



ΔΗΛΩΣΗ GDPR ΣΥΜΜΟΡΦΩΣΗΣ ΛΟΓΙΣΜΙΚΟΥ

ΕΙΣΑΓΩΓΗ

Η ΙΛΥΔΑ μέσω της παρούσας ανακοίνωσης , σας ενημερώνει ότι από τις **25 Μαΐου 2018** τίθεται σε εφαρμογή σε όλα τα κράτη-μέλη της ΕΕ ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων **GDPR (General Data Protection Regulation)**, με τον οποίο οφείλουν να συμμορφωθούν **όλες οι επιχειρήσεις** που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, ανεξαρτήτως κλάδου, οικονομικής δραστηριότητας και μεγέθους.

ΣΥΝΔΡΟΜΗ ΤΗΣ ΙΛΥΔΑ ΣΤΗΝ ΣΥΜΜΟΡΦΩΣΗ ΣΑΣ ΚΑΤΑ GDPR

Η ΙΛΥΔΑ προκειμένου να συμβάλει στην συμμόρφωση σας στις GDPR νομικές υποχρεώσεις σας, συνέταξε την παρούσα δήλωση (οδηγό) που απαριθμεί τις βασικές προφυλάξεις και ενέργειες σας (όσον αφορά τα προσωπικά δεδομένα) που πρέπει να εφαρμόζετε συστηματικά.

Επίσης, η ΙΛΥΔΑ, αξιοποιώντας πλήρως τα σύγχρονα εργαλεία ανάπτυξης λογισμικού, έχει ενσωματώσει στις νέες εκδόσεις των εφαρμογών λογισμικού της, τις αναφερόμενες στην παρούσα δήλωση νέες δυνατότητες και αυτοματισμούς αναφορικά με το GDPR.

Η αναβάθμιση του λογισμικού σας προκειμένου να προσαρμοστεί στις απαιτήσεις GDPR μπορεί να γίνει μέσω των διαθέσιμων εργαλείων Auto Updater που ήδη γνωρίζετε και χρησιμοποιείτε εντός του μηνός Ιουνίου.

1. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ (ΚΑΝΟΝΙΣΜΟΣ)

1.1 ΧΡΗΣΙΜΟΙ ΟΡΙΣΜΟΙ (βάσει του Άρθρου 4 του Κανονισμού):

Για τους σκοπούς του Κανονισμού νοούνται ως :

1. Δεδομένα προσωπικού χαρακτήρα :

Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

2. Επεξεργασία :

Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα



δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή καταστροφή.

3. Περιορισμός της επεξεργασίας :

Η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.

4. Σύστημα αρχειοθέτησης :

Κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε καταναμημένο σε λειτουργική ή γεωγραφική βάση.

5. Υπεύθυνος επεξεργασίας :

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

6. Εκτελών την επεξεργασία :

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

7. Τρίτος :

Οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

8. Συγκατάθεση» του υποκειμένου των δεδομένων :

Κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

9. Παραβίαση δεδομένων προσωπικού χαρακτήρα :

Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

1.2 ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Τα δεδομένα προσωπικού χαρακτήρα αναφέρονται :

- Στα Φυσικά Πρόσωπα
- Στις Ατομικές Επιχειρήσεις
- Στις Μονοπρόσωπες Επιχειρήσεις

1.3 ΠΟΙΑ ΔΕΔΟΜΕΝΑ ΘΕΩΡΟΥΝΤΑΙ “ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ” (ΠΔ)

Είναι τα δεδομένα που μπορούν να χρησιμοποιηθούν για να προσδιοριστεί μονοσήμαντα ένα πρόσωπο ή δεδομένα που είναι σχετικά με ένα άτομο που έχει ήδη αναγνωριστεί.

Ποιο συγκεκριμένα :

1. Στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.)
2. Φυσικά χαρακτηριστικά (εκπαίδευση, εργασία, προϋπηρεσία, εργασιακή συμπεριφορά κλπ.)
3. Οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά)
4. Ενδιαφέροντα, Δραστηριότητες, Συνήθειες
5. IP Address, e-mail, internet cookies
6. GPS location
7. Τα ιατρικά, τα θρησκευτικά, τα πολιτικά, οι ερωτικές προτιμήσεις, η συνδικαλιστική δραστηριότητα, κ.α.

