GDPR - ΑΣΦΑΛΕΙΑ

.PIXEL

CGT
Career Gate Test

MANAGEMENT SYSTEM CERTIFIED
RiG CERT
ISO 9001 ISO/IEC 27001
ISO/IEC 27701

WIDE SERVICES
E-LEARNING SOLUTIONS

moodle Partner
PREMIUM CERTIFIED SERVICES PROVIDER

Στηρίζουμε:

Το χαμόγελο του παιδιού

Περιεχόμενα

Ασφάλεια - GDPR 3
Εισαγωγή 3
ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟΝ ΓΚΠΔ 4
GDPR στο Moodle 5
MOODLE & GDPR COMPLIANCE Ιδιωτικότητα δεδομένων 6
Αιτήματα δεδομένων 6
Απάντηση σε αιτήματα δεδομένων 7
Διαγραφή δεδομένων 7
Επιτρέποντας μόνο στον υπεύθυνο απορρήτου να κατεβάσει δεδομένα 7
Μητρώο δεδομένων 7
Παραδείγματα κατηγοριών 8
Ψηφιακή συναίνεση επαλήθευσης ηλικίας 8
Πολιτικές 8
Ενεργοποίηση του εργαλείου πολιτικών 8
Προσθήκη και διαχείριση πολιτικών 9
Δίνοντας συναίνεση σε πολιτικές 9
Πολιτικές για τους επισκέπτες 10
Ανήλικοι 10
Συναινέσεις χρηστών 10
Δίνοντας συναίνεση για λογαριασμό άλλων χρηστών 10
Δίνοντας συναίνεση για λογαριασμό ενός παιδιού 10
Ρόλος Υπεύθυνου Απορρήτου 10
Προσβασιμότητα στο Moodle 11
Καθιερωμένες πρακτικές 11
Συμμόρφωση με τα πρότυπα 11
WCAG 2.1 11
ATAG 2.0 12
APIA 1.1 12
Πολιτική Απορρήτου WIDE SERVICES P.C. 12
Τεχνικά μέτρα ασφαλείας 15

Διοικητικά μέτρα 19

Οι μηχανισμοί προστασίας των εκπαιδευτικών συστημάτων της WIDE Services που υλοποιούν τη συμμόρφωση με τον GDPR 21

Το Cloud – Microsoft Azure 23

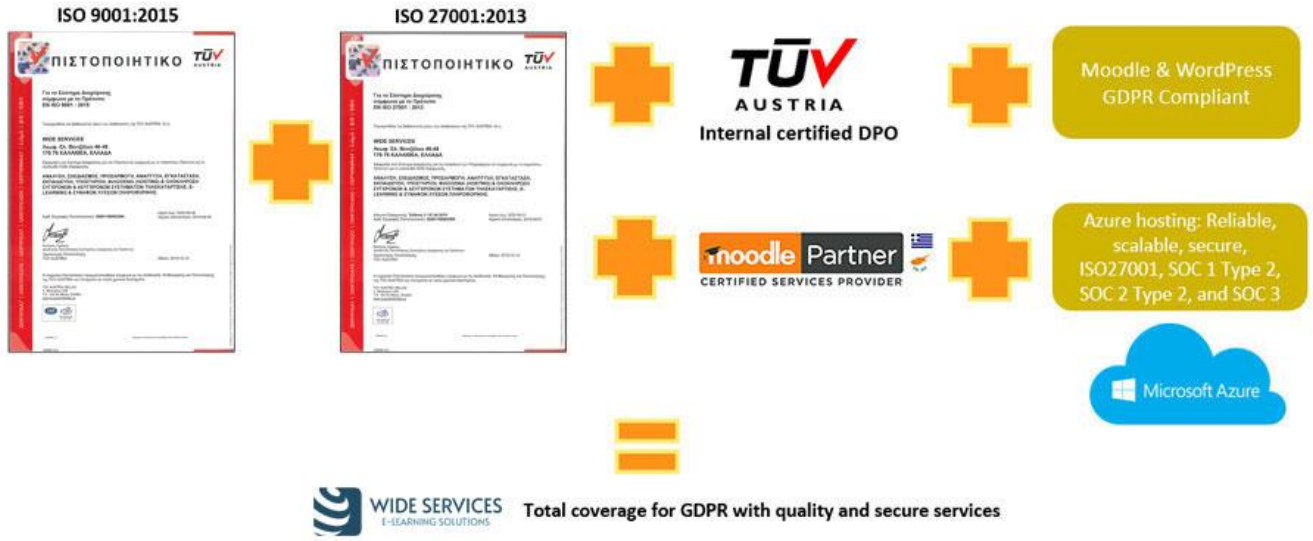
Ασφάλεια - GDPR

Εισαγωγή

Η **WIDE Services** σχεδιάζει λύσεις που καλύπτουν τα πρότυπα GDPR.

- ✓ Η πλατφόρμα **Moodle** συνοδεύεται από όλα τα απαραίτητα εργαλεία για να βοηθήσει έναν υπεύθυνο επεξεργασίας δεδομένων, εκτελών την επεξεργασία και υπεύθυνο προστασίας προσωπικών δεδομένων (DPO) στην εκπλήρωση των υποχρεώσεων και των δικαιωμάτων που απορρέουν από το GDPR.
- ✓ Η εταιρεία κατέχει **ISO 9001: 2015** και **ISO 27001: 2013** από το 2016 στο πεδίο "Ανάλυση, σχεδιασμός, προσαρμογή, ανάπτυξη, εγκατάσταση, εκπαίδευση, υποστήριξη, φιλοξενία (hosting) και ολοκλήρωση σύγχρονων και ασύγχρονων συστημάτων τηλεκατάρτισης, e-Learning και συναφών λύσεων πληροφορικής"
- ✓ Η **WIDE Services** χρησιμοποιεί την υπηρεσία **Microsoft Azure Cloud** η οποία είναι η πιο ασφαλής και αξιόπιστη υπηρεσία cloud από όλες τις διαθέσιμες. Το **Azure** πληροί ένα ευρύ φάσμα διεθνών και βιομηχανικών προδιαγραφών συμμόρφωσης, όπως οι Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 και SOC 2, καθώς και πρότυπα για κάθε χώρα, συμπεριλαμβανομένου του IRAP της Αυστραλίας, G-Cloud της Μ. Βρετανίας και MTCS της Σιγκαπούρης. Οι αυστηροί έλεγχοι τρίτων μερών, όπως αυτοί που έγιναν από το Βρετανικό Ινστιτούτο Τυποποίησης, επαληθεύουν την τήρηση των αυστηρών κανόνων ασφαλείας που επιβάλλει η Azure στους αυστηρούς ελέγχους ασφαλείας. (https://azure.microsoft.com/en-us/overview/trusted-cloud/).
- ✓ Η **WIDE Services** διαθέτει **DPO Executive** που έχει εκπαιδευτεί και πιστοποιηθεί με επιτυχία από την **TÜV AUSTRIA Hellas**.
- ✓ Η εταιρεία βραβεύτηκε τον Νοέμβριου του 2019 στο Global Moodle Moot της Βαρκελώνης από τα Moodle HQ ως η εταιρεία **Educator Partner of the Year**, ανάμεσα στο παγκόσμιο δίκτυο συνεργατών του Moodle.

Όλα τα παραπάνω, είναι σημαντικοί λόγοι για να επιλέξετε την **WIDE Services** για να συμμορφώσετε το LMS σας με το **GDPR**.



ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟΝ ΓΚΠΔ

Οι ακόλουθες ενέργειες αναλαμβάνονται προκειμένου να διασφαλιστεί ότι η WIDE Services συμμορφώνεται ανά πάσα στιγμή με την αρχή της λογοδοσίας του Γενικού Κανονισμού Προστασίας Δεδομένων και της κείμενης νομοθεσίας:

- Εφαρμόζουμε ISO 27001:2013 από το 2017.
- Η πλατφόρμα Moodle διαθέτει όλα τα τεχνικά χαρακτηριστικά ώστε να συμμορφώνεται με τον ΓΚΠΔ και την κείμενη νομοθεσία.
- Ακολουθούμε τις βέλτιστες πρακτικές και εφαρμόζουμε όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα, τόσο για τη συμμόρφωση με τον ΓΚΠΔ και την κείμενη νομοθεσία, όσο και για την αποφυγή περιστατικών παραβίασης προσωπικών δεδομένων.
- Έχουμε ορίσει εσωτερικό DPO, ο οποίος είναι πιστοποιημένος από την TUV Austria και έχει κοινοποιηθεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
- Έχουμε καταγεγραμμένη σαφή και αδιαμφισβήτητη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Όλο το προσωπικό που ασχολείται με τη διαχείριση δεδομένων προσωπικού χαρακτήρα κατανοεί τις ευθύνες του για την τήρηση της καλής πρακτικής προστασίας δεδομένων.
- Όλο το προσωπικό έχει εκπαιδευτεί σε θέματα ασφάλειας πληροφοριών (ISMS) και σε θέματα για την προστασία των δεδομένων.
- Εφαρμόζουμε κανόνες σχετικά με τη συναίνεση των υποκειμένων των δεδομένων

(όπου αυτό είναι απαραίτητο).
- Υπάρχουν διαθέσιμα κανάλια για τα υποκείμενα των δεδομένων που επιθυμούν να ασκήσουν τα δικαιώματά τους όσον αφορά τα προσωπικά δεδομένα και όλα τα αιτήματα αντιμετωπίζονται αποτελεσματικά και μέσα στο χρόνο που προβλέπεται.
- Έχουμε ενσωματώσει πολιτικές που αφορούν τη διαχείριση των δεδομένων προσωπικού χαρακτήρα μέσα στο ISO 27001.
- Οι διαδικασίες που αφορούν τα δεδομένα προσωπικού χαρακτήρα επανεξετάζονται ανά τακτά χρονικά διαστήματα, και επικαιροποιούνται όπου χρειαστεί.
- Η αρχή της ιδιωτικότητας κατά το σχεδιασμό υιοθετείται για όλα τα νέα ή τα μεταβαλλόμενα συστήματα και διαδικασίες.

