστολή ως ανωτέρω, είτε με ψηφιακή υπογραφή που παράγεται βάση ψηφιακού πιστοποιητικού του εξυπηρετητή διακίνησης. Στην περίπτωση αυτή τα πιστοποιητικά εξυπηρετητή δηλώνονται με ασφαλή τρόπο στον οργανισμό αποδέκτη ώστε να διασφαλίζεται η αποδοχή τους και η εμπιστοσύνη προς αυτά. Σε κάθε περίπτωση, το λογισμικό διακίνησης διατηρεί καταγραφές των εισαγωγών δεδομένων προς διακίνηση, συμπεριλαμβανομένων ημερομηνίας, ώρας και διαπιστευτηρίων χρήστη που εισήγαγε τα δεδομένα.

γ) Πλήρως αυτοματοποιημένη διακίνηση. Τα δεδομένα παραμένουν στην ενδιάμεση αποθήκη, για την οποία ισχύουν αυτά που αναφέρονται στην ενότητα Μέτρα Ασφαλείας Δεδομένων. Η τοποθέτηση των δεδομένων γίνεται βάση ερωτήματος (query) που θέτει ο οργανισμός-αποδέκτης στην ενδιάμεση αποθήκη του οργανισμού-κατόχου και το πακέτο δεδομένων προς διακίνηση είναι αποτέλεσμα αυτής της αυτοματοποιημένης διαδικασίας. Γίνεται αμφίδρομη επαλήθευση ταυτότητας των εξυπηρετητών του οργανισμού-αποδέκτη (ο οποίος θέτει το ερώτημα) και του οργανισμού-κατόχου (ο οποίος δέχεται το ερώτημα και παράγει τα δεδομένα προς διακίνηση), είτε με ψηφιακά πιστοποιητικά εξυπηρετητή, είτε με ζεύγη κλειδιών που έχουν εκδοθεί από τους οργανισμούς, βάση αλγορίθμων δημοσίου κλειδιού (public key cryptography), όπως ορίζεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων. Και στις δύο περιπτώσεις έχουν ανταλλαγεί με ασφαλή τρόπο μεταξύ των οργανισμών κατά την αρχικοποίηση του συστήματος.

Η τοποθέτηση του ερωτήματος γίνεται μέσα από ασφαλές κανάλι επικοινωνίας, όπως προδιαγράφεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων. Τα δεδομένα δεν αποθηκεύονται προσωρινά, αλλά προχωρούν κατευθείαν στη φάση μετάδοσης. Η απόδοση προσωπικής ευθύνης γίνεται βάση των προσωπικών διαπιστευτηρίων που χρησιμοποιούν οι χρήστες του συστήματος διακίνησης. Το λογισμικό διακίνησης διατηρεί καταγραφές ερωτημάτων που έχουν τεθεί και των διαπιστευτηρίων εξυπηρετητών και χρηστών που τα έθεσαν.

2.2 Φάση μετάδοσης

Σε αυτή τη φάση τα δεδομένα διακινούνται έτσι ώστε να διασφαλίζεται η εμπιστευτικότητα και να μπορούν να αναγνωστούν μόνο από τα φυσικά πρόσωπα του οργανισμού παραλήπτη που είναι υπεύθυνα για την παραλαβή και τον περαιτέρω χειρισμό και προστασία των δεδομένων. Για το σκοπό αυτό και ανάλογα με το σχήμα διακίνησης διακρίνονται τρεις περιπτώσεις:

α) Χειροκίνητη διακίνηση. Στην περίπτωση αυτή τα φυσικά πρόσωπα που έχουν οριστεί ως υπεύθυνοι για παραλαβές δεδομένων διαθέτουν προσωπικά ψηφιακά πιστοποιητικά, ανάλογα με αυτά των υπευθύνων αποστολής. Ο υπεύθυνος αποστολής ενός συγκεκριμένου πακέτου δεδομένων το κρυπτογραφεί με το πιστοποιητικό ενός των υπευθύνων παραλαβής, μετά από σχετική συμφωνία είτε για το συγκεκριμένο πακέτο, είτε για όλες τις αποστολές.

Με τον τρόπο αυτό τα δεδομένα μπορούν να αποκρυπτογραφηθούν μόνο από το συγκεκριμένο άτομο, ο οποίος ορίζεται εφεξής ως υπεύθυνος χειρισμού και προστασίας του συγκεκριμένου πακέτου στον οργανισμό παραλήπτη. Αντίστοιχα ο παραλήπτης διαθέτει τεχνικό τρόπο (μέσω της ψηφιακής υπογραφής των δεδομένων) για τον έλεγχο της ακεραιότητας και την αυθεντικότητας των δεδομένων που παρέλαβε, όπως και της ταυτότητας του αποστολέα.