1.4 ΔΙΚΑΙΩΜΑΤΑ ΥΠΟΚΕΙΜΕΝΟΥ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΛΟΙΠΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΣΑΣ

Παρακάτω απαριθμούμε τα χαρακτηριστικά που θα πρέπει να εφαρμοσθούν.

- 1.4.1 Δικαίωμα στη λήθη, [“Forget me”](#)
- 1.4.2 Ενημέρωση τρίτων για διαγραφή, [Notify 3rd parties for erasure](#)
Μετά την διαγραφή δεδομένων από το IT σύστημα είστε επίσης υποχρεωμένοι να ενημερώνετε όλα τα τρίτα μέρη που έχετε προωθήσει τα δεδομένα.
- 1.4.3 Περιορισμός της επεξεργασίας, [Restrict processing](#)
- 1.4.4 Εξαγωγή δεδομένων, [Export data](#)
- 1.4.5 Επιτρέψτε στα υποκείμενα προσωπικών δεδομένων να επεξεργαστούν το προφίλ τους, [Allow users to edit their profile](#)
- 1.4.6 Πλαίσια ελέγχου, [Consent checkboxes](#)
- 1.4.7 Ζητήστε ξανά τη συγκατάθεσή, Re-request consent
- 1.4.8 Βλέπω όλα τα δεδομένα μου, [“See all my data”](#)
- 1.4.9 Ηλικία υποκειμένου, [Age checks](#)
Θα πρέπει να ζητήσετε την ηλικία του χρήστη και αν ο χρήστης είναι παιδί (κάτω από 16), πρέπει να ζητήσετε άδεια γονέα.
- 1.4.10 Ρόλοι (χρήστες)
- 1.4.11 Διατήρηση δεδομένων για περισσότερο από ό, τι είναι απαραίτητο, [Keeping data for no longer than necessary](#)
- 1.4.12 Κρυπτογραφήστε τα δεδομένα σε ηρεμία, Encrypt the data at rest
- 1.4.13 Κρυπτογράφηση αντιγράφων ασφαλείας, Encrypt your backups
- 1.4.14 Εφαρμόστε ψευδονυμοποίηση, Implement pseudonymisation
- 1.4.15 Προστατέψτε την ακεραιότητα των δεδομένων, Protect data integrity
- 1.4.16 Μητρώο GDPR
Πρέπει να περιλαμβάνει το σύνολο των δραστηριοτήτων επεξεργασίας (συνιστούμε να MHN είναι σε αρχείο Excel)
Το άρθρο 30 ([Article 30](#)) λέει ότι θα πρέπει να τηρείτε αρχείο όλων των τύπων δραστηριοτήτων για τις οποίες χρησιμοποιείτε προσωπικά δεδομένα.

1.4.17 Καταχώρηση πρόσβασης στα προσωπικά δεδομένα, Log access to personal data

1.4.18 Καταχώρηση όλων των αποδεκτών API, Register all API consumers

1.5 ΕΝΕΡΓΕΙΕΣ ΣΑΣ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ “ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ”

1. Ορίσετε Data Protection Officer (DPO) (εφαρμόζεται όπου υπάρχουν πάνω από 250 εργαζόμενοι ή όπου γίνεται επεξεργασία δεδομένων σε μεγάλη έκταση).
2. Ορίσετε υπεύθυνο διαχείρισης αρχείων προσωπικών δεδομένων (κάθε φύσης)
3. Αναφέρετε συμβάντα υποκλοπής προσωπικών δεδομένων και εν γένει κακόβουλες ενέργειες αμελλητί και το αργότερο 72 ωρών, στην αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

2. ΠΡΟΣΑΡΜΟΓΕΣ ΛΟΓΙΣΜΙΚΟΥ ΙΛΥΔΑ ΣΥΜΜΟΡΦΩΣΗΣ ΚΑΤΑ GDPR

2.1 ΔΙΚΑΙΩΜΑΤΑ ΠΡΟΣΒΑΣΗΣ ΧΡΗΣΤΩΝ

Αφορούν τις διαδικασίες ορισμού δικαιωμάτων χρηστών και τις αντίστοιχες προσβάσεις των χρηστών στις διαθέσιμες επιλογές του λογισμικού.

2.1.1 Στους ρόλους (χρήστες)

Θα ορίζεται “αν ο χρήστης έχει δικαίωμα επεξεργασίας ΠΔ”

2.1.2 Περιορισμός της επεξεργασίας ([Restrict processing](#))

2.1.3 Encryption των passwords των χρηστών και τα connection strings

2.1.4 Στα grids με στοιχεία προσωπικών δεδομένων

Μπορούν να οριστούν δικαιώματα χρηστών ώστε να αποτρέπεται η εκτύπωση προσωπικών δεδομένων μέσω των grids.