- Καταγράφεται η ακόλουθη τεκμηρίωση των δραστηριοτήτων επεξεργασίας:

1. Όνομα εταιρίας και υπεύθυνος επεξεργασίας
2. Σκοπός της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα
3. Κατηγορίες ατόμων και προσωπικά δεδομένα που επεξεργάζονται
4. Κατηγορίες αποδεκτών προσωπικών δεδομένων
5. Συμφωνίες και μηχανισμοί για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρες εντός ή εκτός της ΕΕ, συμπεριλαμβανομένων των λεπτομερειών των ελέγχων που εφαρμόζονται
6. Προγράμματα διατήρησης προσωπικών δεδομένων

Αυτές οι ενέργειες επανεξετάζονται σε τακτική βάση ως μέρος της διαδικασίας διαχείρισης που αφορά την προστασία δεδομένων.

GDPR στο Moodle

Στην πλατφόρμα Moodle έχουν αναπτυχθεί μία σειρά από λειτουργίες, οι οποίες βοηθούν τα Moodle sites να συμμορφωθούν στις ανάγκες του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Οι λειτουργίες αυτές καλύπτουν τα παρακάτω:

- Οι νέοι χρήστες κατατοπίζονται σχετικά με τις εκδόσεις των πολιτικών προστασίας δεδομένων που ακολουθούνται στο Moodle site, και με τις συναινέσεις που πρέπει να παρέχουν ώστε να μπορούν να χρησιμοποιούν το Moodle site
- Διαχείριση αιτημάτων πρόσβασης στα προσωπικά δεδομένα, επεξεργασίας και διαγραφής προσωπικών δεδομένων
- Καταγραφή και ερώτηση για συναίνεση για συλλογή και χρήση δεδομένων από τρίτους
- Ορισμός σκοπού και περιόδου διατήρησης προσωπικών δεδομένων στο Moodle site

Πιο συγκεκριμένα, ο κάθε οργανισμός έχει τη δυνατότητα να αξιοποιεί της λειτουργίες της πλατφόρμας ώστε:

- Να δημιουργεί διαδικασία εγγραφής των χρηστών, με δυνατότητα ορισμού διάφορων πολιτικών προστασίας δεδομένων (σε επίπεδο site, ιδιωτικότητας, χρήση προσωπικών δεδομένων από τρίτους), ιχνηλάτηση συναινέσεων που έχει δώσει ο χρήστης και διαχείρισης ανανεώσεων των εκδόσεων των πολιτικών προστασίας δεδομένων.
- Να δημιουργεί διαδικασία η οποία θα επιτρέπει στους χρήστες να υποβάλλουν αιτήματα πρόσβασης αλλά και διαγραφής των προσωπικών τους δεδομένων. Οι διαχειριστές του Moodle site και οι Υπεύθυνοι Προστασίας Δεδομένων του οργανισμού έχουν τη δυνατότητα να επεξεργάζονται τα αιτήματα αυτά και να προβαίνουν στις αντίστοιχες ενέργειες.

Με τις παραπάνω ενέργειες διασφαλίζεται η συμμόρφωση κάθε Moodle site στις ανάγκες του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), αλλά και στις ειδικές ανάγκες κάθε οργανισμού, σύμφωνα με τις πολιτικές προστασίας δεδομένων που αυτός ακολουθεί.

MOODLE & GDPR COMPLIANCE Ιδιωτικότητα δεδομένων

Η λειτουργία απορρήτου δεδομένων παρέχει τη διαδικασία στους χρήστες της πλατφόρμας να υποβάλουν ένα αίτημα δεδομένων (επίσης γνωστό ως αίτημα πρόσβασης) και στον διαχειριστή του ιστότοπου ή στον υπεύθυνο απορρήτου να επεξεργαστεί αυτά τα αιτήματα.

Αιτήματα δεδομένων

Κάθε χρήστης μπορεί να στείλει ένα μήνυμα στον υπεύθυνο απορρήτου μέσω του συνδέσμου «Επικοινωνήστε με τον υπεύθυνο απορρήτου» στη σελίδα του προφίλ του. Επιπλέον, μπορούν να ζητήσουν αντίγραφο όλων των προσωπικών τους δεδομένων ή να ζητήσουν να διαγραφούν τα προσωπικά τους δεδομένα.
Ο υπεύθυνος απορρήτου λαμβάνει μια ειδοποίηση αιτήματος δεδομένων.
Εάν ο χρήστης έχει ζητήσει αντίγραφο όλων των προσωπικών του δεδομένων, μόλις εγκριθεί το αίτημα, θα λάβει μια ειδοποίηση που θα τον ενημερώνει ότι τα προσωπικά του δεδομένα μπορούν να ληφθούν από τη σελίδα αιτήσεων δεδομένων. Ο χρήστης έχει από προεπιλογή μία εβδομάδα για να κατεβάσει τα δεδομένα του προτού λήξει ο σύνδεσμος λήψης. Ένας διαχειριστής μπορεί να ορίσει διαφορετικό χρόνο λήξης για το

αίτημα δεδομένων.
Εάν ο χρήστης έχει ζητήσει να διαγραφούν τα προσωπικά του δεδομένα, αφού εγκριθεί το αίτημα, θα λάβουν ένα email για να τους ενημερώσουν και δεν θα μπορούν πλέον να συνδεθούν στον ιστότοπο.

Απάντηση σε αιτήματα δεδομένων

Ο υπεύθυνος απορρήτου μπορεί να απαντήσει σε αιτήματα δεδομένων επιλέγοντας Προβολή, Έγκριση ή Άρνηση ανάλογα με την περίπτωση
Εάν ο χρήστης έχει στείλει ένα μήνυμα, ο υπεύθυνος απορρήτου μπορεί να δει το μήνυμα και να αντιγράψει τη διεύθυνση email του χρήστη και, στη συνέχεια, να απαντήσει μέσω email. Αφού απαντήσουν, μπορούν να το επισημάνουν ως ολοκληρωμένο.

Διαγραφή δεδομένων

Όταν διαγράφονται τα δεδομένα ενός χρήστη, τυχόν δημοσιεύσεις σε φόρουμ διαγράφονται και αντικαθίστανται με μια πρόταση που δηλώνει ότι η ανάρτηση έχει αφαιρεθεί. Ωστόσο, εάν ο χρήστης ξεκίνησε οποιαδήποτε συζήτηση, το όνομά του εξακολουθεί να εμφανίζεται στη σελίδα του φόρουμ.

Επιτρέποντας μόνο στον υπεύθυνο απορρήτου να κατεβάσει δεδομένα

Κάνοντας χρήση των δικαιωμάτων ενός ρόλου στο Moodle 3.5.2 και έπειτα, οι οργανισμοί μπορούν να εμποδίσουν τους χρήστες να κατεβάσουν τα δικά τους δεδομένα και, αντίθετα, να επιτρέψουν σε έναν υπεύθυνο απορρήτου να το κατεβάσει για αυτούς. Ο υπεύθυνος απορρήτου μπορεί στη συνέχεια να υποβάλει ένα αίτημα δεδομένων για λογαριασμό ενός χρήστη (μέσω «Αιτημάτων δεδομένων» στη διαχείριση του ιστότοπου), να το εγκρίνει και να το κατεβάσει μέσω του αναπτυσσόμενου μενού Ενέργειες. Σε αυτήν την περίπτωση, ο υπεύθυνος απορρήτου θα λαμβάνει μηνύματα ειδοποίησης και ΟΧΙ ο χρήστης.

Μητρώο δεδομένων

Ο υπεύθυνος απορρήτου μπορεί να ορίσει σκοπούς (γιατί ο οργανισμός επεξεργάζεται δεδομένα) με περιόδους διατήρησης και κατηγορίες για δεδομένα που αποθηκεύονται στο Moodle στο μητρώο δεδομένων.
Ένας προεπιλεγμένος σκοπός και περίοδος διατήρησης μπορεί να οριστεί για κατηγορίες μαθημάτων, μαθήματα, ενότητες δραστηριότητας και μπλοκ Η περίοδος διατήρησης ξεκινάει να μετράει από την ημερομηνία λήξης του μαθήματος για το μάθημα στο οποίο βρίσκεται μια δραστηριότητα. Για έναν χρήστη είναι από την τελευταία ώρα σύνδεσης από τη στιγμή που δεν είναι πλέον εγγεγραμμένος (ή έχει ήδη διαγραφεί).

Παραδείγματα κατηγοριών

- Διοικητικά: Στοιχεία ταυτότητας, δεδομένα αναγνώρισης, φωτογραφίες
- Προσωπικά (τρόπος ζωής, οικογενειακή κατάσταση κ.λπ.)
- Οικονομικές και χρηματοοικονομικές πληροφορίες (εισόδημα, οικονομική κατάσταση, φορολογική κατάσταση κ.λπ.)
- Δεδομένα σύνδεσης (διεύθυνση IP, αρχεία καταγραφής κ.λπ.)
- Εκπαιδευτικά δεδομένα (Αξιολογημένα μαθήματα, σενάρια εξετάσεων κ.λπ.)
- Αρχεία επίτευξης εκπαίδευσης (Αποτελέσματα εξετάσεων, αξιολογήσεις, προσόντα κ.λπ.)
- Δεδομένα τοποθεσίας (δεδομένα GPS, GSM κ.λπ.)

Ψηφιακή συναίνεση επαλήθευσης ηλικίας

Στο Moodle 3.4.2 και μετά, μπορεί να ενεργοποιηθεί μια «Ψηφιακή συναίνεση επαλήθευσης ηλικίας». Μπορεί να καθοριστεί η προεπιλεγμένη ηλικία συναίνεσης και η ηλικία σε οποιαδήποτε χώρα όπου διαφέρει από την προεπιλογή. Οι κωδικοί χώρας καθορίζονται στο ISO 3166-2.