Για κάθε πακέτο δεδομένων που στάλθηκαν είναι επομένως γνωστός τόσο ο αποστολέας όσο και ο παραλήπτης. Καθένας από αυτούς θεωρείται το σημείο οροθεσίας και επαφής της εμπιστοσύνης ανάμεσα στους δύο οργανισμούς για τη συγκεκριμένη αποστολή. Ο αποστολέας υπογράφει για την παραγωγή και την αποστολή των δεδομένων και ο παραλήπτης «υπογράφει» την παραλαβή και τον περαιτέρω χειρισμό τους. Ο αποστολέας υπογράφει για την ορθότητα, την εμπιστευτικότητα και τη διαφύλαξη των δεδομένων για τον οργανισμό που αποστέλλει και ο αποδέκτης υπογράφει για την ορθότητα, την εμπιστευτικότητα και τη διαφύλαξη των δεδομένων για τον οργανισμό που παραλαμβάνει. Κατά τη διερεύνηση περιστατικού διαρροής ή αλλοίωσης δεδομένων, γίνεται ανίχνευση για το αν προήλθαν από τον οργανισμό-αποδέκτη και αποδίδονται προσωπικές ευθύνες στον αντίστοιχο υπεύθυνο παραλαβής.

Ο αποστολέας είναι δυνατό να ζητήσει και την φυσική υπογραφή του παραλήπτη για την παραλαβή των δεδομένων.

β) Μερικώς αυτοματοποιημένη διακίνηση. Η διακίνηση γίνεται από το ειδικό λογισμικό διακίνησης, μέσα από ασφαλές κανάλι επικοινωνίας μεταξύ των εξυπηρετητών που μετέχουν, με χρήση αλγορίθμων κρυπτογράφησης και με επαλήθευση ταυτότητας που διασφαλίζεται από ψηφιακά πιστοποιητικά εξυπηρετητών ή ζεύγη κλειδιών, όπως ορίζεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων. Το ασφαλές κανάλι επικοινωνίας υλοποιείται, είτε βάση των πιστοποιητικών εξυπηρετητή με ασφαλές πρωτόκολλο μετάδοσης, είτε μέσα από ιδιωτικό ιδεατό δίκτυο (VPN) με αντίστοιχη ασφάλεια, όπως ορίζεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων. Το λογισμικό διακίνησης υλοποιεί καταγραφές διακίνησης δεδομένων, όπως ορίζεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων.

γ) Πλήρως αυτοματοποιημένη διακίνηση. Το πακέτο δεδομένων που έχει δημιουργηθεί στη φάση τοποθέτησης μεταδίδεται μέσα από ασφαλές κανάλι επικοινωνίας, όπως περιγράφεται στην ενότητα Μέτρα Ασφαλείας Δεδομένων. Το λογισμικό διακίνησης υλοποιεί καταγραφές διακίνησης δεδομένων, όπως περιγράφεται στην υποφάση τοποθέτησης.

2.3 Φάση κατανάλωσης

Η κατανάλωση των δεδομένων από τον οργανισμό αποδέκτη γίνεται με αντίστροφη διαδικασία αυτής της παραγωγής τους, ο οποία διακρίνεται σε υποφάσεις παραλαβής, μετασχηματισμού και αποθήκευσης-κατανάλωσης. Οι διαδικασίες διακρίνονται ανάλογα με τον τρόπο διακίνησης.

α) Χειροκίνητη διακίνηση. Στην υποφάση παραλαβής ο υπεύθυνος παραλαβής αποκρυπτογραφεί τα δεδομένα και ελέγχει την ακεραιότητά τους και την αυθεντικότητα του αποστολέα. Στη συνέχεια φροντίζει για την ασφαλή αρχειοθέτηση της πρωτότυπης μορφής τους, έτσι ώστε να είναι εφεξής δυνατή η αντιπαραβολή τους. Όσο βρίσκονται στην αρχική τους μορφή, τα δεδομένα συνοδεύονται πάντα (σε περίπτωση που είναι αποκομμένη) με την ψηφιακή υπογραφή τους. Ο υπεύθυνος παραλαβής φροντίζει για την ασφαλή

και με απόδοση προσωπικής ευθύνης μεταβίβαση των δεδομένων προς μετασχηματισμό, με τους κανόνες που έχουν περιγραφεί παραπάνω.

