



**Προστασία Δεδομένων Φυσικών  
Προσώπων - GDPR**

## Περιεχόμενα

Γενική περιγραφή .....	3
Παραμετροποίηση εφαρμογής .....	3
Στοιχεία GDPR .....	3
Ομάδες Χρηστών .....	4
Οντότητες GDPR .....	4
Εταιρείες .....	4
Εργασίες οντοτήτων .....	5
Δεδομένα GDPR .....	5
Λήθη δεδομένων GDPR .....	5
Δικαιώματα Ομάδων χρηστών .....	6
Browsers εφαρμογής .....	6
Αποθηκευμένες όψεις .....	6
Εκτυπώσεις εφαρμογής .....	6
GDPR Audit Log .....	7
Επίπεδα GDPR .....	8
Πολιτικές κωδικών πρόσβασης .....	9
Διαδικασία κλειδώματος/ξεκλειδώματος χρηστών .....	11

Ημερ/νια	Τροποποίηση	Έκδοση
10/05/2018	Αρχικό	3.2.2683.1
21/6/2018	Πολιτικές κωδικών πρόσβασης	3.2.2683.5

## Γενική περιγραφή

Στην εφαρμογή ATLANTIS υπάρχει διαθέσιμη η ενότητα GDPR μέσω της οποίας παρέχεται η δυνατότητα εναρμόνισης των διαδικασιών που εκτελούνται στην εφαρμογή σε σχέση με τα προσωπικά δεδομένα φυσικών προσώπων και τις απαιτήσεις του σχετικού Γενικού Ευρωπαϊκού κανονισμού προστασίας δεδομένων. Στην έννοια του «**φυσικού προσώπου**» στην εφαρμογή Atlantis περιλαμβάνονται οι Πελάτες, οι Πελάτες C.R.M., οι Επαφές αυτών, οι Προμηθευτές (εφόσον είναι φυσικά πρόσωπα), οι Πωλητές, οι Ειδικοί λογαριασμοί (εφόσον είναι φυσικά πρόσωπα) καθώς και το προσωπικό της επιχείρησης (δηλ. Υπάλληλοι και Χρήστες της εφαρμογής).

Ως «**Δεδομένα φυσικών προσώπων**» ορίζονται οι πληροφορίες εκείνες μέσω των οποίων μπορεί να ταυτοποιηθεί ένα φυσικό πρόσωπο (π.χ. Α.Φ.Μ., Α.Μ.Κ.Α., όνομα, επώνυμο,..., κ.λ.π.) και η επιχείρηση είναι υπεύθυνη για την προστασία τους.

## Παραμετροποίηση εφαρμογής

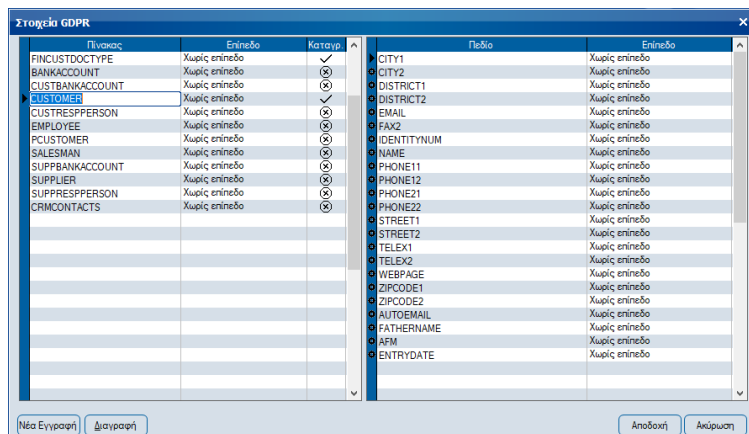
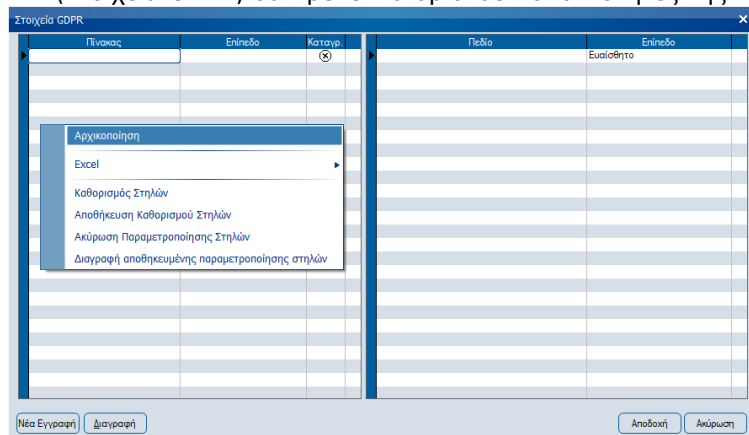
Για την ενεργοποίηση της προστασίας προσωπικών δεδομένων φυσικών προσώπων στην εφαρμογή θα πρέπει να ακολουθηθούν κατά σειρά τα παρακάτω βήματα:

### Στοιχεία GDPR

Από το μενού Οργάνωση\Βοηθητικές εργασίες\GDPR\Στοιχεία GDPR, θα πρέπει να οριστούν οι οντότητες της εφαρμογής για τις οποίες θα εφαρμοστεί η προστασία προβολής δεδομένων. Τα στοιχεία των οντοτήτων της εφαρμογής (π.χ. Πελάτες, Προμηθευτές, ..., κ.λ.π.) στα οποία μπορεί να καθοριστεί έλεγχος GDPR είναι οι πίνακες ή/και τα πεδία πινάκων των οντοτήτων αυτών.