2.1.5 Ορισμός χρόνου ζωής των κωδικών

Μπορεί να οριστεί στο λογισμικό ο χρόνος ζωής του κωδικού, πέραν του οποίου ο κωδικός αδρανοποιείται (δεν έχει ισχύ) και ο χρήστης δεν έχει πρόσβαση στην εφαρμογή.

2.1.6 Βαθμός πολυπλοκότητας κλειδιών

Ρυθμίζεται ο βαθμός πολυπλοκότητας του κλειδιού πρόσβασης.

2.1.7 Ορισμός ομάδων χρηστών

Παρέχεται η δυνατότητα δημιουργίας ομάδων χρηστών με τα ίδια δικαιώματα πρόσβασης.

Ουσιαστικά μέσω των παραπάνω λειτουργιών απαγορεύεται κάθε είδους επεξεργασία (τροποποίηση, διαγραφή, προβολή, εκτύπωση) ευαίσθητων και προσωπικών δεδομένων από μη εξουσιοδοτημένους χρήστες του συστήματος.

2.2 LOG FILES

Κάθε ενέργεια (καταχώρηση, διόρθωση, διαγραφή, εμφάνιση) που σχετίζεται με προσωπικά δεδομένα θα καταγράφεται, έτσι ώστε να προκύπτει ποιος έκανε την συγκεκριμένη ενέργεια και για ποιο σκοπό. Αυτό δεν προκύπτει άμεσα από τις διατάξεις του κανονισμού, αλλά υποδηλώνεται από τις αρχές λογοδοσίας.

2.2.1 Καταγραφή πρόσβασης

Καταγραφή της πρόσβασης (δηλαδή στις ενέργειες : Νέα καταχώρηση, Διόρθωση, Διαγραφή, Αναζήτηση-Εμφάνιση) σε αρχεία που σχετίζονται με προσωπικά δεδομένα.

Σε κάθε ενέργεια (σε αρχείο ΠΔ) θα καταγράφονται τα ακόλουθα :
Χρήστης, Ημερομηνία, Ώρα, Υποσύστημα, Επιλογή λογισμικού, Ενέργεια.

2.2.2 Πληροφορίες από τα log files, με κριτήρια :

- Χρήστης (συγκεκριμένος ή *****)
- Περίοδος (από – έως)
- Ενέργεια (συγκεκριμένη από τις αναφερόμενες στο 2.2.1 ή *)

2.2.3 Διαγραφή log files

Τα στοιχεία αυτά ΔΕΝ πρέπει να φυλάσσονται για υπερβολικά μεγάλο χρονικό διάστημα (π.χ. 6 μήνες) διότι το σύστημα θα γίνει αργό.

Θα υπάρχει διαδικασία διαγραφής των με κριτήριο :

“Διαγραφή log files πριν από την ημερομηνία : x”

Πριν την διαγραφή επιβάλλεται δημιουργία backup.

2.3 ΔΙΚΑΙΩΜΑΤΑ ΥΠΟΚΕΙΜΕΝΩΝ ΠΟΥ ΕΠΕΞΕΡΓΑΖΟΜΑΣΤΕ ΠΔ

2.3.1 Πλαίσια ελέγχου, [Consent checkboxes](#)

"Σύμφωνα με τους όρους και τις προϋποθέσεις" δεν αρκεί πλέον να υποστηρίξουμε ότι το υποκείμενο προσωπικών δεδομένων έχει δώσει τη συγκατάθεσή τους για την επεξεργασία των δεδομένων του.

Πρέπει να επιτρέψτε στα υποκείμενα να αποσύρουν τη συγκατάθεσή τους, Επιβεβαίωση συγκατάθεσης, Re-request consent

Εάν η συγκατάθεση που έδωσαν τα υποκείμενα δεν ήταν σαφής (π.χ. εάν απλώς συμφωνούσαν με τους όρους και τις προϋποθέσεις), θα πρέπει να επιβεβαιώσετε τη συγκατάθεσή τους.

2.3.2 Βλέπω όλα τα δεδομένα μου, [“See all my data”](#)

2.3.3 Διατήρηση δεδομένων μόνο όσο είναι απαραίτητο, [Keeping data for no longer than necessary](#)

Υπάρχει πεδίο στη βάση δεδομένων για την αποθήκευση της προθεσμίας μετά την οποία τα δεδομένα πρέπει να διαγραφούν.