- *, 16
- AT, 14
- ES, 14
- US, 13

Στην παραπάνω λίστα, η προεπιλεγμένη ψηφιακή ηλικία είναι τα 16 χρόνια.
Εάν είναι ενεργοποιημένη η εγγραφή ΚΑΙ η «Ψηφιακή συναίνεση επαλήθευσης ηλικίας», όταν ένας νέος χρήστης κάνει κλικ στο κουμπί «Δημιουργία νέου λογαριασμού», θα του ζητηθεί να εισαγάγει την ηλικία και τη χώρα του. Εάν η ηλικία του χρήστη είναι χαμηλότερη από την ηλικία συγκατάθεσης για τη χώρα του, θα δει ένα μήνυμα που θα του ζητά να ζητήσει από τον γονέα / κηδεμόνα του να επικοινωνήσει με τον υπεύθυνο του ιστότοπου, όπως ορίζεται στην ενότητα «Επικοινωνία υποστήριξης».

Πολιτικές

Το εργαλείο πολιτικών παρέχει τη διαδικασία αποδοχής πολιτικών κατά την πρώτη σύνδεση ενός νέου χρήστη, τη δυνατότητα καθορισμού πολλαπλών πολιτικών (ιστότοπος, απόρρητο, τρίτο μέρος, cookies), την παρακολούθηση των συγκαταθέσεων των χρηστών και τη διαχείριση ενημερώσεων και νεότερων εκδόσεων των πολιτικών.
Το εργαλείο πολιτικών αποτελεί μέρος του συνόλου λειτουργιών απορρήτου του Moodle που βοηθά τους ιστότοπους να συμμορφώνονται με το GDPR.

Ενεργοποίηση του εργαλείου πολιτικών

Με την ενεργοποίηση του εργαλείου των πολιτικών, εμφανίζεται μία μπάρα στο κάτω μέρος της αρχικής σελίδας του ιστοτόπου. Η αρχική σελίδα μπορεί να είναι σελίδα με

πληροφορίες ή η σελίδα σύνδεσης (login page). Στην μπάρα αυτή εμφανίζονται σύνδεσμοι προς όλες τις πολιτικές που έχουν οριστεί, ώστε οι χρήστες να μπορούν να τις διαβάζουν πριν προχωρήσουν στη σύνδεση ή στην εγγραφή (αν υπάρχει).

Προσθήκη και διαχείριση πολιτικών

Ένας διαχειριστής ή οποιοσδήποτε χρήστης με τη δυνατότητα διαχείρισης πολιτικών (από προεπιλογή είναι ο διαχειριστής) μπορεί να έχει πρόσβαση στη σελίδα «Διαχείριση πολιτικών» στη διαχείριση του ιστότοπου και να:

- προσθέτει μία νέα πολιτική ιστότοπου / απορρήτου / τρίτου μέρους / άλλη πολιτική για όλους τους χρήστες, τους ενεργούς χρήστες ή τους επισκέπτες
- αλλάζει την ενεργή / ανενεργή κατάσταση κάθε πολιτικής
- βλέπει τον αριθμό και το ποσοστό των χρηστών που έχουν συμφωνήσει σε κάθε πολιτική
- επεξεργάζεται μια πολιτική και να καθορίζει αν πρόκειται για μια μικρή αλλαγή (που δεν απαιτεί από τους χρήστες να επιβεβαιώσουν εκ νέου τη συγκατάθεσή τους) ή μία σημαντική αλλαγή (που απαιτεί εκ νέου τη συγκατάθεση των χρηστών)
- Δει την τρέχουσα έκδοση κάθε πολιτικής, καθώς και τις προηγούμενες εκδόσεις
- αλλάζει τη σειρά με την οποία εμφανίζονται οι πολιτικές στους χρήστες

Λάβετε υπόψη ότι μόλις δημιουργηθεί, μια πολιτική μπορεί να επεξεργαστεί ή να οριστεί ως ανενεργή, αλλά εάν οι χρήστες έχουν συμφωνήσει, δεν μπορεί να διαγραφεί.
Ο τύπος πολιτικής (ιστότοπος / απόρρητο / τρίτα μέρη) εμφανίζεται μόνο στη σελίδα «Πολιτικές» που είναι συνδεδεμένος στο υποσέλιδο και η συμπεριφορά είναι η ίδια για όλους τους τύπους πολιτικής.

Δίνοντας συναίνεση σε πολιτικές

Όλοι οι χρήστες (με εξαίρεση τους διαχειριστές) θα πρέπει να δώσουν τη συγκατάθεσή τους σε όλες τις πολιτικές που ορίζονται είτε για "Πιστοποιημένους χρήστες" είτε για "'Ολους τους χρήστες" πριν προχωρήσουν περαιτέρω στον ιστότοπο.
Εάν προστεθεί μια νέα πολιτική, όλοι οι χρήστες θα πρέπει να δώσουν τη συγκατάθεσή τους κατά την επόμενη σύνδεσή τους. Ομοίως, εάν μια υπάρχουσα πολιτική έχει τροποποιηθεί και δεν επισημανθεί ως μικρή αλλαγή, όλοι οι χρήστες θα πρέπει να δώσουν τη συγκατάθεσή τους στην επόμενη σύνδεση τους.
Εάν η εγγραφή είναι ενεργοποιημένη στον ιστότοπο, οι νέοι χρήστες θα πρέπει να δώσουν τη συγκατάθεσή τους σε όλες τις πολιτικές πριν προχωρήσουν στη φόρμα εγγραφής. Εάν η ψηφιακή συναίνεση επαλήθευσης ηλικίας είναι ενεργοποιημένη στις "Ρυθμίσεις απορρήτου", όταν ένας νέος χρήστης κάνει κλικ στο κουμπί "Δημιουργία νέου λογαριασμού", θα τους ζητηθεί να εισάγει την ηλικία του και τη χώρα. Εάν η ηλικία του χρήστη είναι χαμηλότερη από την ηλικία συγκατάθεσης για τη χώρα του, θα δει ένα μήνυμα που θα του ζητά να ζητήσει από τον γονέα / κηδεμόνα του να επικοινωνήσει με τον ιστότοπο (όπως ορίζεται στην ενότητα «Επικοινωνία υποστήριξης»).

Πολιτικές για τους επισκέπτες

Εάν ένας χρήστης συνδεθεί ως επισκέπτης, θα εμφανιστεί ένα αναδυόμενο παράθυρο στο κάτω μέρος του παραθύρου του προγράμματος περιήγησης με συνδέσμους προς όλες τις πολιτικές που ορίζονται είτε για τους επισκέπτες είτε για όλους τους χρήστες.

Ανήλικοι

Οι χρήστες που είναι νεότεροι από την ηλικία της ψηφιακής συναίνεσης, και ονομάζονται «ανήλικοι», εμποδίζονται να δώσουν τη συγκατάθεσή τους απαγορεύοντας τη δυνατότητα «Συμφωνώ με τις πολιτικές». Στη συνέχεια, δεν θα μπορούν να προχωρήσουν περαιτέρω στον ιστότοπο έως ότου κάποιος μπορεί να δώσει τη συγκατάθεσή του για λογαριασμό τους.

Συναινέσεις χρηστών

Ένας διαχειριστής ή οποιοσδήποτε χρήστης με την ικανότητα Προβολή αναφορών συναινέσεων χρηστών (από προεπιλογή ο διαχειριστής) μπορεί να έχει πρόσβαση στη σελίδα "Συμφωνίες χρήστη" στη διαχείριση του ιστότοπου και:

- να βλέπει τις συναινέσεις των χρηστών
- να φιλτράρει κατά πολιτική, άδεια, κατάσταση ή ρόλο
- να δίνει τη συγκατάθεση για λογαριασμό ανηλίκων
- να κάνει λήψη του πίνακα δεδομένων

Οι συναινέσεις χρηστών για μια συγκεκριμένη πολιτική μπορούν επίσης να προβληθούν μέσω της σελίδας "Διαχείριση πολιτικών" κάνοντας κλικ στο σύνδεσμο στη στήλη Συναινέσεις.

Δίνοντας συναίνεση για λογαριασμό άλλων χρηστών

Ένας διαχειριστής ή οποιοσδήποτε χρήστης με την ικανότητα Συμφωνείτε με τις πολιτικές για λογαριασμό κάποιου άλλου μπορεί να δώσει συγκατάθεση για λογαριασμό ανηλίκων ή όταν έχει δοθεί γραπτή συγκατάθεση.
Χρήστες που έχουν τη δυνατότητα στο «Συμφωνώ με τις πολιτικές για λογαριασμό κάποιου άλλου», όπως οι διαχειριστές, μπορούν να δώσουν συγκατάθεση για λογαριασμό πολλών χρηστών.

Δίνοντας συναίνεση για λογαριασμό ενός παιδιού

Ένας γονέας ή κηδεμόνας μπορεί να επιτραπεί να δώσει συγκατάθεση εκ μέρους του παιδιού του, παρέχοντάς του τη δυνατότητα «Συμφωνώ με τις πολιτικές για λογαριασμό κάποιου άλλου».

Ρόλος Υπεύθυνου Απορρήτου

Συνιστάται να δημιουργηθεί ένας ρόλος υπευθύνου απορρήτου και να ανατεθεί στον αντίστοιχο υπεύθυνο του οργανισμού. Εάν δεν υπάρχει κανένας στον ιστότοπο με το

ρόλο του υπευθύνου απορρήτου, δηλαδή κανείς που δεν έχει τη δυνατότητα να διαχειριστεί αιτήματα δεδομένων, τότε ένας διαχειριστής ιστότοπου μπορεί να απαντά σε αιτήματα δεδομένων και να διαχειρίζεται το μητρώο δεδομένων.

Ο ρόλος του Υπευθύνου Απορρήτου έχει τις εξής δυνατότητες:

- Να διαχειρίζεται το μητρώου δεδομένων
- Να διαχειρίζεται τις πολιτικές
- Να διαχειρίζεται τις συναινέσεις
- Να απαντάει σε αιτήματα

Μπορούμε επίσης να δώσουμε και επιπλέον δικαιώματα στον ρόλο αυτό

Προσβασιμότητα στο Moodle

Το Moodle είναι μία πλατφόρμα πλήρως προσβάσιμη και χρησιμοποιήσιμη για όλους τους χρήστες ανεξάρτητα από τις ειδικές ικανότητες που μπορεί να υπάρχουν.