Παρέχεται η δυνατότητα αρχικοποίησης των στοιχείων των οντοτήτων της εφαρμογής με δεξί κλικ στο αριστερό grid της οθόνης στοιχείων GDPR. Κατά τη διαδικασία αυτή προστίθενται αυτόματα τα στοιχεία πινάκων και πεδίων από τις συγκεκριμένες οντότητες της εφαρμογής με GDPR περιεχόμενο.

Στο χρήστη παρέχεται η δυνατότητα της τροποποίησης / προσθήκης των αρχικοποιημένων στοιχείων.

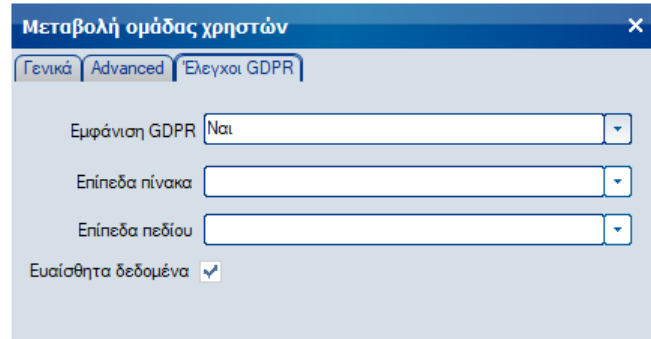


## Ομάδες Χρηστών

Από το menu Οργάνωση\Γενικές παράμετροι\Χρήστες\Ομάδες χρηστών, στη σελίδα «Έλεγχος GDPR» θα πρέπει να καθοριστεί η τιμή του πεδίου «Εμφάνιση GDPR» για κάθε ομάδα χρηστών ώστε να καθοριστεί η δυνατότητα πρόσβασης ή όχι των χρηστών της ομάδας στα δεδομένα τα οποία έχουν χαρακτηριστεί ως GDPR. Η αρχική παραμετροποίηση της συγκεκριμένης σελίδας επιτρέπει τη πρόσβαση στα στοιχεία GDPR. Προσοχή, μετά από οποιαδήποτε αλλαγή στη παραμετροποίηση της σελίδας «Έλεγχος GDPR» στις Ομάδες χρηστών απαιτείται επανασύνδεση (Relogin) των χρηστών της Ομάδας για την ενεργοποίηση των αλλαγών.

Σχετικά με τη χρήση των πεδίων «Επίπεδα πίνακα» και «Επίπεδα πεδίου» γίνεται αναφορά σε επόμενη παράγραφο του κειμένου.

Το πεδίο «Ευαίσθητα δεδομένα» καθορίζει κατά πόσο οι χρήστες της Ομάδας θα έχουν πρόσβαση σε πληροφορίες που έχουν χαρακτηριστεί ως «Ευαίσθητες» σε επίπεδο πεδίου στα «Στοιχεία GDPR».

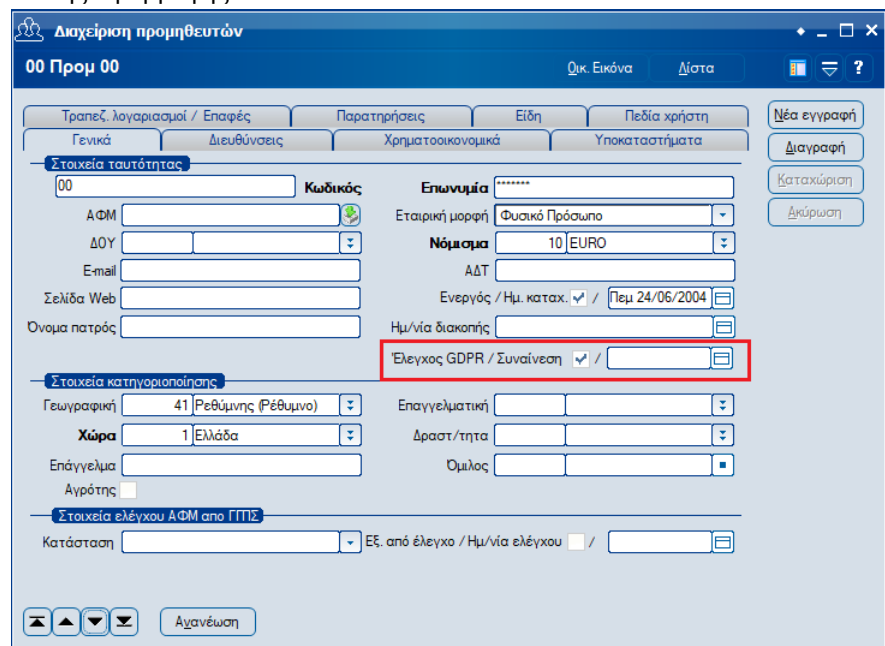


## Οντότητες GDPR

Στις καρτέλες των παρακάτω οντοτήτων της εφαρμογής:

- Πελάτες
- Πελάτες CRM
- Προμηθευτές
- Ειδικοί Λογαριασμοί

στις οποίες ορίστηκαν «Στοιχεία GDPR», θα πρέπει στη σελίδα «Γενικά στοιχεία» να επιλεγεί το πεδίο «Έλεγχος GDPR» ώστε να ενεργοποιηθεί ο έλεγχος για τη συγκεκριμένη εγγραφή. Στο ίδιο σημείο της οθόνης στο πεδίο «Συναίνεση», εφόσον υπάρχει διαθέσιμη η σχετική πληροφορία, μπορεί να καταχωρηθεί η ημερομηνία λήψης της συναίνεσης της οντότητας για τη διατήρηση των GDPR πληροφοριών που την αφορούν.