Στην υποφάση μετασχηματισμού τα δεδομένα μετασχηματίζονται στη μορφή που απαιτείται για την αποθήκευσή τους στον οργανισμό παραλήπτη και την περαιτέρω κατανάλωσή τους. Οι κανόνες που ακολουθούνται είναι ίδιοι με αυτούς στην υποφάση μετασχηματισμού της παραγωγής τους, με έμφαση στην απόδοση προσωπικής ευθύνης για τη μεταβίβαση.

Στην υποφάση αποθήκευσης-κατανάλωσης τα δεδομένα τοποθετούνται στην κεντρική βάση δεδομένων του οργανισμού αποδέκτη προς κατανάλωση. Ισχύουν οι κανόνες που περιγράφονται στην ενότητα Μέτρα Ασφαλείας Δεδομένων για την φυσική ασφάλεια στον εξοπλισμό, τον έλεγχο πρόσβασης στα δεδομένα και την ασφαλή διακίνησή τους εντός του οργανισμού στου οποίου την κυριότητα περιήλθαν.

β) Μερικώς αυτοματοποιημένη διακίνηση. Στη υποφάση παραλαβής, τα δεδομένα παραλαμβάνονται από τους εξυπηρετητές του λογισμικού διακίνησης του οργανισμού αποδέκτη και τοποθετούνται στην εσωτερική αποθήκη του.

Στην υποφάση μετασχηματισμού, οι υπεύθυνοι διακίνησης του οργανισμού-αποδέκτη εξάγουν τα δεδομένα που διακινήθηκαν από το σύστημα διακίνησης και τα εισάγουν στην ενδιάμεση αποθήκη δεδομένων του οργανισμού επιτελώντας αν χρειαστεί όποιους μετασχηματισμούς απαιτούνται.

Στη υποφάση αποθήκευσης-κατανάλωσης, οι υπεύθυνοι διακίνησης του οργανισμού-αποδέκτη μεταβιβάζουν τα δεδομένα από την ενδιάμεση αποθήκη στην κεντρική αποθήκη προς κατανάλωση. Η φάση αυτή μπορεί να παραληφθεί, αν το ΠΣ του οργανισμού αποδέκτη είναι προγραμματισμένο για την απευθείας πρόσβαση και κατανάλωση των δεδομένων από την ενδιάμεση αποθήκη. Ισχύουν οι ίδιοι κανόνες ασφαλείας και καταγραφών που περιγράφονται στις φάσεις πρόσβασης, μετασχηματισμού και τοποθέτησης των δεδομένων στον οργανισμό-κάτοχο.

γ) Πλήρως αυτοματοποιημένη διακίνηση. Στην υποφάση παραλαβής-μετασχηματισμού, οι εξυπηρετητές που παραλαμβάνουν τα δεδομένα τα αποθηκεύουν στην ενδιάμεση βάση δεδομένων του οργανισμού-αποδέκτη, εκτελώντας ότι μετασχηματισμούς απαιτούνται. Στην υποφάση αποθήκευσης τα δεδομένα μεταβιβάζονται από την ενδιάμεση αποθήκη στην κεντρική αποθήκη. Η φάση αυτή μπορεί να παραληφθεί, αν το ΠΣ του οργανισμού αποδέκτη είναι προγραμματισμένο για την απευθείας πρόσβαση και κατανάλωση των δεδομένων από την ενδιάμεση αποθήκη. Ισχύουν οι ίδιοι κανόνες ασφαλείας και καταγραφών που περιγράφονται στις φάσεις πρόσβασης, μετασχηματισμού και τοποθέτησης των δεδομένων στον οργανισμό-κάτοχο.

3. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Τα τεχνικά και διαδικαστικά μέτρα ασφάλειας που υλοποιούνται από την παρούσα πολιτική προκειμένου να επιτευχθούν οι στόχοι που έχουν τεθεί παραπάνω έχουν ως ακολούθως.

α) Η εμπιστευτικότητα των δεδομένων διαφυλάσσεται σε όλες τις φάσεις της διακίνησής τους.