Καθιερωμένες πρακτικές

Οι προγραμματιστές του Moodle ξοδεύουν πολύ χρόνο για να διασφαλίσουν ότι οι νέες δυνατότητες είναι προσβάσιμες. Μέρος της διαδικασίας κατά τη δημιουργία νέου κώδικα στο Moodle είναι η παρακολούθηση καθιερωμένων βέλτιστων πρακτικών και μέρος της διαδικασίας αποδοχής νέου κώδικα στον πυρήνα είναι η προσεκτική δοκιμή των σελίδων και η συλλογή σχολίων από ειδικούς.

Συμμόρφωση με τα πρότυπα

Η πλατφόρμα Moodle είναι ένα πολύπλοκο σύστημα με πολλά μέρη και επίπεδα. Ο κώδικάς του εξελίσσεται συνεχώς. Οι δυνατότητες του μπορούν να ενεργοποιηθούν και να απενεργοποιηθούν. Η εμφάνιση μπορεί να προσαρμοστεί σε μεγάλο βαθμό χρησιμοποιώντας θέματα και χιλιάδες ρυθμίσεις. Το πραγματικό περιεχόμενο μπορεί να δημιουργηθεί από οποιονδήποτε δάσκαλο ή οποιονδήποτε μαθητή. Ως εκ τούτου, είναι αδύνατο να πούμε με 100% βεβαιότητα εάν το Moodle είναι απολύτως προσβάσιμος ή όχι. Η προσβασιμότητα δεν είναι μια κατάσταση, είναι μια διαδικασία συνεχούς βελτίωσης ως απάντηση στους χρήστες μας και στο ευρύτερο τεχνικό περιβάλλον.

WCAG 2.1

Το Moodle πληροί όλες τις προυποθέσεις για το πρότυπο WCAG 2.1 και γι’ αυτό έχει πιστοποιηθεί από την WebKeyIT. Λεπτομέρειες στον παρακάτω σύνδεσμο.
https://www.webkeyit.com/accessibility-services/accessibility-accreditations/moodle/
Η WIDE Services, ελέγχει την συμμόρφωση με το πρότυπο WCAG 2.1 χρησιμοποιώντας και το εργαλείο achecker.ca

ATAG 2.0

Καθώς το Moodle είναι μία πλατφόρμα για την κατασκευή περιεχομένου (καθώς και για προβολή περιεχομένου), πρέπει να υπάρχει συμβατότητα με το πρότυπο ATAG 2.0. Από την έκδοση 2.7 του Moodle έχει προστεθεί ο νέος επεξεργαστής κειμένου Atto που όχι μόνο βοηθά στη βελτίωση του τρόπου με τον οποίο όλοι μπορούν να χρησιμοποιήσουν τον ίδιο τον επεξεργαστή, αλλά επίσης βοηθούν στη βελτίωση της προσβασιμότητας του περιεχομένου που παράγεται με αυτόν.

ARIA 1.1

Καθώς πολλά μέρη της διεπαφής των χρηστών του Moodle είναι δυναμικά και διαδραστικά, το Moodle ακολουθεί τις οδηγίες του προτύπου ARIA 1.1 για την ενημέρωση βοηθητικών τεχνολογιών, όπως οι αναγνώστες οθόνης.

Πολιτική Απορρήτου WIDE SERVICES P.C.

1. ΣΚΟΠΟΣ

Σκοπός της παρούσας πολιτικής είναι να καθορίσει και να γνωστοποιήσει τις υποχρεώσεις, καθώς και τις πολιτικές της WIDE Services για την ιδιωτικότητα και την προστασία των δεδομένων προσωπικού χαρακτήρα.

Η διοίκηση της WIDE Services, δεσμεύεται για την εκπλήρωση των απαιτήσεων του Γενικού Κανονισμού Προστασίας των Δεδομένων (GDPR) και του νόμου 4624/2019 για την προστασία προσωπικών δεδομένων και αναγνωρίζει την προστασία των δεδομένων προσωπικού χαρακτήρα ως προτεραιότητα. Η δημιουργία περιβάλλοντος ασφάλειας και εμπιστοσύνης, εσωτερικά και εξωτερικά, αποτελεί αρχή της WIDE Services και για τη διασφάλιση της εφαρμογής του, η εταιρεία δεσμεύεται ότι θα διαθέσει κάθε αναγκαίο πόρο που θα χρειαστεί.

2. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η πολιτική απορρήτου αφορά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από την WIDE Services.

3. ΥΠΕΥΘΥΝΟΤΗΤΕΣ

Υπεύθυνοι για την τήρηση της παρούσας πολιτικής είναι ο Data Protection Officer και η ομάδα ασφάλειας πληροφοριών όπως ορίζεται σε αντίστοιχη διαδικασία της εταιρίας.

4. ΑΡΧΕΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

Η WIDE Services διασφαλίζει τη συμμόρφωση με τις θεμελιώδεις αρχές του Κανονισμού Προστασίας Προσωπικών Δεδομένων και του νόμου 4624/2019 για την προστασία προσωπικών δεδομένων τόσο στην επεξεργασία που εκτελείται επί του παρόντος όσο και στο πλαίσιο της εισαγωγής νέων μεθόδων επεξεργασίας, όπως τα νέα πληροφοριακά

συστήματα που ενδέχεται να εγκατασταθούν.
Συγκεκριμένα οι αρχές επεξεργασίας με τις οποίες η WIDE Services διασφαλίζει τη συμμόρφωση αφορούν:
- Τη νομιμότητα, την αντικειμενικότητα και τη διαφάνεια
- Τον περιορισμό του σκοπού
- Την ελαχιστοποίηση των δεδομένων
- Την ακρίβεια
- Τον περιορισμό της περιόδου αποθήκευσης
- Την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα
- Τη λογοδοσία

5. ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΑΤΟΜΟΥ

Τα δικαιώματα των υποκειμένων των δεδομένων υποστηρίζονται από κατάλληλες διαδικασίες που επιτρέπουν την ανάληψη των απαιτούμενων ενεργειών εντός των χρονικών ορίων που ορίζονται στον Γενικό Κανονισμό Προστασίας Δεδομένων και τον νόμο 4624/2019 για την προστασία προσωπικών δεδομένων.
Τα δικαιώματα των υποκειμένων είναι τα παρακάτω:
• Το δικαίωμα της ενημέρωσης
• Το δικαίωμα πρόσβασης
• Το δικαίωμα διόρθωσης
• Το «δικαίωμα στη λήθη»
• Το δικαίωμα στον περιορισμό της επεξεργασίας
• Το δικαίωμα στην φορητότητα
• Το δικαίωμα αντίρρησης
• Το δικαίωμα αντίρρησης στις περιπτώσεις profiling

6. ΝΟΜΙΜΟΤΗΤΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Είναι πολιτική της WIDE Services να προσδιορίζει την κατάλληλη νομική βάση για κάθε επεξεργασία και να την τεκμηριώνει, σύμφωνα με τον Κανονισμό Προστασίας Προσωπικών Δεδομένων και τον νόμο 4624/2019 για την προστασία προσωπικών δεδομένων.

7. ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ

Η εταιρία υιοθετεί την αρχή της προστασίας των δεδομένων προσωπικού χαρακτήρα από τον σχεδιασμό και διασφαλίζει ότι ο προσδιορισμός και ο σχεδιασμός όλων των νέων ή μεταβαλλόμενων πληροφοριακών συστημάτων που συλλέγουν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα θα υπόκεινται στην κατάλληλη εξέταση των θεμάτων προστασίας της ιδιωτικής ζωής.
Όταν οι πράξεις επεξεργασίας ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, η WIDE Services διενεργεί εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων.

Η χρήση τεχνικών και διαδικασιών όπως η ελαχιστοποίηση των δεδομένων, η ψευδωνυμοποίηση, η ανωνυμοποίηση και η κρυπτογράφηση, λαμβάνονται υπόψη και υλοποιούνται, όπου αυτό είναι εφικτό και κατάλληλο.

8. ΣΥΜΒΑΣΕΙΣ ΠΟΥ ΠΕΡΙΛΑΜΒΑΝΟΥΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Η εταιρία διασφαλίζει ότι όλες οι δραστηριότητες που εισάγει στο πλαίσιο ανάπτυξης συνεργασιών και αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, υπόκεινται σε τεκμηριωμένη σύμβαση που περιλαμβάνει τις συγκεκριμένες πληροφορίες και τους όρους που απαιτούνται από τον Γενικό Κανονισμό Προστασίας Δεδομένων και την κείμενη νομοθεσία.

Με κάθε εκτελών την επεξεργασία ή υπεργολάβο, υπογράφεται ιδιωτικό συμφωνητικό σύμφωνα με το άρθρο 28 του κανονισμού, το οποίο αναφέρει μεταξύ άλλων τα ακόλουθα:

- πεδίο εφαρμογής και διάρκεια
- σκοπό
- τεκμηρίωση μορφών και έκτασης επεξεργασίας,
- προηγούμενη εξουσιοδότηση σε περίπτωση που χρησιμοποιείται άλλος επεξεργαστής,
- την παροχή οποιασδήποτε τεκμηρίωσης που αποδεικνύει τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων και την κείμενη νομοθεσία.
- άμεση κοινοποίηση οποιασδήποτε παραβίασης των δεδομένων

Τα δικαιώματα των εργαζομένων, των συμβαλλομένων και άλλων τρίτων όταν δεν έχουν πλέον άδεια πρόσβασης σε χώρους ή πόρους ή όταν λήξει η σύμβαση εργασίας τους, ανακαλούνται ή σε κάθε περίπτωση που χρειάζεται γίνεται επανεκτίμηση και επανέλεγχος των προσβάσεών τους.

9. ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΣΕ ΤΡΙΤΕΣ ΧΩΡΕΣ

Στην περίπτωση που υπάρχουν διαβιβάσεις δεδομένων προσωπικού χαρακτήρα εντός ή εκτός της Ευρωπαϊκής Ένωσης εξετάζονται προσεκτικά πριν από τη διαβίβαση, ώστε να διασφαλιστεί ότι εμπίπτουν στα όρια που επιβάλλει ο Γενικός Κανονισμός Προστασίας Δεδομένων και η κείμενη νομοθεσία. Αυτό εξαρτάται εν μέρει από την κρίση της Ευρωπαϊκής Επιτροπής σχετικά με την επάρκεια των διασφαλίσεων για τα προσωπικά δεδομένα που ισχύουν στη χώρα υποδοχής και το οποίο μπορεί να αλλάξει με την πάροδο του χρόνου ή/και από την αξιοπιστία της εταιρείας που πρόκειται να διαβιβαστούν τα δεδομένα προσωπικού χαρακτήρα η οποία αξιολογείται κατά περίπτωση.

10. ΧΡΟΝΟΣ ΔΙΑΤΗΡΗΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Η WIDE Services διατηρεί τα δεδομένα προσωπικού χαρακτήρα για όσο χρόνο διαρκεί ο σκοπός επεξεργασίας τους. Μετά τη λήξη του, η WIDE Services διατηρεί, σύννομα,

τα δεδομένα προσωπικού χαρακτήρα, όταν είναι αναγκαίο, για τη συμμόρφωση με νομική της υποχρέωση, απορρέουσα από διατάξεις του Ενωσιακού ή Εθνικού Δικαίου. Εάν δεν υπάρξει τέτοια ανάγκη, τα δεδομένα προσωπικού χαρακτήρα, διαγράφονται από όλα τα πληροφορικά της συστήματα και τα αντίγραφά τους.

11. ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Η WIDE Services διαθέτει εσωτερικό DPO, ο οποίος είναι πιστοποιημένος από την TUV Austria και έχει κοινοποιηθεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Αρμοδιότητες του είναι η συνεχής παρακολούθηση της συμμόρφωσης της εταιρείας με το νόμο 4624/2019 για την προστασία προσωπικών δεδομένων, που ενσωματώνει τον ΓΚΠΔ.

12. ΔΗΛΩΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Η πολιτική της WIDE Services είναι δίκαιη και αναλογική όταν εξετάζει τα μέτρα που πρέπει να ληφθούν για την ενημέρωση των επηρεαζόμενων μερών σχετικά με τις παραβιάσεις δεδομένων προσωπικού χαρακτήρα. Αυτό θα γίνεται σύμφωνα με το σχέδιο διαχείρισης που καθορίζει τη συνολική διαδικασία αντιμετώπισης περιστατικών ασφάλειας πληροφοριών.

12. ΕΠΙΒΟΛΗ ΠΟΙΝΗΣ

Αν βρεθεί υπάλληλος ή συνεργάτης που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

Αυτή η πολιτική απορρήτου μπορεί να αλλάζει ανά διαστήματα σύμφωνα με τη νομοθεσία ή τις εξελίξεις στον κλάδο. Η πολιτική αυτή είναι μέρος ενός συνόλου πολιτικών που εφαρμόζει η WIDE Services στα πλαίσια εφαρμογής των ISO 27001 και ISO 9001.

Τεχνικά μέτρα ασφαλείας

1. Αντίγραφα ασφαλείας

Α) Η WIDE Services έχει αναπτύξει συγκεκριμένη πολιτική για τη λήψη και διαχείριση των αντιγράφων ασφαλείας. Η πολιτική περιλαμβάνει, μεταξύ άλλων, τους κανόνες/διαδικασίες που αφορούν την επιλογή των κρίσιμων πόρων (εφαρμογές, λειτουργικά συστήματα, αρχεία, δεδομένα αρχείων χρηστών, κ.λπ.) που χρήζουν δημιουργίας αντιγράφων ασφαλείας, τη συχνότητα της δημιουργίας/λήψης των αντιγράφων ασφαλείας, την κατάλληλη επισήμανση αυτών, την ασφαλή αποθήκευσή τους και την ορθή ανάκτηση των δεδομένων από τα αντίγραφα ασφαλείας.

Β) Τα αντίγραφα ασφαλείας διατηρούνται σε διαφορετικό χώρο/φυσική τοποθεσία από τα πρωτογενή δεδομένα, ο οποίος διαθέτει μέτρα ασφαλείας ανάλογα με τα μέτρα που υιοθετούνται για τα πρωτογενή δεδομένα. Επίσης, λαμβάνονται μέτρα για την ασφαλή

μεταφορά του.
Γ) Κατά τη διαγραφή Δεδομένων Προσωπικού Χαρακτήρα από τα παραγωγικά συστήματα, αυτά διαγράφονται και από τα αντίγραφα ασφαλείας.
Δ) Τα backup που δημιουργούνται και αποθηκεύονται έχουν την παρακάτω δομή:

- 1 ημερήσιο backup για τις τελευταίες 15 ημέρες
- 1 εβδομαδιαίο backup για τις τελευταίες 12 εβδομάδες
- 1 μηνιαίο backup για τους τελευταίους 12 μήνες
- 1 backup για τους τελευταίους 24 μήνες

Οπότε αν για οποιαδήποτε περίπτωση χρειαστεί να επαναφέρουμε την πλατφόρμα σε προηγούμενη ημερομηνία, μπορούμε να επιλέξουμε ανάμεσα σε 40 αρχεία.
Ε) Ο διαχειριστής του συστήματος έχει τη δυνατότητα να δημιουργήσει αντίγραφα ασφαλείας του εκπαιδευτικού υλικού, σε επίπεδο μαθήματος και δραστηριοτήτων, και να τα αφήσει στον server για πιθανή μελλοντική χρήση ή να τα «κατεβάσει» στον υπολογιστή του για μεγαλύτερη ασφάλεια.

2. Διαμόρφωση υπολογιστών

Α) Σε κάθε υπολογιστή του προσωπικού της WIDE Services, που τηρεί ή επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, υπάρχει προστασία από κακόβουλο λογισμικό. Αυτό επιτυγχάνεται (πέραν της σωστής χρήσης αυτών από τους υπαλλήλους) με προγράμματα antivirus, καθώς και με χρήση προγραμμάτων firewall. Τόσο το antivirus όσο και το firewall διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις. Επιπλέον, στο λειτουργικό σύστημα των υπολογιστών και στις εφαρμογές που αυτό είναι δυνατόν, (εφόσον είναι συνδεδεμένοι στο Διαδίκτυο) εγκαθίστανται ανά τακτά διαστήματα ενημερώσεις ασφαλείας.
Β) Η WIDE Services δεν επιτρέπει ενέργειες απλών χρηστών στους υπολογιστές οι οποίες επηρεάζουν τη συνολική τους διαμόρφωση (π.χ. απενεργοποίηση αντιβιοτικών προγραμμάτων, εγκατάσταση νέων προγραμμάτων ή αλλαγή ρυθμίσεων υπαρχόντων, κ.λπ.). Μόνο οι System Administrators της εταιρείας έχουν τα απαραίτητα δικαιώματα για να κάνουν τέτοιου είδους τροποποιήσεις. Επίσης γίνεται περιοδικός έλεγχος του εγκατεστημένου λογισμικού από τους System Administrators για τον τυχόν εντοπισμό προγραμμάτων που έχουν εγκατασταθεί εκτός των εγκεκριμένων διαδικασιών.
Γ) Ο υπολογιστής που χρησιμοποιείται σαν κεντρικός διακομιστής (server) για άλλους υπολογιστές, δε χρησιμοποιείται ως σταθμός εργασίας από κάποιον χρήστη.
Δ) Οι ηλεκτρονικοί υπολογιστές που χρησιμοποιούνται από τους τελικούς χρήστες δεν διαθέτουν δυνατότητα εξαγωγής δεδομένων με τη χρήση αποσπώμενων μέσων (π.χ. USB, CD/DVD) – εκτός αν υπάρχει έγκριση από τον Υπεύθυνο Ασφαλείας (ή άλλης μορφής έγκριση, μέσω διαδικασίας που προβλέπεται στην πολιτική ασφαλείας).
Ε) Στους υπολογιστές που έχουν πρόσβαση στο διαδίκτυο δεν αποθηκεύονται δεδομένα προσωπικού χαρακτήρα (εκτός αν κάτι τέτοιο είναι απολύτως απαραίτητο στο πλαίσιο

του ρόλου/αρμοδιοτήτων που έχουν ανατεθεί στο χρήστη του υπολογιστή).
ΣΤ) Η WIDE Services διαθέτει κατάλληλους μηχανισμούς για την αποφυγή περιπτώσεων όπου δύναται κάποιος να έχει εύκολα πρόσβαση οποιουδήποτε τύπου σε προσωπικά δεδομένα, λόγω ενός ανοιχτού υπολογιστή, ο οποίος μένει χωρίς επίβλεψη (έστω και για λίγα λεπτά). Προς αυτή την κατεύθυνση έχουν αναπτυχθεί διαδικασίες αυτόματης αποσύνδεσης (μετά από ένα εύλογο χρονικό διάστημα αδράνειας) ή/και ενεργοποίηση της προφύλαξης οθόνης (screen saver) του υπολογιστή – για την απενεργοποίηση της οποίας απαιτείται χρήση συνθηματικού.

3. Αρχεία καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας

Α) Σε όλες τις πλατφόρμες που διαχειρίζεται η WIDE Services, υπάρχουν διαδικασίες για την τήρηση και τον έλεγχο των αρχείων καταγραφής όλων των ενεργειών (log files) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων ασφαλείας. Στα αρχεία αυτά έχουν πρόσβαση ο υπεύθυνος ασφαλείας, οι διαχειριστές συστημάτων και όποια άλλα μέλη του προσωπικού είναι επιφορτισμένα με αρμοδιότητες διαχείρισης περιστατικών ασφαλείας κατόπιν έγγραφης εξουσιοδότησης.
Β) Η διαδικασία διαγραφής των αρχείων καταγραφής των συστημάτων δεν είναι δυνατή από ένα μόνο άτομο. Τέτοια διαγραφή γίνεται με την παρουσία 2 τουλάχιστον ατόμων, τα οποία θα έχουν διαφορετικούς ρόλους (π.χ. υπεύθυνος ασφαλείας + διοικητικός διευθυντής).