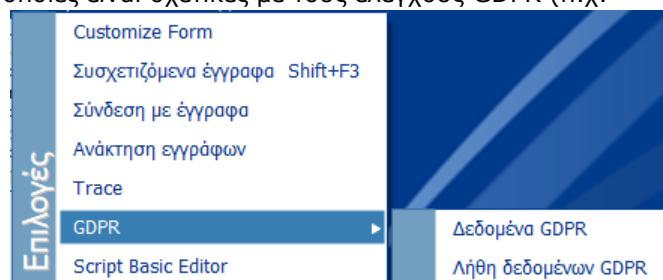
## Εταιρείες

Εφόσον έχουν ολοκληρωθεί -κατ' ελάχιστο- τα παραπάνω βήματα, μπορεί να ενεργοποιηθεί ο γενικός διακόπτης λειτουργίας των ελέγχων GDPR σε συγκεκριμένες εταιρείες της εφαρμογής. Αυτό γίνεται από το

menu Οργάνωση \Γενικές παράμετροι \Εταιρείες, όπου στη σελίδα «Παράμετροι» θα πρέπει να επιλεγεί το πεδίο «Ενεργοποίηση ελέγχων GDPR».

## Εργασίες οντοτήτων

Στις «Εργασίες» των οντοτήτων της εφαρμογής οι οποίες είναι σχετικές με τους ελέγχους GDPR (π.χ. Πελάτες, Προμηθευτές, ..., κ.λ.π.), έχει προστεθεί η επιλογή GDPR με δύο (2) διαθέσιμες εργασίες:



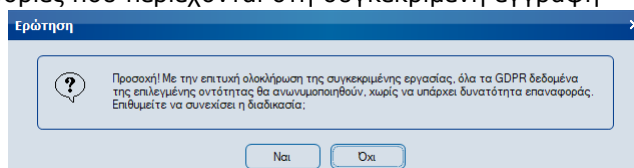
## Δεδομένα GDPR

Με την επιλογή αυτή εμφανίζεται η λίστα των GDPR πληροφοριών της συγκεκριμένης εγγραφής της οντότητας με τις αντίστοιχες τιμές τους. Η λίστα αυτή μπορεί να εκτυπωθεί, αποθηκευτεί σε αρχείο ή/και να αποσταλεί με email.

## Λήθη δεδομένων GDPR

Με την επιλογή αυτή ανωνυμοποιούνται οι GDPR πληροφορίες που περιέχονται στη συγκεκριμένη εγγραφή της οντότητας.

**Προσοχή !!!** όπως εμφανίζεται και στο σχετικό μήνυμα της εφαρμογής, η εργασία αυτή έχει μόνιμο αποτέλεσμα και δεν μπορεί να αντιστραφεί. Για το λόγο αυτό πριν την εκτέλεσή της θα πρέπει ο χρήστης να έχει προβεί σε όλους τους απαραίτητους ελέγχους στα



καταχωρημένα δεδομένα στην εφαρμογή (π.χ. συναλλαγές, ..., κ.λ.π.) ώστε να εξασφαλίσει ότι η ανωνυμοποίηση για τη συγκεκριμένη εγγραφή της οντότητας είναι σύννομη.

## Δικαιώματα Ομάδων χρηστών

Η ενότητα «GDPR» στο menu Οργάνωση λειτουργίας της εφαρμογής, αλλά και οι εργασίες «Δεδομένα GDPR» και «Λήθη δεδομένων GDPR» σε όλες τις σχετικές οντότητες της εφαρμογής (Πελάτες, Προμηθευτές, ..., κ.λ.π.), καλύπτονται από αντίστοιχα δικαιώματα ομάδων χρηστών. Μέσω των δικαιωμάτων αυτών παρέχεται πρόσβαση στις συγκεκριμένες λειτουργίες μόνο στους εξουσιοδοτημένους χρήστες της εφαρμογής.

## Browsers εφαρμογής

Έχει ληφθεί μέριμνα ώστε οι πληροφορίες που έχουν χαρακτηριστεί GDPR στα «Στοιχεία GDPR» να εμφανίζονται κρυπτογραφημένες και στους αντίστοιχους νέους browsers της εφαρμογής. Επιπλέον για τις custom στήλες των browser έχει δοθεί η δυνατότητα χαρακτηρισμού τους από το χρήστη ως «GDPR» πληροφορία.