1) Εντός του οργανισμού-κατόχου και του οργανισμού-αποδέκτη φυλάσσονται σε ασφαλείς διατάξεις βάσεων δεδομένων με κρυπτογράφηση των δεδομένων εν ακινησία (in situ). Ορίζεται η χρήση αλγορίθμου κρυπτογράφησης AES με μήκος κλειδιού 128 bits ή εφάμιλλου. Υλοποιούνται μέτρα φυσικής προστασίας των εξυπηρετητών και των μονάδων επιγραμμικής (on-line) και εφεδρικής (backup) αποθήκευσης με κάρτες εισόδου ή βιομετρικά στοιχεία, καθώς και με αντίστοιχες καταγραφές εισόδου/εξόδου.

2) Κατά τη διακίνηση μεταξύ οργανισμών τα δεδομένα μεταφέρονται μέσα από ασφαλή κανάλια επικοινωνίας που υλοποιούνται είτε με ασφαλή πρωτόκολλα επικοινωνίας βάση αλγορίθμων κρυπτογράφησης δημοσίου κλειδιού, είτε με ιδιωτικά ιδεατά δίκτυα (VPN) ανάλογης ασφάλειας. Κατά τη διακίνηση μεταξύ εξυπηρετητών, ορίζεται αμφίδρομη επαλήθευση ταυτότητας των δύο άκρων βάση, είτε ψηφιακών πιστοποιητικών εξυπηρετητών, είτε ζευγών κλειδιών, με χρήση αλγορίθμων δημοσίου κλειδιού. Εφόσον χρησιμοποιηθούν ψηφιακά πιστοποιητικά εξυπηρετητών, αυτά μετέχουν στην ίδια έμπιστη ιεραρχία πιστοποίησης, είτε έχουν ανταλλαγεί με ασφαλή τρόπο μεταξύ των οργανισμών. Εφόσον χρησιμοποιηθούν ζεύγη κλειδιών, αυτά ανταλλάσσονται με ασφαλή τρόπο μεταξύ των οργανισμών.

3) Όταν τα δεδομένα διακινούνται μέσω τοπικού δικτύου εντός του οργανισμού-κατόχου ή του οργανισμού αποδέκτη, η εμπιστευτικότητά τους διαφυλάσσεται είτε με κρυπτογράφηση, ως ανωτέρω, είτε, αν η κρυπτογράφηση δεν είναι δυνατή, με καταγραφές πρόσβασης και διακίνησης και διακριτά προσωπικά διαπιστευτήρια χρηστών που τα διακινούν. Τα διαπιστευτήρια παράγονται και αποδίδονται στο προσωπικό, βάση καλώς ορισμένης πολιτικής ασφαλείας και τεχνικών μέτρων που επιβάλλουν την εφαρμογή της. Πρέπει να είναι δυνατή η αντιστοίχιση ανάμεσα στα διαπιστευτήρια που χρησιμοποιήθηκαν για τη διακίνηση ενός πακέτου δεδομένων και του ιδίου του πακέτου δεδομένων.

Εφόσον τα δεδομένα διακινηθούν μεταξύ εξυπηρετητών, η εμπιστευτικότητά τους διαφυλάσσεται με καταγραφές πρόσβασης και διακίνησης. Εφόσον τα δεδομένα διακινηθούν μέσω εφαρμογών που χρησιμοποιούν φυσικά πρόσωπα, στις καταγραφές που παράγονται είναι δυνατή η αντιστοίχιση ανάμεσα στα διαπιστευτήρια του χρήστη που χρησιμοποιεί την εφαρμογή και στα διαπιστευτήρια που χρησιμοποιεί η εφαρμογή για την πρόσβαση στη βάση δεδομένων. Οι εφαρμογές που χρησιμοποιούνται είναι είτε ειδι-

κού τύπου, περιλαμβάνοντας έλεγχο ακεραιότητας της εφαρμογής, είτε ασφαλείς ιστοσελίδες με πρωτόκολλο HTTPS.

Σε κάθε περίπτωση είναι επιθυμητό να υλοποιείται πολιτική ασφαλείας δικτύου των οργανισμών, με σύστημα προστασίας από διαρροές δεδομένων, έλεγχο πρόσβασης στις θύρες του δικτύου και κεντρικές καταγραφές συμβάντων και προσβάσεων.

4) Εφόσον στη διακίνηση των δεδομένων μετέχει τρίτος φορέας, ισχύουν γι' αυτόν όλα τα παραπάνω μέτρα για την διαφύλαξη της εμπιστευτικότητας των δεδομένων. Επιπλέον, ο φορέας διακίνησης υπογράφει σύμβαση ποιότητας υπηρεσίας, εμπιστευτικότητας και απόδοσης προσωπικής ευθύνης στα φυσικά πρόσωπα που εμπλέκει, με οικονομικές ρήτρες διαρροής δεδομένων.