Όλες οι παραπάνω διαδικασίες υποστηρίζονται από την λειτουργικότητα του λογισμικού της ΙΛΥΔΑ.

2.4 ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Η οποιαδήποτε διαδικασία κρυπτογράφησης που θα επιλέξουμε ΠΡΕΠΕΙ να καλύπτει τα ακόλουθα :

2.4.1 Κρυπτογράφηση δεδομένων κατά την αποθήκευσή τους στην βάση δεδομένων.

Αυτή η δυνατότητα ΔΕΝ παρέχεται από τη δωρεάν έκδοση της MS-SQL, παρέχεται ΜΟΝΟ στην Enterprise έκδοση.

Εναλλακτικά προτείνουμε να χρησιμοποιηθούν :

- α) Κρυπτογραφημένοι σκληροί δίσκοι (HDD),
- β) Έλεγχος προσβασιμότητας διαχείρισης του SQL server.

2.4.2 Κρυπτογράφηση αντίγραφων ασφαλείας.

Αφορά την περίπτωση που πρέπει να αποσταλεί το backup προς έλεγχο εκτός επιχείρησης.

Αυτό είναι ευθύνη του διαχειριστή του συστήματος. Προτείνουμε το backup να αποθηκεύεται σε κρυπτογραφημένο σκληρό δίσκο.

2.4.3 Κρυπτογράφηση δεδομένων κατά τη μεταφορά.

Προτείνουμε εφόσον γίνεται με φορητά μέσα αυτά να εξασφαλίζουν κρυπτογράφηση, εφόσον γίνεται με απομακρυσμένη πρόσβαση να χρησιμοποιείτε ασφαλή διασύνδεση (π.χ. μέσω VPN).

2.5 ΣΥΓΚΑΤΑΘΕΣΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΔ

Το λογισμικό της ΙΛΥΔΑ υποστηρίζει διαδικασία λήψης συγκατάθεσης πελάτη για την αποθήκευση και τη χρήση των προσωπικών στοιχείων του.

2.5.1 Tab ΠΔ (GDPR)

Ότι αφορά τις διαδικασίες διαχείρισης προσωπικών δεδομένων καταχωρούνται σε διακριτό **tab** στην καρτέλα συναλλασσόμενου που περιλαμβάνει :

- i. Τα scan-αρισμένα κείμενα :
 - α) της συγκατάθεσης,
 - β) των τροποποιήσεων συγκατάθεσης και
 - γ) της ολικής διαγραφής (Right to be Forgotten).
- ii. Την ημερομηνία της συγκατάθεσης
Αρχικά η ημερομηνία θα είναι κενή “ / / ”
- iii. Το μέσο βάσει του οποίου δόθηκε η συγκατάθεση (scan-αρισμένο έγγραφο, e-mail, sms, υπογραφή σε tablet, ...)
Αν e-mail ή sms τότε πρέπει να καταχωρήσετε χειρόγραφα :
 - Λογαριασμό e-mail ή Κινητό (by default αυτό στο οποίο το στείλαμε)
 - Ημερομηνία
 - Ώρα
- iv. Διάρκεια τήρησης προσωπικών δεδομένων (συγκατάθεση μέχρι την ημερομηνία x), δηλαδή μέχρι ποια ημερομηνία μας δίνεται η συγκατάθεση, για αορίστου λήξης να θεωρούμε την κενή “ / / ” ημερομηνία.
- v. Τον σκοπό που αφορά η συγκατάθεση (ενδεικτικά με multi select επιλογές από τον σχετικό πίνακα παραμέτρων).
- vi. Κατάλογος τρίτων στους οποίους έχουν αποσταλεί ΠΔ του συγκεκριμένου συναλλασσόμενου.
Τα πεδία αυτού του πίνακα είναι : Επωνυμία, Διεύθυνση, Τηλέφωνα, Αρμόδιος, Αιτιολόγηση Αποστολής ΠΔ.

2.5.2 Νέα Πεδία (στους υπάρχοντες πίνακες)

- Στην καρτέλα συναλλασσόμενου προστέθηκε νέο πεδίο “Υποκείμενο σε Δεδομένα προσωπικού χαρακτήρα” με αποδεκτές τιμές Ν/Ο (αρχικά το κενό να εκλαμβάνεται ως Όχι).
- Στην καρτέλα συναλλασσόμενου προστέθηκε νέο πεδίο “Ημερομηνία γέννησης”.