### Αποθηκευμένες όψεις

Σε περίπτωση που στο σύστημα υπάρχουν αποθηκευμένες όψεις υπάρχει η πιθανότητα να μην εμφανίζεται σωστά στη μπάρα του browser η σύντομη περιγραφή της εγγραφής στην οποία βρίσκεται ο κέρσορας. Αυτό συμβαίνει διότι πιθανότατα δεν έχει οριστεί καθόλου ή δεν έχει οριστεί το σωστό «Πεδίο caption» στη παραμετροποίηση των στηλών της όψης. Επίσης για τη στήλη η οποία θα οριστεί ως «Πεδίο caption», θα πρέπει να δοθεί και κατάλληλη τιμή στο πεδίο «Επίπεδο GDPR» σύμφωνα με την πολιτική προστασίας δεδομένων η οποία έχει υλοποιηθεί για τη συγκεκριμένη πληροφορία.

## Εκτυπώσεις εφαρμογής

Έχει ληφθεί μέριμνα ώστε οι πληροφορίες οντοτήτων οι οποίες έχουν χαρακτηριστεί GDPR στα «Στοιχεία GDPR» να εμφανίζονται κρυπτογραφημένες και στις εκτυπώσεις των αντίστοιχων ενοτήτων της εφαρμογής στις οποίες εμφανίζονται.

Επιπλέον για τυχόν custom στήλες στις εκτυπώσεις αυτές, έχει δοθεί η δυνατότητα χαρακτηρισμού τους από το χρήστη ως «GDPR» πληροφορία μέσω του πεδίου «Επίπεδο GDPR». Η ίδια λειτουργικότητα ισχύει και για τα υπόλοιπα είδη εκτυπώσεων της εφαρμογής (Basic reports, Advanced reports, ...).

Εκτυπώσεις πελατών

Καρτέλα

Παρ 04/05/18

Α/Α Κωδικός Επωνυμία

1 6888

Α/Α	Ημερομηνία	Παραστατικό	Κ.Κ.	Περιγραφή κίνησης	Απολογία	Χρέωση
Από μεταφορά						
1	23/6/2004	007ΔΑ0000770	1001	ΤΙΜΟΛΟΓΙΟ ΠΩΛΗΣΗΣ	ΤΙΜΟΛΟΓΙΟ ΠΩΛΗΣΗΣ	885,00
2	23/6/2004	00ΑΜΑ0000872	2001	ΕΙΣΠΡΑΞΗ ΜΕΤΡΗΤΩΝ / ΠΑΡΑΛΑΒΗ ΑΞΙΟΓΡΑΦΩΝ	ΕΙΣΠΡΑΞΗ ΜΕΤΡΗΤΩΝ / ΠΑΡΑΛΑΒΗ ΑΞΙΟΓΡΑΦΩΝ	0,00
3	8/3/2011	901000000002	9001	ΠΑΡΑΓΓΕΛΙΑ ΑΠΟ ΠΕΛΑΤΗ	amaki aspro kai paxy	0,00
Σύνολο						
2	4521					885,00