4. Ασφάλεια επικοινωνιών

Α) Οι System Administrators και ο Υπεύθυνος Ασφαλείας της WIDE Services είναι υπεύθυνοι ώστε να υπάρχει επαρκής έλεγχος των συνδεόμενων στο δίκτυο συσκευών (ως προς την πρόσβαση σε αυτές αλλά και τη χρήση τους).
Β) Η WIDE Services διαθέτει συγκεκριμένη διαδικασία για τη διαχείριση της απομακρυσμένης πρόσβασης σε συστήματα μέσω ασφαλών καναλιών με δυνατή ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση. Προς τούτο, επισημαίνεται ιδιαίτερα ότι οι τεχνολογίες απομακρυσμένης πρόσβασης (π.χ. Remote Desktop, VPN, ασύρματη σύνδεση, κ.λπ.) επιτρέπονται μόνο σε εξουσιοδοτημένα πρόσωπα για τα οποία είναι απόλυτα απαραίτητες στο πλαίσιο των αρμοδιοτήτων τους. Συνεπώς, η απομακρυσμένη πρόσβαση γίνεται υπό την εποπτεία και έλεγχο του System Administrator και του Υπεύθυνου Ασφαλείας και καταγράφεται.
Γ) Η WIDE Services έχει εξασφαλίσει ότι η επικοινωνία μεταξύ υπολογιστών γίνεται μέσω επαρκώς ασφαλούς καναλιού επικοινωνίας (π.χ. με χρήση κρυπτογράφησης ή ιδιωτικών γραμμών ελεγχόμενης φυσικής πρόσβασης).
Δ) Η WIDE Services αποφεύγει τη χρήση ευπαθών ως προς την ασφάλεια πρωτοκόλλων όπως FTP, telnet (όπου δεν γίνεται κρυπτογράφηση) και, όταν υπηρεσίες τέτοιων πρωτοκόλλων είναι αναγκαίες, γίνεται χρήση των αντίστοιχων ασφαλών (όπως, για παράδειγμα, SFTP, SSH).

Ε) Η WIDE Services διαθέτει διαδικασία για τον επαρκή έλεγχο των δικτυακών συνδέσεων του εσωτερικού δικτύου από και προς το διαδίκτυο ή άλλα εξωτερικά, μη έμπιστα, δίκτυα όπως μέσω του σημείου ελέγχου της περιμέτρου (firewall). Οι συνδέσεις που ενεργοποιούνται μέσω του firewall και οι υπηρεσίες που εξυπηρετούν εγκρίνονται από τον υπεύθυνο ασφαλείας και τους System Administrators.

5. Αποσπώμενα μέσα αποθήκευσης

Α) Η WIDE Services διαθέτει διαδικασίες για την αποτελεσματική κρυπτογράφηση (επιλογή σύγχρονων και ισχυρών αλγορίθμων κρυπτογράφησης, κατάλληλο μέγεθος κλειδιών και τεχνικές διαχείρισης αυτών, κ.λπ.) αρχείων με προσωπικά δεδομένα, ιδίως ευαίσθητα, που τηρούνται σε φορητά αποθηκευτικά μέσα (π.χ. USB δίσκους κ.ο.κ.), αφού για αυτές τις περιπτώσεις ο κίνδυνος διαρροής δεδομένων αυξάνεται. Αποθήκευση αρχείων με προσωπικά δεδομένα, αποφεύγεται να γίνεται σε αποσπώμενα μέσα αποθήκευσης, εκτός αν αυτό κριθεί απαραίτητο.

6. Ασφάλεια λογισμικού

Α) Ο σχεδιασμός των εφαρμογών που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων πραγματοποιείται λαμβάνοντας υπόψη τις βασικές αρχές της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας (privacy by design). Ως εκ τούτου, οι εφαρμογές ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων (data minimization), καθώς και της ποιότητας των δεδομένων και περιλαμβάνουν τη δυνατότητα της διαγραφής δεδομένων μετά το χρονικό διάστημα που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Επίσης, επιτρέπουν την υλοποίηση όλων των απαιτούμενων τεχνικών μηχανισμών ασφαλείας για την προστασία των δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

Β) Σε περίπτωση ανάπτυξης εφαρμογών, είτε εσωτερικά στον οργανισμό είτε από εξωτερικό συνεργάτη, προβλέπεται διαδικασία ασφαλούς υλοποίησης λογισμικού, ώστε να εντοπισθούν τυχόν ευπάθειες αυτού ως προς την ασφάλεια προτού αυτό μεταβεί σε λειτουργική φάση. Στις περιπτώσεις όπου η ανάπτυξη των εφαρμογών γίνεται από εξωτερικό συνεργάτη, υπάρχουν προδιαγραφές ασφαλείας της εφαρμογής στο έγγραφο περιγραφής απαιτήσεων λογισμικού, το οποίο εμπεριέχεται στη σύμβαση με τον εκάστοτε ανάδοχο.

Γ) Τα λειτουργικά αρχεία των συστημάτων (system files), τα δεδομένα ελέγχου συστημάτων (system test data), καθώς και ο πηγαίος κώδικας (source code) των προγραμμάτων λογισμικού ελέγχονται και προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση.

7. Διαχείριση αλλαγών

Α) Η WIDE Services έχει ορίσει σαφή πολιτική διαχείρισης όλων των αλλαγών που πραγματοποιούνται στα πληροφοριακά συστήματα, η οποία περιέχει: καταγραφή των

αιτημάτων αλλαγής, καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών, καθορισμό των κριτηρίων αποδοχής της αλλαγής και χρονοδιάγραμμα υλοποίησης.
Β) Για όλες τις πλατφόρμες η WIDE Services πραγματοποιεί δοκιμές των ενημερώσεων λογισμικού, τόσο σε επίπεδο επιμέρους εφαρμογών όσο και σε επίπεδο λειτουργικού συστήματος, σε δοκιμαστικό περιβάλλον. Η ανάπτυξη λογισμικού γίνεται σε δοκιμαστικό περιβάλλον, το οποίο είναι απομονωμένο από το παραγωγικό σύστημα και επικαιροποιημένο. Κατά την ανάπτυξη ή αναβάθμιση λογισμικού και τη δοκιμή του, χρησιμοποιούνται δοκιμαστικά και όχι πραγματικά δεδομένα ή δεδομένα του παραγωγικού συστήματος, εκτός εάν κάτι τέτοιο είναι απολύτως απαραίτητο και δεν υπάρχει εναλλακτική λύση. Αν είναι αναγκαίο χρησιμοποιούνται πραγματικά δεδομένα σε ανωνυμοποιημένη μορφή ή διαφορετικά περιορίζονται στα απολύτως απαραίτητα για τους σκοπούς του ελέγχου.

Διοικητικά μέτρα

1. Εφαρμογή ISO 27001:2013 και ISO 9001:2015

Η WIDE Services εφαρμόζει από το 2016 ISO 9001:2015 και από το 2017 ISO 27001:2013 για την ποιότητα των υπηρεσιών της και την ασφάλεια των πληροφοριών. Επιπλέον έχει αναπτύξει επιπλέον πολιτικές σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, τις οποίες τις έχει εντάξει στην εφαρμογή του ISO 27001:2013

2. Ορισμός DPO

Η WIDE Services διαθέτει εσωτερικό DPO, ο οποίος είναι πιστοποιημένος από την TUV Austria και έχει κοινοποιηθεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Αρμοδιότητες του είναι η συνεχής παρακολούθηση της συμμόρφωσης της εταιρείας με το νόμο 4624/2019 για την προστασία προσωπικών δεδομένων, που ενσωματώνει τον ΓΚΠΔ.

3. Έλεγχος πρόσβασης

Α) Η WIDE Services διαθέτει συγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών των χρηστών, οι οποίες περιλαμβάνουν διαδικασίες για την προσθήκη, μεταβολή ιδιοτήτων και διαγραφή τους. Σε κάθε χρήστη αποδίδεται διαφορετικός λογαριασμός πρόσβασης με διαφορετικό Username και Password.
Β) Η WIDE Services έχει αναπτύξει μηχανισμούς που δεν επιτρέπουν προσβάσεις σε πόρους/εφαρμογές/αρχεία από μη εξουσιοδοτημένους χρήστες: ουσιαστικά, διαθέτει κατάλληλα μέτρα που εξασφαλίζουν την εγγυημένα ορθή ταυτοποίηση και αυθεντικοποίηση των χρηστών, ενώ ταυτοχρόνως γίνεται σε τεχνικό επίπεδο συγκεκριμένη εκχώρηση δικαιωμάτων/εξουσιοδοτήσεων σε κάθε χρήστη.
Γ) Η WIDE Services διαθέτει συγκεκριμένη πολιτική διαχείρισης των συνθηματικών των χρηστών, η οποία περιλαμβάνει κανόνες αποδοχής για το ελάχιστο μήκος 8 χαρακτήρων και επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την

ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του. Τα συνθηματικά δεν είναι κάπου καταγεγραμμένα στην πραγματική τους μορφή (ούτε σε φυσικό ούτε σε ηλεκτρονικό αρχείο). Επίσης, οι χρήστες υποχρεώνονται να αλλάζουν οι ίδιοι το (προκαθορισμένο) συνθηματικό που τους ανατίθεται εξαρχής, καθώς επίσης υποχρεώνονται να αλλάζουν το συνθηματικό τους ανά τακτά χρονικά διαστήματα (οπωσδήποτε εντός διαστήματος μικρότερου του ενός έτους).
Δ) Η WIDE Services διαθέτει κατάλληλους μηχανισμούς που απαγορεύουν την πρόσβαση σε έναν εξουσιοδοτημένο χρήστη, μετά από ένα πλήθος επαναλαμβανομένων αποτυχημένων αιτήσεων πρόσβασης (για παράδειγμα, υποβολή λανθασμένων συνθηματικών). Για έναν τέτοιο χρήστη, επανεξετάζεται η εξουσιοδότησή του για να έχει δικαίωμα πρόσβασης.