β) Η ακεραιότητα των δεδομένων διαφυλάσσεται με χρήση ισχυρών αλγορίθμων κατάτμησης, SHA1 τουλάχιστον (μήκος κατάτμησης 160 bits).

γ) Προσωπική απόδοσης ευθύνης.

Στη χειροκίνηση διακίνηση η προσωπική απόδοση ευθύνης γίνεται κυρίως με χρήση ψηφιακών πιστοποιητικών ταυτότητας (identity digital certificates), τόσο στον οργανισμό που τα κατέχει αρχικά, όσο και στον οργανισμό που τα παραλαμβάνει. Τα δεδομένα διακινούνται εντός και εκτός των οργανισμών υπογεγραμμένα ψηφιακά από τον αποστολέα και κρυπτογραφημένα με το πιστοποιητικό του παραλήπτη, έτσι ώστε να μπορούν να διαβαστούν μόνο από αυτόν.

Χρησιμοποιούνται ψηφιακά πιστοποιητικά ταυτότητας προηγμένης ψηφιακής υπογραφής, τα οποία έχουν παραχθεί από αναγνωρισμένο από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) πάροχο υπηρεσιών πιστοποίησης και είναι αποθηκευμένα σε ασφαλείς διατάξεις αποθήκευσης (usb token ή smartcard). Εάν αυτό δεν είναι δυνατό, χρησιμοποιούνται ομότιμα (peer-to-peer) προσωπικά ψηφιακά πιστοποιητικά τύπου GNU Privacy Guard (GPG), αποθηκευμένα σε προσωπικό υπολογιστή, σύμφωνα και με την πολιτική ασφάλειας προσωπικών σταθμών εργασίας του οργανισμού. Στην περίπτωση χρήσης πιστοποιητικών GPG, πρέπει να υλοποιηθεί ασφαλές πρωτόκολλο ανταλλαγής πιστοποιητικών βασισμένο στη φυσική παρουσία των κατόχων τους, έτσι ώστε να είναι δυνατή η δημιουργία σχέσης εμπιστοσύνης μεταξύ των εμπλεκομένων μερών.

Εάν υπάρχουν παραπάνω του ενός πρόσωπα υπεύθυνα για την αποστολή, παράγονται ισόποσες ψηφιακές υπογραφές, για κάθε ένα από τα αρχεία που απαρτίζουν το πακέτο αποστολής (πχ. για τρία αρχεία και δύο υπεύθυνους αποστολής παράγονται συνολικά έξι ψηφιακές υπογραφές).

Εφόσον είναι δυνατόν, η ψηφιακή υπογραφή ενσωματώνεται στο αρχείο των δεδομένων, διαφορετικά παράγεται αποκομμένη (detached) και συνοδεύει εφεξής το κάθε αρχείο δεδομένων. Η ψηφιακή υπογραφή ενσωματώνει και τον έλεγχο ακεραιότητας που αναφέρθηκε παραπάνω και το μηχανισμό προσωπικής απόδοσης ευθύνης στο φυσικό πρόσωπο υπεύθυνο για την αποστολή. Κάθε

πακέτο δεδομένων συνοδεύεται από το/τα ψηφιακά πιστοποιητικά του/των αποστολέων.

Η επαλήθευση ακεραιότητας των δεδομένων μπορεί να γίνει τόσο από τον αποστολέα, με χρήση του πιστοποιητικού που διαθέτει, όσο και από τον παραλήπτη, με χρήση του πιστοποιητικού του αποστολέα.

Τεχνικά, η ψηφιακή υπογραφή γίνεται με κρυπτογράφηση της κατάτμησης του αρχείου δεδομένων με το ιδιωτικό κλειδί του υπογράφοντος. Η κρυπτογράφηση των δεδομένων γίνεται είτε απευθείας με αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού RSA, είτε μέσω παραγωγής δέσμης συμμετρικών κλειδιών, κρυπτογράφηση της δέσμης με RSA και κρυπτογράφηση των δεδομένων με χρήση της δέσμης με αλγόριθμους συμμετρικής κρυπτογράφησης AES, Blowfish ή Twofish με μήκος κλειδιού τουλάχιστον 128 bits.

