SMILE SECURITY MANUAL

Created 2/12/18
Redrafted 20/3/19

Η Invent It Πληροφορική τηρεί κατά γράμμα τις αυστηρότερες προδιαγραφές του νομικού πλαισίου GDPR πλέον του βαθμού **πιστοποίησης,** συνεργαζόμενη με την εταιρεία εκπαίδευσης και παροχής πιστοποιητικών Master.

Κάθε της συνεργασία συνοδεύεται από τα αυστηρότερα NDAs (Non Disclosure Agreements) τόσο σε σχέση με τον πελάτη όσο και με τον υπάλληλο ή εξωτερικό συνεργάτη. Ένα τυπικό δείγμα μπορείτε να δείτε εδώ :

Επίσης, κάθε νέο στέλεχός μας που με τον ένα ή τον άλλο τρόπο πρόκειται να συνεργαστεί με πελάτη μας, ευαίσθητα δεδομένα του οποίου πιθανώς να επεξεργαστούμε, συστήνεται και εγκρίνεται από τον ίδιο τον πελάτη.

Τέλος, όλες οι εφαρμογές της στηρίζονται στην ασφαλέστερη online βάση δεδομένων, το Azure, trademark της Microsoft της μεγαλύτερης εταιρείας παροχής λογισμικού στον πλανήτη. Το Azure το εμπιστεύονται οι μεγαλύτερες εταιρείες της Γης που διαχειρίζονται καθημερινά δισεκατομμύρια ευαίσθητων δεδομένων, από τον τομέα της Δημοσιογραφίας, της Έννομης Τάξης αλλά και της Ιατρικής. Με τεράστια διαφορά κόστους από τα υπόλοιπα, καθώς σε τέτοια θέματα είμαστε αδιαπραγμάτευτοι.

Smile, αρχιτεκτονική ασφάλειας, πρώτο επίπεδο

Το Smile βασίζεται στην εν λόγω πλατφόρμα (Azure), όχι σε επίπεδο εταιρείας μόνο αλλά σε επίπεδο πελάτη.

Συγκεκριμένα, κάθε παιδικός σταθμός διαθέτει την δική του αποκλειστική βάση δεδομένων και όχι κομμάτι σε μία ευρύτερη όπως συμβαίνει στην συντριπτική πλειοψηφία των ανταγωνιστικών πακέτων. Κάτι τέτοιο φυσικά δεν είναι απαιτητό από το πλαίσιο GDPR αλλά είναι κάτι που επιδιώκουμε,ώστε να παρέχουμε την μέγιστη δυνατή ασφάλεια στους πελάτες μας.

Επίσης, κάθε παιδικός σταθμός έχει την δυνατότητα να ρυθμίσει την πλατφόρμα κατά τέτοιο τρόπο ώστε να αποκλείεται ακόμα και οποιαδήποτε πρόσβαση έξω από τα γεωγραφικά όρια του κτιρίου του. Ακόμα και σε περίπτωση διακοπής συμβολαίου με εμάς, η βάση δεδομένων, εφόσον ανήκει στον πελάτη, μπορεί να διαχειριστεί με τέτοιο τρόπο ώστε να μας αποκλείσει κάθε πιθανή πρόσβαση.

Smile, αρχιτεκτονική ασφάλειας, δεύτερο επίπεδο

Τα δεδομένα που αποθηκεύονται στο smile είναι κρυπτογραφημένα. Σύμφωνα με την ρυθμιστική αρχή, οποιαδήποτε διαρροή **μη κρυπτογραφημένων δεδομένων** πρέπει να καταγγελθεί άμεσα στην Αρχή Προστασίας Δεδομένων. Ακόμη και στην περίπτωση πχ που ο διαχειριστής του παιδικού σταθμού απωλέσει κάποιο έγγραφο με τα στοιχεία σας, αν το τελευταίο δεν είναι κρυπτογραφημένο, είναι **υποχρεωμένος βάσει Ευρωπαϊκού νόμου** να το αναφέρει. **Ελέγξτε τους υπεύθυνους του σταθμού σας.** Τα δεδομένα των παιδιών μας πρέπει να διαφυλάττονται με την δέουσα αυστηρότητα.

Στο smile, ακριβώς επειδή τα δεδομένα είναι α) κρυπτογραφημένα και β) όχι με την μορφή του τυπικού “αρχείου χύμα” δεν δύνανται να ανακτηθούν κακοβούλως ή να απωλεσθούν εκτός από περιπτώσεις

- Κλοπής του ψηφιακού μέσου
- Φυσικής Καταστροφής του ψηφιακού μέσου

Smile, αρχιτεκτονική ασφάλειας, δεύτερο επίπεδο

Και στις δύο περιπτώσεις το μόνο που πρέπει να γίνει είναι να ενημερώσει ο σταθμός την εταιρεία μας. Μέσα σε 5 λεπτά το αργότερο γίνονται οι ακόλουθες διαδικασίες.

1) Αλλαγή κλειδιού κρυπτογράφησης
2) Αλλαγή χαρακτηριστικών της βάσης Δεδομένων
3) Μεταφορά των αλλαγών στο νέο ψηφιακό μέσο

Ως συνέπεια τα απολεσθέντα δεδομένα αχρηστεύονται ενώ ο σταθμός συνεχίζει την εργασία του απρόσκοπτα με τα ίδια δεδομένα ως προϊόν ανάκτησης (automatic backup κάθε 5 λεπτά).