4. Πολιτικές

Η WIDE Services έχει αναπτύξει πολιτικές ασφάλειας, κατευθυντήριες οδηγίες και διαδικασίες για την προστασία των πληροφοριακών αγαθών και των σχετικών συστημάτων, οι οποίες να επεκτείνονται και σε προμηθευτές υπηρεσιών και αγαθών, καθώς και σε παρόχους υπηρεσιών νέφους (cloud).

5. Συμβάσεις εμπιστευτικότητας

Η WIDE Services έχει συνάψει συμβάσεις εμπιστευτικότητας με το προσωπικό, τους προμηθευτές και τους εξωτερικούς συνεργάτες για τη διασφάλιση της ασφάλεια των πληροφοριών.

6. Εκπαίδευση προσωπικού

Η WIDE Services έχει δημιουργήσει και υλοποιεί σε τακτική βάση προγράμματα ευαισθητοποίησης του προσωπικού και διαμόρφωσης κουλτούρας ασφάλειας (security awareness training) σε θέματα ασφάλειας πληροφοριών ISMS αλλά και θέματα σχετικά με τον ΓΚΠΔ. Εκτός από την εσωτερική εκπαίδευση, η WIDE Services έχει αναπτυγμένη την κουλτούρα να παρέχει εξειδικευμένη εκπαίδευση στο προσωπικό, σχετικά με τις υποχρεώσεις επεξεργασίας δεδομένων και τον εντοπισμό παραβάσεων.

7. Αντιμετώπιση περιστατικών

Η WIDE Services έχει αναπτύξει σχέδιο αντιμετώπισης περιστατικών (incidence response plan), το οποίο περιλαμβάνει σαφείς ρόλους και ενέργειες και δοκιμάζεται σε περιοδική βάση.

8. Φυσική ασφάλεια

Η WIDE Services εφαρμόζει μέτρα προστασίας και ανάκαμψης από φυσικές και περιβαλλοντικές απειλές (διαταραχή ηλεκτροδότησης, πλημμύρες, πυρκαγιές κ.λπ.).Επίσης έχει αναπτύξει πολιτικές για το προσωπικό να κλειδώνουν τα έγγραφά τους σε ασφαλή ερμάρια και να καταστρέφουν ευαίσθητες εκτυπωμένες πληροφορίες

που πλέον δεν χρειάζονται μέσω κάδου εμπιστευτικών εγγράφων ή καταστροφέων, πολιτική καθαρού γραφείου και οθόνης.

9. Χρήση ιδίων συσκευών
Η WIDE Services έχει αναπτύξει πολιτικής BYOD (Bring Your Own Device) σχετικά με την αδειοδότηση για τη χρήση προσωπικών συσκευών για εργασία. Αυτή θα πρέπει να γίνεται σε ελεγχόμενο περιβάλλον.

10. Χρήση Email
Η WIDE Services εφαρμόζει αυστηρή απαγόρευση χρήσης προσωπικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από τον εταιρικό λογαριασμό.

11. Χρήση Wi-Fi
Ο κωδικός του Wi-Fi διατηρείτε εμπιστευτικά και γίνεται τακτική αλλαγή του για την αποφυγή δημιουργίας σημείων πρόσβασης «Κακών Διδύμων» Wi-Fi.

12. Χρήση διαδικτύου
Η WIDE Services εφαρμόζει φιλτράρισμα διαδικτυακού περιεχομένου για την παρεμπόδιση πρόσβασης σε επικίνδυνες διευθύνσεις URL.

Οι μηχανισμοί προστασίας των εκπαιδευτικών συστημάτων της WIDE Services που υλοποιούν τη συμμόρφωση με τον GDPR

Κρυπτογραφημένη βάση δεδομένων: Η βάση δεδομένων του συστήματος είναι κρυπτογραφημένη και επιπλέον δεν μπορεί να αντιγραφεί καθώς δεν βρίσκεται τοπικά σε κάποιον υπολογιστή του πελάτη.

Κρυπτογραφημένη επικοινωνία: Η επικοινωνία με το σύστημα και η μεταφορά δεδομένων είναι πλήρως κρυπτογραφημένη.

Πρόσβαση στο σύστημα μέσω ζεύγους κλειδιών (username / password): Κάθε χρήστης διαθέτει το δικό του μοναδικό συνδυασμό χρήστη/κλειδιού για να έχει πρόσβαση στην εφαρμογή.

Ορισμός χρόνου ζωής των κλειδιών - Βαθμός πολυπλοκότητας κλειδιών: Ορίζεται στην εφαρμογή, ο χρόνος ζωής ενός κλειδιού, πέραν του οποίου το κλειδί δεν

έχει ισχύ και ο χρήστης δεν έχει πρόσβαση στην εφαρμογή (απενεργοποιείται).

Διαβαθμισμένη πρόσβαση σε πληροφορίες και δεδομένα: Ο κάθε χρήστης έχει πρόσβαση μόνο στα δεδομένα τα οποία αφορούν την εργασία του.

Διαβαθμισμένη πρόσβαση σε ευρετήρια και λίστες: Ο κάθε χρήστης έχει πρόσβαση μόνο σε προκαθορισμένα ευρετήρια και λίστες.

Διαβαθμισμένη πρόσβαση σε στοιχεία εκπαιδευτών και εκπαιδευόμενων: Υπάρχουν πεδία και πληροφορίες που μπορούν να είναι μη ορατά σε ομάδες χρηστών.

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

Καταγραφή (Logging): Καταγραφή (Logging) των μεταβολών στα προσωπικά δεδομένα, η οποία θα επεκτείνεται συνεχώς στο μέλλον ώστε να γνωρίζετε ποιος χρήστης έκανε τι.

Δικαίωμα στη φορητότητα. Παραγωγή εκτύπωσης ή αρχείου σε οποιαδήποτε μορφή με το σύνολο των προσωπικών και ευαίσθητων δεδομένων φυσικού προσώπου.

IP lock ανά χρήστη: Παρέχεται η δυνατότητα κλειδώματος της πρόσβασης στην εφαρμογή μόνο από συγκεκριμένη IP διεύθυνση ή εύρος διευθύνσεων.

Ρόλοι χρηστών: Δυνατότητα διαβάθμισης των χρηστών της εφαρμογής (ανάλογα με τις ανάγκες του πελάτη) ώστε να βλέπουν μόνο την πληροφορία για την οποία έχουν ανάλογη εξουσιοδότηση. Απαγόρευση κάθε είδους επεξεργασίας (προβολή, εκτύπωση, τροποποίηση) ευαίσθητων και προσωπικών δεδομένων φυσικών προσώπων από μη εξουσιοδοτημένους χρήστες του συστήματος.

Ευαίσθητα προσωπικά δεδομένα: Απαγόρευση της εμφάνισης ευαίσθητων προσωπικών δεδομένων σε όλα τα Reports, ανάλογα με το επίπεδο διαβάθμισης χρήστη / πληροφορίας.

Διαγραφή προσωπικών δεδομένων: Δυνατότητα πλήρους διαγραφής των

προσωπικών δεδομένων ενός χρήστη, εκτός αυτών φυσικά που επιβάλλονται από τη νομοθεσία και τους κανόνες λειτουργίας του οργανισμού.

Το Cloud – Microsoft Azure

Όλα τα δεδομένα του eLearning περιβάλλοντος, καθώς και όλες οι πληροφορίες που καταχωρεί ο κάθε πελάτης σε αυτό αποθηκεύονται στο Cloud της Microsoft, το Azure.

Το Microsoft Azure είναι ένα από τα πλέον σύγχρονα κέντρα δεδομένων στον πλανήτη σήμερα, που εμπιστεύονται χιλιάδες οργανισμοί που διαχειρίζονται ιδιαίτερα κρίσιμα και ευαίσθητα δεδομένα όπως: Τράπεζες, Κυβερνητικοί Οργανισμοί, Ασφαλιστικές Εταιρείες, Οργανισμοί Υγείας, Τηλεπικοινωνιακοί Φορείς κλπ.

Το Microsoft Azure παρέχει μοναδική ασφάλεια σε θέματα απώλειας δεδομένων. Τα πάντα βρίσκονται σε 2 διαφορετικές τοποθεσίες με αυτόματη μετάβαση στην δεύτερη αν συμβεί κάτι στην πρώτη, χωρίς την παραμικρή απώλεια και με πλήρη redundancy του υλικού μέρους: Δίσκοι, μνήμες, CPU κλπ είναι πολλαπλά. Συγχρόνως η WIDE Services εφαρμόζει αυστηρό backup policy σύμφωνα με τις ανάγκες κάθε έργου.

Η ασφάλεια και προστασία δεδομένων, η διαφάνεια και η ακεραιότητα Δεδομένων (data sovereignty), παρέχονται από την πλατφόρμα Microsoft Azure, χρησιμοποιώντας το Security Development Lifecycle (SDL), από τον αρχικό σχεδιασμό ως την δρομολόγηση της λύσης.

Διεθνείς Πιστοποιήσεις Συμμόρφωσης

Μαζί, η τεχνολογία με ενισχυμένη ασφάλεια και οι αποτελεσματικές διαδικασίες συμμόρφωσης επιτρέπουν στην Microsoft να διατηρήσει και να επεκτείνει ένα πλούσιο σύνολο των πιστοποιήσεων από τρίτους. Ως μέρος της δέσμευσής της για διαφάνεια, η Microsoft μοιράζεται τα αποτελέσματα των πιστοποιήσεων από τρίτους με τους πελάτες της και τις παραθέτουμε στη συνέχεια.