Α/Α Ημερομηνία Παραστατικό Κ.Κ. Περιγραφή κίνησης Απολογία Χρέωση

1 Από μεταφορά

1 13/4/2011 ΤΙΜ000000008

2 9/5/2011 Α-ΚΑΤ0000046

3 19/9/2011 9010000000003

4 5/10/2012 ΠΥΠ000000037

1 ΓΕΝΙΚΗ ΧΡΕΩΣΗ

2105 ΠΛΗΡΩΜΗ ΠΕΛΑΤΗ ΑΠΟ ΤΡΑΠΕΖΑ

9001 ΠΑΡΑΓΓΕΛΙΑ ΑΠΟ ΠΕΛΑΤΗ

4 ΤΙΜΟΛΟΓΙΟ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ

amaki aspro kai paxy

ΠΛΗΡΩΜΗ ΠΕΛΑΤΗ ΑΠΟ ΤΡΑΠΕΖΑ

amaki aspro kai & paxy

ΤΙΜΟΛΟΓΙΟ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ

200,00

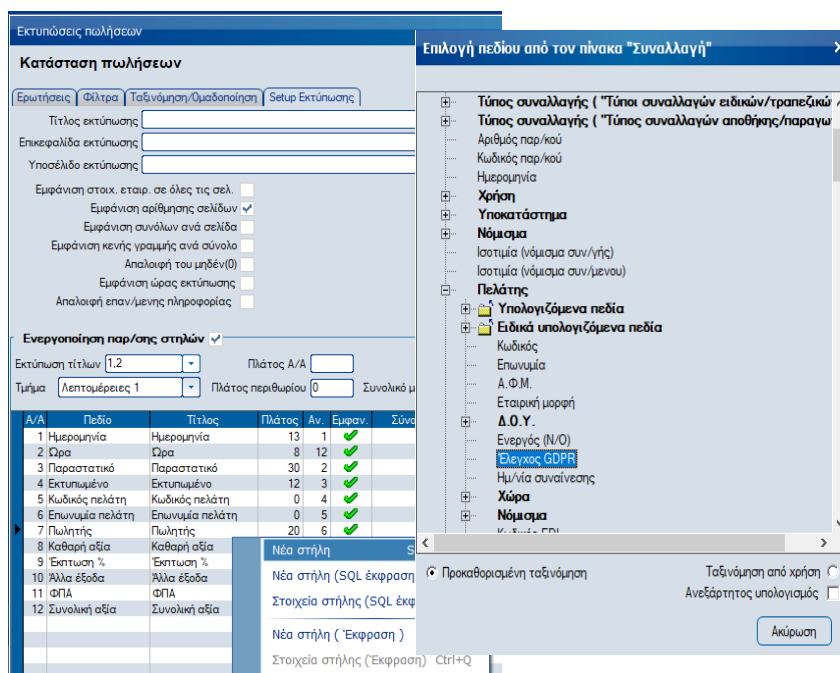
0,00

0,00

2,15

Επιπρόσθετα αναφέρουμε ότι στην περίπτωση κατά την οποία η GDPR οντότητα (Πελάτης, Προμηθευτής, ..., κ.λ.π.) ΔΕΝ είναι η κύρια οντότητα της εκτύπωσης τότε για να εμφανιστούν ορθά τα στοιχεία GDPR τα οποία υπάρχουν ήδη στην εκτύπωση και αφορούν τη μη κύρια οντότητα θα πρέπει να προστεθεί στην εκτύπωση ως «**Νέα στήλη**» το πεδίο «**Έλεγχος GDPR**» από την σχετική ενότητα (Πελάτης, Προμηθευτής, ..., κ.λ.π.) του λεξικού δεδομένων της εφαρμογής.

Στο παράδειγμα λαμβάνεται η εκτύπωση «Κατάσταση πωλήσεων» στην οποία εμφανίζεται το στοιχείο «Επωνυμία πελάτη» από την GDPR οντότητα «Πελάτης». Οπότε για τη ορθή εμφάνιση των αποτελεσμάτων πρέπει να γίνει προσθήκη της στήλης «Έλεγχος GDPR» και στη συνέχεια να αποθηκευτεί η εκτύπωση ώστε να λαμβάνεται από τους επιλεγμένους χρήστες οι οποίοι παράλληλα πρέπει να εξασφαλιστεί μέσω δικαιωμάτων ομάδων χρηστών ότι ΔΕΝ θα έχουν πρόσβαση στην default εκτύπωση της εφαρμογής. Η νέα στήλη που προστέθηκε δεν είναι υποχρεωτικό να εμφανίζεται στα αποτελέσματα της εκτύπωσης. Επιπλέον πεδία -από τις μη κύριες οντότητες- τα οποία προστίθενται από το χρήστη στις εκτυπώσεις θα πρέπει οπωσδήποτε να χαρακτηρίζονται βάσει του πεδίου «Επίπεδο GDPR» στο setup της εκτύπωσης ώστε να εμφανιστούν ορθά.

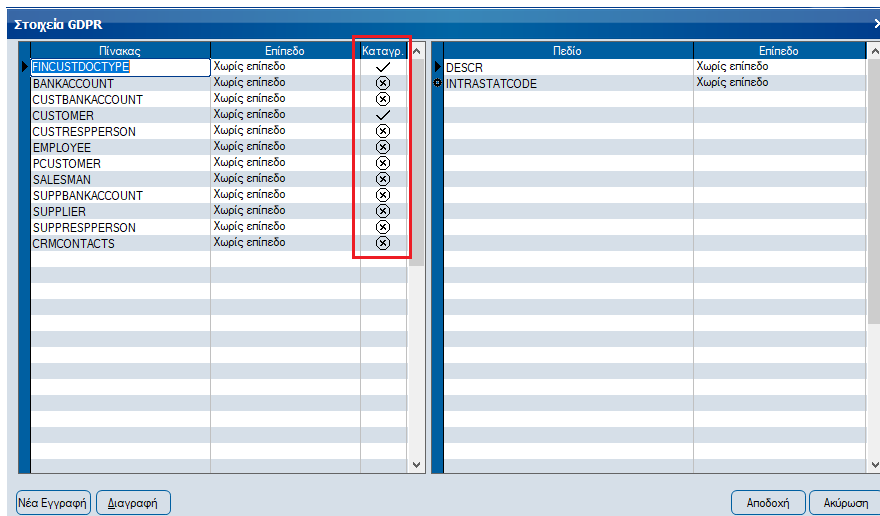


## GDPR Audit Log

Μέσω του αντίστοιχου menu item του κόμβου GDPR στην ενότητα «Βοηθητικές εργασίες» της εφαρμογής παρέχεται η δυνατότητα προβολής των τροποποιήσεων (προσθήκες, ενημερώσεις, διαγραφές) που έχουν επιφέρει οι χρήστες της εφαρμογής στα δεδομένα που έχουν χαρακτηριστεί ως GDPR.

GDPR Audit Log						
Από Ημερομηνία		01/05/2018	Έως Ημερομηνία		04/05/2018	Εμφάνιση
Ημ/νία ενέργειας	Ενέργεια	Πίνακας	Πρωτεύον κλειδί	Τιμή πρωτ. κλειδιού	Χρήστης	
4/5/2018 15:04	Μεταβολή	CUSTOMER	ID	642	unisoft	
Πεδίο	Παλιά τιμή	Νέα τιμή				
NAME	ΤΕΣΤ 1999-2001	WCYKNACGEEIYQI				

Η ενεργοποίηση στην εφαρμογή της διαδικασίας καταγραφής (Audit Log) των τροποποιήσεων στα GDPR δεδομένα υλοποιείται ανά οντότητα μέσω της ενότητας «Στοιχεία GDPR» με την επιλογή του πεδίου «Καταγραφή».