Τελικά, εάν τα αρχεία που απαρτίζουν ένα πακέτο αποστολής είναι πολλά, μπορούν σε αυτό το σημείο να ενοποιηθούν σε ένα, με χρήση λογισμικού συμπίεσης (προτείνεται το ανοικτό λογισμικό 7zip).

Κατά την πρόσβαση στα δεδομένα και για την απόδοση προσωπικής ευθύνης, υλοποιούνται μέτρα ελέγχου και καταγραφής της πρόσβασης και μέτρα προστασίας από απώλεια στο δίκτυο και τους σταθμούς εργασίας που χρησιμοποιούνται για την πρόσβαση, όπως περιγράφεται παραπάνω.

Εφόσον οι διαχειριστές των βάσεων δεδομένων και των συστημάτων έχουν πρόσβαση στα δεδομένα, υπάρχει καταγραφή των ενεργειών τους έτσι ώστε να μην είναι δυνατή η αλλοίωση αυτής από αυτούς, πιθανώς με ξεχωριστά επίπεδα διαχείρισης/επιθεώρησης (administration/auditing).

Οι σταθμοί εργασίας και εξυπηρετητές που χρησιμοποιούνται για την πρόσβαση και τη διακίνηση δεδομένων, είτε άμεσα, είτε μέσω εφαρμογής, διαθέτουν όλες τις τρέχουσες ενημερώσεις ασφαλείας λειτουργικού συστήματος και εφαρμογών, ενημερωμένο λογισμικό προστασίας από κακόβουλο λογισμικό, λογισμικό ανίχνευσης διαρροών, πολιτικές ασφαλείας που επιβάλλονται με τεχνικά μέσα από τον οργανισμό, καταγραφές έναρξης συνόδου (logon) και μη επιτρεπόμενων ενεργειών, καθώς και λογισμικό διαχείρισης αφαιρούμενων μέσων.

4. ΕΞΕΙΔΙΚΕΥΣΗ ΠΟΛΙΤΙΚΗΣ

Η Πολιτική αυτή συνοδεύεται από Σχέδιο Υλοποίησης για κάθε συγκεκριμένη σχέση ανταλλαγής δεδομένων μεταξύ δύο οργανισμών, με επακριβή καθορισμό των κατωτέρω τουλάχιστον:

α) της ακριβούς ροής δεδομένων εντός και μεταξύ των οργανισμών που ανταλλάσουν δεδομένα και
β) των αναλυτικών μέτρων που χρησιμοποιούνται για την επίτευξη των στόχων ασφαλείας σε κάθε φάση διακίνησης των δεδομένων.

Τόσο η Πολιτική όσο και το Σχέδιο Υλοποίησης αυτής κοινοποιούνται στη διοίκηση των οργανισμών, όπως και σε όλα τα εμπλεκόμενα στην ανταλλαγή δεδομέ-

νων άτομα. Το Σχέδιο Υλοποίησης αναθεωρείται ανάλογα υπό τις ακόλουθες συνθήκες:

α) Όταν αναθεωρείται η παρούσα Πολιτική.
β) Όταν προκύπτουν αναφορές που μπορεί να καθιστούν ανασφαλή τα πρωτόκολλα που χρησιμοποιούνται ή τεχνολογικές εξελίξεις που παρέχουν μεγαλύτερο επίπεδο ασφάλειας.

γ) Όταν γίνονται αλλαγές στα πληροφοριακά συστήματα των οργανισμών που συμμετέχουν στην ανταλλαγή των στοιχείων.

5. ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΗΣ

Η παρούσα Πολιτική αναθεωρείται ανάλογα με τις ακόλουθες συνθήκες:

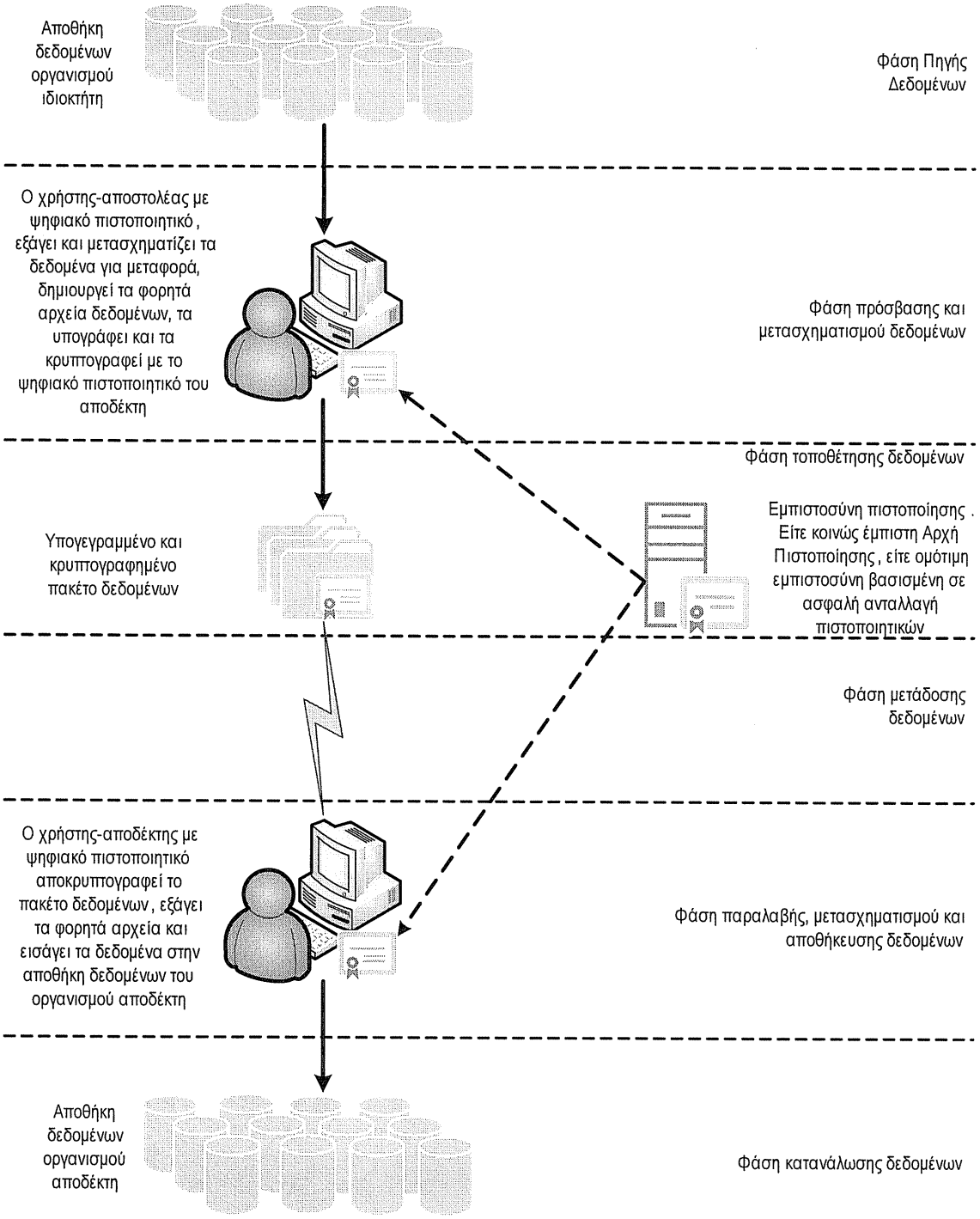
α) Αλλαγές στις επιχειρησιακές ανάγκες των εμπλεκομένων οργανισμών που ανταλλάσσουν δεδομένα.
β) Αλλαγές στη νομοθεσία και το κανονιστικό πλαίσιο που διέπει τη συνεργασία των οργανισμών που μετέχουν και τη διακίνηση ευαίσθητων δεδομένων.
γ) Νεώτερες τεχνολογικές εξελίξεις που μπορεί να καθιστούν ανασφαλή τα πρωτόκολλα που χρησιμοποιούνται ή παρέχουν μεγαλύτερο επίπεδο ασφάλειας.
δ) Παύση της ανταλλαγής δεδομένων μεταξύ των οργανισμών.

Η επικαιροποίηση της παρούσας Πολιτικής και του Σχεδίου Υλοποίησης αυτής γίνεται μετά από αμοιβαία απόφαση των διοικήσεων των εμπλεκομένων οργανισμών και ενέχει:

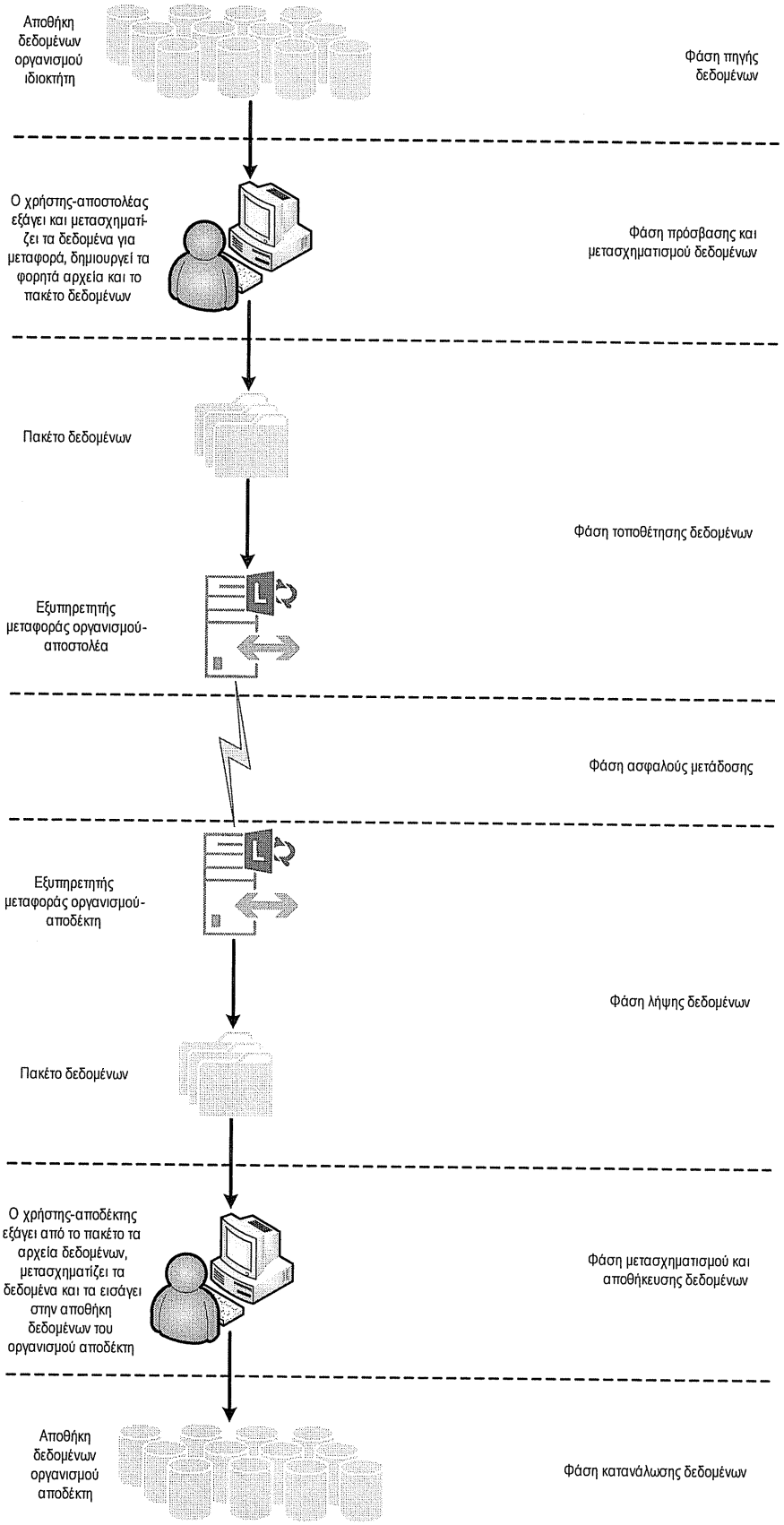
α) Πρόταση αλλαγής στην Πολιτική και το Σχέδιο Υλοποίησης με πρωτοβουλία ενός εκ των εμπλεκομένων οργανισμών.
β) Διαβούλευση με όλους τους εμπλεκόμενους οργανισμούς.
γ) Έκδοση νέας Πολιτικής ή/και Σχεδίου Υλοποίησης αυτής.
δ) Υλοποίηση των αποφασισμένων μέτρων και διαδικασιών εντός των οργανισμών.
ε) Περιοδικούς ελέγχους για την αποτελεσματικότητα, την αποδοτικότητα, τη λειτουργικότητα των διαδικασιών και των μέτρων ασφαλείας που προδιαγράφονται.

ΠΑΡΑΡΤΗΜΑ

Σχήμα 1 – Φάσεις και ενέργειες κατά τη χειροκίνητη διαβίβαση δεδομένων



Σχήμα 2 – Φάσεις και ενέργειες κατά τη μερικώς αυτοματοποιημένη διαβίβαση δεδομένων



Σχήμα 3 – Φάσεις και ενέργειες κατά την πλήρως αυτοματοποιημένη διαβίβαση δεδομένων