2.5.3 Πληροφοριακές Καταστάσεις

- Κατάλογος συναλλασσόμενων που δεν έχει οριστεί συναίνεση ΠΔ
- Συναιέσεις ΠΔ ανά σκοπό επεξεργασίας
- Λήξεις συναίνεσης προσωπικών δεδομένων

- Εξαγωγή προσωπικών δεδομένων σε οθόνη, εκτυπωτή και αρχεία (αυτή η εξαγωγή καλύπτει τις ανάγκες του νόμου για “Δικαίωμα στη φορητότητα” και “Δικαίωμα στην πρόσβαση”)

Μέσω αυτής της εκτύπωσης θα μπορεί η επιχείρηση να δίνει στον “αιτούντα” αντίγραφο με όλα τα προσωπικά δεδομένα που τον αφορούν.

2.5.4 Βοηθητικές Διαδικασίες

- Συμπλήρωση μαζικά “Υποκείμενο σε Δεδομένα προσωπικού χαρακτήρα”. Διαδικασία που συμπληρώνει μαζικά το πεδίο “Υποκείμενο σε Δεδομένα προσωπικού χαρακτήρα” με την τιμή N. Ουσιαστικά αυτή η διαδικασία θα χρησιμοποιηθεί άπαξ για να ορίσουν οι συναλλασσόμενοι που είναι “Υποκείμενα σε Δεδομένα προσωπικού χαρακτήρα”.
- Διαγραφή προσωπικών δεδομένων Διαδικασία που γίνεται κάθε φορά για ένα μόνο συναλλασσόμενο. Διαγραφή του συνόλου των προσωπικών δεδομένων του κατόπιν αίτησης του για ολική διαγραφή, το λεγόμενο “Δικαίωμα στη λήθη, Right to be Forgotten”.

2.5.5 Παράμετροι

- Πίνακας που θα περιλαμβάνει τα κείμενα διαφορετικών τύπων συγκατάθεσης Ο πίνακας αυτός να μπορεί να κληθεί από διάφορα σημεία του λογισμικού μας για να μπορεί ο χρήστης να εκτυπώνει το έγγραφο συγκατάθεσης που επιθυμεί.
- Πίνακας που θα περιλαμβάνει τους λόγους που δίνεται η συγκατάθεση (π.χ. για λήψη SMS, λήψη e-mail, λήψη Newsletter, Τηλεφωνική Επικοινωνία).

2.5.6 Λοιπές Διαδικασίες

που σχετίζονται με την “συναίνεση τήρησης προσωπικών δεδομένων”

- Όταν ανοίγετε νέα καρτέλα συναλλασσόμενου το πεδίο “Υποκείμενο σε Δεδομένα προσωπικού χαρακτήρα” είναι υποχρεωτικό και πρέπει να συμπληρωθεί με την τιμή N ή O.
- Κατά τις συναλλαγές με τον συναλλασσόμενο όταν δεν έχει δοθεί συγκατάθεση, το λογισμικό κοκκινίζει το όνομα του συναλλασσόμενου και υπενθυμίζει στον χρήστη ότι ΠΡΕΠΕΙ να πάρει την συγκατάθεση.
- Χρήση πολιτικής για τον κωδικό πρόσβασης : Εφαρμογή νέας πολιτικής κωδικού πρόσβασης στην εφαρμογή με αντίστοιχη τροποποίηση της οθόνης Login χρήστη. Σύστημα απόκρυψης, προστασίας και ανανέωσης των στοιχείων εισόδου στις εφαρμογές, σύμφωνα με τα διεθνή πρότυπα.

3. Πληροφορίες

Υπεύθυνος Προστασίας Δεδομένων (DPO - Data Protection Officer) για την ΙΛΥΔΑ ΑΕ και τις εταιρείες του ομίλου, είναι ο κ. Μανόλης Ψυλλάκης με τον οποίο μπορείτε να επικοινωνείτε με τη χρήση ηλεκτρονικού ταχυδρομείου στην ηλεκτρονική διεύθυνση dpo@ilyda.com και στο τηλέφωνο: 210-670.50.00 .

Είμαστε στην διάθεση σας για κάθε σχετική πληροφορία ή διευκρίνιση.

Για την ΙΛΥΔΑ Α.Ε.
Ανυφαντάκης Βασίλης