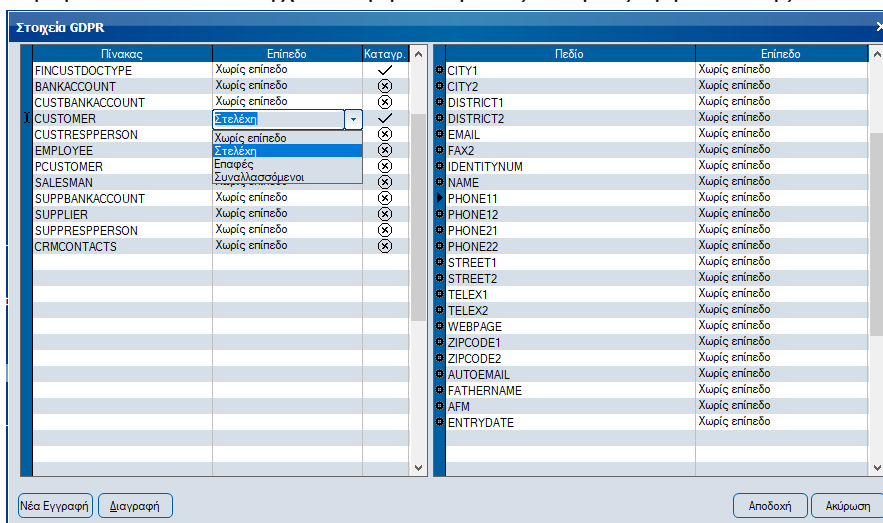


## Επίπεδα GDPR

Στην ενότητα «Στοιχεία GDPR» περιλαμβάνεται και η λειτουργικότητα «Επίπεδα» ελέγχων, μέσω των οποίων δίνεται η δυνατότητα να διαφοροποιηθεί η πρόσβαση των ομάδων χρηστών στα χαρακτηρισμένα ως GDPR δεδομένα της εφαρμογής.

Υποστηρίζεται ελεύθερη παραμετροποίηση «επιπέδων» ελέγχων σύμφωνα με τις ανάγκες οργανωτικής διάρθρωσης των ομάδων χρηστών κάθε επιχείρησης. Τα επίπεδα ελέγχων μπορούν να ενεργοποιηθούν τόσο για τους πίνακες οντοτήτων της εφαρμογής όσο και για τα πεδία των πινάκων αυτών.

Ο καθορισμός επιπέδων «Πεδίων» αποτελεί ανεξάρτητη λειτουργικότητα σε σχέση με τα επίπεδα «Πινάκων». Δηλαδή για παράδειγμα, υποστηρίζεται παραμετροποίηση οντοτήτων με καθορισμό μόνο επιπέδων πεδίων και όχι επιπέδων πινάκων και το αντίστροφο. Επίσης υποστηρίζεται διαφοροποίηση παραμετροποίησης επιπέδων στην ίδια οντότητα μεταξύ πινάκων και πεδίων.



Μετά από την ενεργοποίηση της λειτουργίας «Επίπεδα GDPR» στην εφαρμογή στους πίνακες ή/και στα πεδία θα πρέπει στις ομάδες χρηστών να καθοριστούν τα επιτρεπτά επίπεδα πίνακα ή/και πεδίου.



Προσοχή, τα «Επίπεδα» ενεργοποιούνται μόνο εφόσον στη παραμετροποίηση του χρήστη έχει επιλεγεί η τιμή «Ναι» στο πεδίο «Εμφάνιση GDPR».

Μεταβολή ομάδας χρηστών

Γενικά Advanced Έλεγχος GDPR

Εμφάνιση GDPR

Επίπεδα πίνακα

Επίπεδα πεδίου

Επιλεγμένες εγγραφές

Ευαίσθητα δεδομένα

2 - Στελέχη  
4 - Συναλλασσόμενοι

Αποδοχή Ακύρωση

## Πολιτικές κωδικών πρόσβασης

Με την ενεργοποίηση των ελέγχων GDPR στην εφαρμογή είναι δυνατή η ταυτόχρονη αναβάθμιση

λειτουργικότητας των ελέγχων της πρόσβασης των χρηστών σε αυτή. Από το μενού της εφαρμογής Οργάνωση λειτουργίας Γενικές παράμετροι \ Χρήστες \ Πολιτικές κωδικών πρόσβασης, παρέχεται η δυνατότητα δημιουργίας πολιτικών κωδικών πρόσβασης.

Μπορεί να καθοριστεί πληθώρα στοιχείων ελέγχου κωδικών πρόσβασης των χρηστών όπως:

- η διάρκεια ισχύος των κωδικών
- η επιτρεπόμενη συχνότητα αλλαγής
- η χρήση επαναλαμβανόμενων κωδικών
- το πλήθος επιτρεπτών προσπαθειών εισόδου στην εφαρμογή
- τα ελάχιστο πλήθος χαρακτήρων των κωδικών
- τους απαιτητούς συνδυασμούς ομάδων χαρακτήρων στους κωδικούς πρόσβασης

Μεταβολή Πολιτικών κωδικών πρόσβασης

Περιγραφή:

Οι κωδικοί πρόσβασης πρέπει να αλλάζουν τουλάχιστον κάθε  ημέρες, αλλά να μην αλλάζουν πριν την παρέλευση  ημερών από την τελευταία αλλαγή τους.