Smile, αρχιτεκτονική ασφάλειας, τρίτο επίπεδο

Σε επίπεδο **εφαρμογής** ο σταθμός δύναται να ορίσει βαθμούς προσβασιμότητας του προσωπικού με πολύ μεγάλη λεπτομέρεια. Αν δηλαδή ο διαχειριστής (administrator) το ζητήσει ευαίσθητα δεδομένα μπορεί να αποκλειστούν πλήρως από π.χ μη εξουσιοδοτημένο προσωπικό.

Για παράδειγμα στην τάξη Α, πρόσβαση μπορεί να έχει μόνο ο πρωτεύον και ο δευτερεύον εκπαιδευτικός και κανένας άλλος.
Στα οικονομικά και στην ηλεκτρονική αλληλογραφία μπορεί να οριστεί αποκλειστικός διαχειριστής, στα της διατροφής που πιθανώς να συνοδεύονται από ευαίσθητα δεδομένα ιατρικής φύσεως (π.χ αλλεργίες, δυσανεξίες) επίσης ξεχωριστός διαχειριστής κ.ο.κ.

Σε περίπτωση που οποιαδήποτε μέλος του προσωπικού διακόψει την συνεργασία με τον σταθμό τότε αυτόματα οποιαδήποτε πρόσβασή του ανακαλείται άμεσα με απόδειξη διαγραφής (proof of deletion).

Smile, αρχές GDPR

- Δικαίωμα στην λήθη (right to be forgotten)

Σε απόλυτο σεβασμό με το άνω δικαίωμα που κατοχυρώθηκε το 2006 και αυστηροποιήθηκε με το νομικό πλαίσιο του GDPR , το smile, άπαξ και ο σταθμός διακόψει την συνεργασία με μία οικογένεια, είτε επειδή το παιδάκι αποφοίτησε ή για οποιαδήποτε άλλο λόγο, το σύστημα μετατρέπει τις εγγραφές του παιδιού σε “ανενεργές”. Στην συνέχεια μετά από 3 μήνες διαγράφονται αυτόματα με αποδεικτικό **εκτός αν υπάρχει πρότερη συναίνεση γονέων να κρατηθούν τα επικοινωνιακά τους στοιχεία,** οπότε και το σύστημα κρατάει **αυτά και μόνον**.

- Συμμόρφωση στην ορθή χρήση (compliance)

Το smile χρησιμοποιεί δεδομένα μόνο όπως αυτά φαίνονται στην οθόνη του τελικού χρήστη. Με ευκρινή ερωτήματα και ξεκάθαρες οθόνες παρέχει σαφήνεια ως προς στην χρήση κάθε υπο εφαρμογής.

- Συμμόρφωση στην αλλαγή επιπέδου χρήσης (consumer choice)

Οποιαδήποτε στιγμή οποιασδήποτε γονέας επιθυμεί να αλλάξει πολιτική, αυτόματα το smile με μερικά κλικ ικανοποιεί την επιθυμία του. Διαγραφή του email του από το σύστημα τον αποκλείει από μαζικές ειδοποιήσεις, διαγραφή της διεύθυνσης τον αποκλείει από την εφαρμογή tracking του σχολικού κ.ο.κ

Εσάς πόσο ο σταθμός σας σέβεται τα δεδομένα σας ?

- Αρχεία χύμα και “χαρτούρα”

Δυστυχώς ίδιον πολλών σχολείων “παλαιάς” κοπής. Κοινώς τα δεδομένα σας αλλά και των παιδιών σας είναι “στον αέρα”. Ζητήστε από τον διαχειριστή του σταθμού σας να αλλάξει μέθοδο.

- Το τυπικό BCC στα email

Η συντριπτική πλειοψηφία των σταθμών (εκτός φυσικά αυτών που διαθέτουν το smile) διαχειρίζονται μαζικές αποστολές ηλεκτρονικού ταχυδρομείου με την μέθοδο του Blind Carbon Copy. Τούτο είναι στα όρια της νομιμότητας και σίγουρα ξεπερνά αυτά της αγένειας. Οι λόγοι.

α) Υπάρχει σοβαρότατος κίνδυνος αντί για μεταφορά της λίστας αλληλογραφίας στο πεδίο BCC να γίνει στο CC. Σε μιά τέτοια τραγική περίπτωση, όλοι οι γονείς θα μάθουν τις διευθύνσεις όλων. Αν ο σταθμός σας λειτουργεί υπό αυτόν τον τρόπο ζητήστε του να αλλάξει μέθοδο άμεσα.

β) Τέτοιες αποστολές είναι ιδανικός στόχος για spam φίλτρα, οπότε ενδέχεται να μην λάβετε την πληροφορία.

γ) Θυμίζουν “κουτσομπολιό”. ‘Ενα email προς εσάς πρέπει να είναι προς **εσάς και μόνο** και όχι προς κάποιον άγνωστο με ιδιαίτερη κοινοποίηση εσάς. Ζητήστε από το σχολείο σας να αλλάξει οπωσδήποτε μέθοδο.

- Φωτογραφίες χωρίς υδατογράφημα

Το smile σε ότι φωτογραφικό υλικό αποστέλλει, υπογράφει με ένα υδατογράφημα της σχολής. Έτσι κανένα τέτοιο αρχείο δεν μπορεί να “παραχαρακτεί” ή κοινοποιηθεί χωρίς τις αναμενόμενες νομικές συνέπειες.