Απαγορεύεται η επανάληψη των τελευταίων  κωδικών πρόσβασης που χρησιμοποιήθηκαν.

Επιτρέπονται έως  αποτυχημένες προσπάθειες πληκτρολόγησης του σωστού κωδικού πρόσβασης.

Ένας κωδικός πρόσβασης για να είναι αποδεκτός από το σύστημα θα πρέπει:

- Να έχει μήκος τουλάχιστον  χαρακτήρων.
- Να περιλαμβάνει τουλάχιστον  από τις παρακάτω τέσσερις ομάδες χαρακτήρων:
  - Κεφαλαίους χαρακτήρες της λατινικής αλφαβήτου (Α έως Ζ)
  - Πεζούς χαρακτήρες της λατινικής αλφαβήτου (α έως z)
  - Αριθμούς (0 έως 9)
  - Ειδικούς χαρακτήρες (π.χ. !, \$, #, κλπ)

Αποδοχή Ακύρωση

Η σύνδεση συγκεκριμένης πολιτικής σε κάθε ομάδα χρηστών, υλοποιείται από το menu Οργάνωση λειτουργίας Γενικές παράμετροι\ Χρήστες\ Ομάδες χρηστών, όπου στη σελίδα «Γενικά» στο πεδίο «Πολιτική κωδικών πρόσβασης» επιλέγεται η επιθυμητή πολιτική.

Μεταβολή ομάδας χρηστών

Γενικά Advanced Έλεγχος GDPR

Κωδικός 3

Περιγραφή Πωλητές

**Κωδικός πρόσβασης**

Πολιτική κωδικών πρόσβασης Πολιτική πρόσβασης χρηστών επιπέδου

Αλλαγή κάθε (ημέρες)

Προειδοποίηση (ημέρες)

Μήκος μεγαλύτερο από

Περιέχει αριθμούς και χαρακτήρες

Δικαιώματα σειρών

Αποδοχή Ακύρωση

Εναλλακτικά της επιλογής πολιτικής ελέγχου πρόσβασης υπάρχει η δυνατότητα καθορισμού ειδικών παραμέτρων ελέγχου κωδικών πρόσβασης για την συγκεκριμένη ομάδα χρηστών, μέσω των υπολοίπων πεδίων της υποενότητας «Κωδικός πρόσβασης» της σελίδας «Γενικά». Τα συγκεκριμένα πεδία ενεργοποιούνται εφόσον ΔΕΝ υπάρχει επιλεγμένη πολιτική κωδικών πρόσβασης στην ομάδα χρηστών.

Μεταβολή ομάδας χρηστών

Γενικά Advanced Έλεγχος GDPR

Κωδικός 3

Περιγραφή Πωλητές

**Κωδικός πρόσβασης**

Πολιτική κωδικών πρόσβασης

Αλλαγή κάθε (ημέρες)

Προειδοποίηση (ημέρες)

Μήκος μεγαλύτερο από

Περιέχει αριθμούς και χαρακτήρες

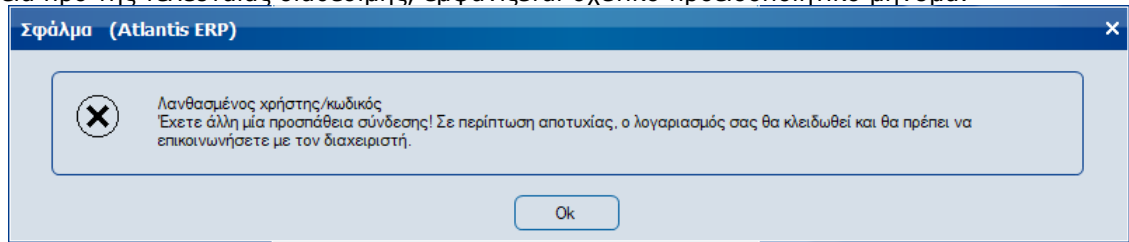
Δικαιώματα σειρών

Αποδοχή Ακύρωση

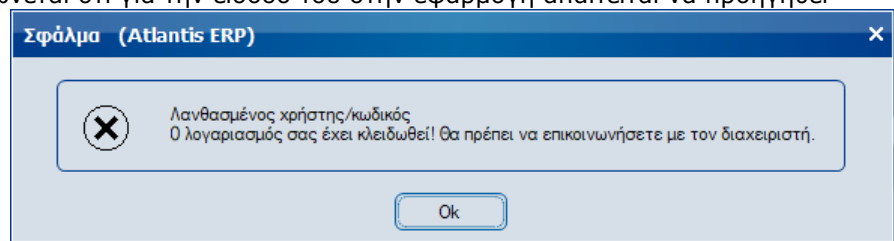
## Διαδικασία κλειδώματος/ξεκλειδώματος χρηστών

Σύμφωνα με τον αριθμό αποτυχημένων προσπαθειών εισόδου, στην ισχύουσα για το χρήστη πολιτική πρόσβασης στην εφαρμογή, ξεκινά αυτόματα η διαδικασία του αποκλεισμού πρόσβασης του χρήστη.

Μία (1) προσπάθεια προ της τελευταίας διαθέσιμης, εμφανίζεται σχετικό προειδοποιητικό μήνυμα.



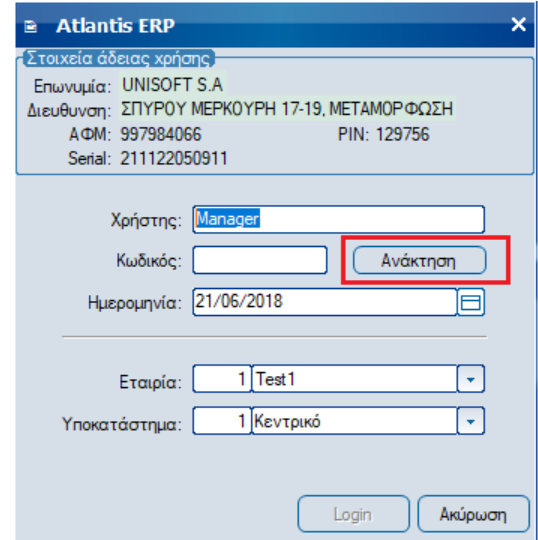
Στην περίπτωση που υπάρξει νέα αποτυχημένη προσπάθεια εισόδου, ο χρήστης κλειδώνεται και εμφανίζεται σχετικό μήνυμα με το οποίο ενημερώνεται ότι για την είσοδό του στην εφαρμογή απαιτείται να προηγηθεί επικοινωνία με το διαχειριστή.



Η εφαρμογή παρέχει τη δυνατότητα αυτοματοποιημένης ενημέρωσης του διαχειριστή καθώς και ανάκτησης και αποστολής του κωδικού ασφαλείας (password) στο χρήστη αρκεί να πληρούνται οι παρακάτω προϋποθέσεις:

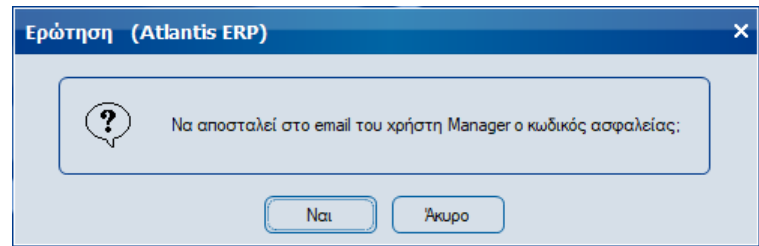
1. Να υπάρχει καταχωρημένη email διεύθυνση στα στοιχεία τουλάχιστον ενός χρήστη ο οποίος έχει χαρακτηριστεί ως supervisor.
2. Να υπάρχει καταχωρημένη email διεύθυνση στα στοιχεία του χρήστη ο οποίος έχει κλειδωθεί.
3. Να υπάρχουν καταχωρημένα πλήρη και λειτουργικά «Στοιχεία Ηλεκτρονικού Ταχυδρομείου» και «Email εταιρείας» στη σελίδα «Στοιχεία Επικοινωνίας» στην καρτέλα της Εταιρείας στην εφαρμογή.

Εφόσον πληρούνται οι προϋποθέσεις, μετά το παραπάνω μήνυμα κλειδώματος του χρήστη, εμφανίζεται η login οθόνη της εφαρμογής στην οποία έχει ενεργοποιηθεί το πλήκτρο «Ανάκτηση».

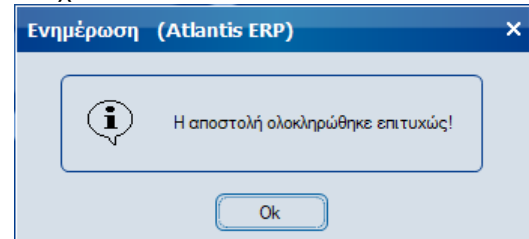


Με την επιλογή του πλήκτρου, εμφανίζεται ερώτημα αποστολής του κωδικού ασφαλείας στο email του χρήστη.

Εφόσον επιλεγεί «Ναι» τότε η επιλογή αποστέλλει δύο (2) μηνύματα. Το πρώτο στην email διεύθυνση χρήστη, το οποίο περιέχει το κωδικό ασφαλείας (password). Το δεύτερο στο/στους διαχειριστή/ες του συστήματος, ώστε να ενημερωθούν για τον αποκλεισμό εισόδου του συγκεκριμένου χρήστη στην εφαρμογή.



Μετά την επιτυχή αποστολή των μηνυμάτων ο χρήστης ενημερώνεται σχετικά.



Τέλος ένας εκ των διαχειριστών της εφαρμογής, ο οποίος ενημερώθηκε μέσω email για τον αποκλεισμό πρόσβασης συγκεκριμένου χρήστη, θα πρέπει να προχωρήσει σε επανενεργοποίηση των προσπαθειών πρόσβασης για το χρήστη αυτό. Η διαδικασία υλοποιείται από το σχετικό πλήκτρο το οποίο έχει ενεργοποιηθεί από την εφαρμογή χρήστη.

Μετά την ενέργεια αυτή είναι δυνατή η επανέναρξη προσπαθειών εισόδου του αποκλεισμένου χρήστη στην εφαρμογή.