Πιστοποιήσεις και βεβαιώσεις. Το Azure συναντά μια ευρεία σειρά από διεθνή και τοπικά καθώς και ειδικά βιομηχανικά πρότυπα συμμόρφωσης, όπως το **ISO 27001**, **FedRAMP**, **SOC 1** και **SOC 2**. Η συμμόρφωση του Azure στους αυστηρούς ελέγχους ασφαλείας που περιέχονται σε αυτά τα πρότυπα επαληθεύεται από ακριβείς ελέγχους από τρίτους που αποδεικνύουν ότι οι υπηρεσίες του Azure πληρούν βιομηχανικά

πρότυπα παγκόσμιας κλάσης, πιστοποιήσεις, βεβαιώσεις και άδειες.

Ολοκληρωμένη, ανεξάρτητα επικυρωμένη συμμόρφωση. Το Azure έχει σχεδιαστεί με μια στρατηγική συμμόρφωσης που βοηθά τους πελάτες να αντιμετωπίζουν επιχειρηματικούς στόχους και βιομηχανικά πρότυπα και κανονισμούς. Το πλαίσιο συμμόρφωσης ασφαλείας περιλαμβάνει φάσεις δοκιμών και ελέγχων, security analytics, βέλτιστες πρακτικές διαχείρισης κινδύνου και security benchmark analysis για να επιτευχθούν τα πιστοποιητικά και οι βεβαιώσεις. Το Microsoft Azure προσφέρει τις ακόλουθες πιστοποιήσεις:

- **CDSA.** Το Content Delivery and Security Association παρέχει προστασία περιεχομένου και το πρότυπο (CPS) Ασφαλείας για τη συμμόρφωση με τις διαδικασίες αντι-πειρατείας που διέπουν τα ψηφιακά μέσα. Το Azure πέρασε τον έλεγχο CDSA, επιτρέποντας ασφαλείς ροές εργασίας για την ανάπτυξη και τη διανομή περιεχομένου.
- **CJIS.** Κάθε πολιτεία της Αμερικής και κάθε τοπική υπηρεσία που θέλει να έχει πρόσβαση στην βάση δεδομένων της υπηρεσίας πληροφοριών ποινικής Δικαιοσύνης (CJIS) του FBI, απαιτείται να συμμορφώνονται με την Πολιτική Ασφαλείας CJIS. Το Azure είναι ο μόνος cloud πάροχος που δεσμεύεται να συμμορφωθεί με την πολιτική ασφαλείας CJIS.
- **CSA CCM.** Η Cloud Security Alliance (CSA) είναι ένας μη κερδοσκοπικός οργανισμός, με αποστολή την προώθηση της χρήσης των βέλτιστων πρακτικών για την παροχή ασφάλειας μέσα στο σύννεφο. Το CSA Cloud Controls Matrix (CCM) παρέχει λεπτομερείς πληροφορίες σχετικά με το πώς το Azure πληροί την ασφάλεια, την ιδιωτικότητα, τη συμμόρφωση, και τις απαιτήσεις διαχείρισης κινδύνου που ορίζονται στην 1.2 CCM έκδοση και δημοσιεύεται στο CSA's Security Trust and Assurance Registry (STAR).
- **EU Model Clauses.** Η Microsoft παρέχει στους πελάτες της το EU Standard Contractual Clauses, εγγυήσεις για την μεταβίβαση των προσωπικών τους δεδομένων εκτός Ευρώπης. Η Microsoft είναι η πρώτη εταιρεία που λαμβάνει κοινή έγκριση από το EU's Article 29 Working Party. Αυτό εξασφαλίζει ότι οι πελάτες του Azure μπορούν να χρησιμοποιούν τις υπηρεσίες της Microsoft για να μετακινήσουν τα δεδομένα τους ελεύθερα μέσα από το cloud από την Ευρώπη προς τον υπόλοιπο κόσμο.
- **FERPA.** Ο νόμος Family Educational Rights and Privacy Act (FERPA) – Νόμος για τα οικογενειακά εκπαιδευτικά δικαιώματα και ιδιωτικότητα - είναι μια

ομοσπονδιακή νομοθεσία των Η.Π.Α. που προστατεύει τα εκπαιδευτικά δεδομένα των μαθητών. Η Microsoft συμφωνεί να χρησιμοποιεί και να δημοσιοποιεί τους περιορισμούς που επιβάλλονται από τον FERPA.

- **FIPS 140-2.** Το Azure συμμορφώνεται με το Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών (FIPS) Δημοσίευση 140-2, ένα κυβερνητικό πρότυπο των ΗΠΑ που καθορίζει ένα ελάχιστο σύνολο απαιτήσεων ασφάλειας για τα προϊόντα και τα συστήματα που εφαρμόζουν κρυπτογράφηση.
- **ISO/IEC 27018.** Η Microsoft είναι ο πρώτος cloud πάροχος που έχει υιοθετήσει το πρότυπο ISO/IEC 27018, το οποίο καλύπτει την επεξεργασία των προσωπικών πληροφοριών από παρόχους cloud υπηρεσιών.
- **ISO/IEC 27001/27002:2013.** Το Azure συμμορφώνεται με αυτό το πρότυπο το οποίο καθορίζει τους ελέγχους ασφαλείας που απαιτούνται από ένα σύστημα διαχείρισης πληροφοριών.
- **PCI DSS.** Το Azure παρέχει επιπέδου 1 συμβατότητα με τα πρότυπα ασφάλειας δεδομένων καρτών πληρωμών - Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0 - το παγκόσμιο πρότυπο πιστοποίησης για τους οργανισμούς που δέχονται κάρτες πληρωμών, καθώς και την αποθήκευση, επεξεργασία ή μετάδοση δεδομένων του κατόχου της κάρτας.
- **SOC 1 και SOC 2.** Το Azure έχει ελεγχθεί από την Υπηρεσία Ελέγχου Οργανισμού (SOC) και για τα δύο πλαίσια SOC 1 Type 2 and SOC 2 Type 2. Και οι δύο εκθέσεις είναι διαθέσιμες στους πελάτες για να πληρούν ένα ευρύ φάσμα διεθνών απαιτήσεων. Ο SOC 1 Type 2 έλεγχος βεβαιώνει για το σχεδιασμό και την αποτελεσματική λειτουργία του Azure ελέγχου. Ο SOC 2 Type 2 έλεγχος περιλαμβάνει περαιτέρω εξέταση των ελέγχων του Azure που σχετίζονται με την ασφάλεια, τη διαθεσιμότητα και την εμπιστευτικότητα.
- TCS CCCPPF
- UK G-Cloud
- MLPS
- MTCS
- HIPAA
- IRAP
- FDA 21 CFR Part 11.
- FedRAMP

Το Microsoft Azure χρησιμοποιεί πολλαπλές διασφαλίσεις για την προστασία των

δεδομένων των πελατών και των επιχειρήσεων. Αυτές οι πρακτικές και τεχνολογίες ασφάλειας περιλαμβάνουν:

- **Identity and access management** – Το Azure Active Directory βοηθά στο να διασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα και την πλατφόρμα σας, και παρέχει multi-factor πιστοποίηση για εξαιρετικά ασφαλή σύνδεση.
- **Encryption** – Το Azure χρησιμοποιεί βιομηχανικά πρότυπα πρωτοκόλλων (industry-standard protocols) για την κρυπτογράφηση των δεδομένων καθώς ταξιδεύουν μεταξύ των συσκευών και των κέντρων δεδομένων της Microsoft.
- **Secure networks** – Azure Virtual Networks extend your on-premises network to the cloud via a site-to-site virtual private network (VPN). Μπορείτε επίσης να χρησιμοποιήσετε ένα ExpressRoute για να δημιουργήσετε μια cross-premises σύνδεση όταν χρειάζεται να χρησιμοποιήσετε το internet.
- **Threat management** – Το Microsoft Antimalware προστατεύει τις Azure υπηρεσίες και τις εικονικές μηχανές (virtual machines). Η Microsoft ακόμα χρησιμοποιεί intrusion detection, denial-of-service (DDoS) attack prevention, penetration testing, data analytics, and machine learning για τη συνεχή ενίσχυση της άμυνας του και τη μείωση των κινδύνων.
- **Compliance** – Το Azure είναι συμμορφωμένο με τα διεθνή και βιομηχανικά-ειδικά πρότυπα και συμμετέχει σε αυστηρούς ελέγχους από τρίτους, οι οποίοι επαληθεύουν τα επίπεδα ασφαλείας του.

Προστασία κατά το σχεδιασμό (Privacy by Design)

- **Κυριότητα δεδομένων**

Ο πελάτης έχει την κυριότητα των δεδομένων του και διατηρεί όλα τα δικαιώματα επ' αυτών.

Εάν κάποιος πελάτης αποφασίσει να σταματήσει τη λήψη της υπηρεσίας, τα δεδομένα του διαγράφονται το αργότερο εντός 180 ήμερων ή όπως ορισθεί στην μεταξύ μας σύμβαση.

- **Όχι για διαφήμιση**

Δεν δημιουργεί προϊόντα διαφήμισης χρησιμοποιώντας δεδομένα πελατών.

Δεν σαρώνει (no scanning) ηλεκτρονικά μηνύματα (email) ή έγγραφα για σκοπούς διαφήμισης.

Στάδια κρυπτογράφησης

Προστασία δεδομένων σε όλα τα στάδια επικοινωνίας.

1. **Δεδομένα υπό διαβίβαση μεταξύ χρήστη και υπηρεσίας**

Προστατεύει το χρήστη από υποκλοπή των επικοινωνιών του και βοηθάει τη διασφάλιση της ακεραιότητας των διαβιβάσεων

2. **Δεδομένα υπό διαβίβαση (in transit) μεταξύ data centers**

Προστατεύει από μαζική υποκλοπή των δεδομένων

3. **Δεδομένα σε αδράνεια (data at rest)**

Προστατεύει από αφαίρεση φυσικών μέσων

4. **Ολοκληρωμένη (end- to-end) κρυπτογράφηση επικοινωνιών μεταξύ χρηστών**

Προστατεύει από υποκλοπή ή απώλεια δεδομένων κατά τη διαβίβαση (data in transit) μεταξύ των χρηστών

Διαφάνεια για τοποθεσία δεδομένων

Πού αποθηκεύονται τα δεδομένα;

- Πιστοποιημένα data centers της Microsoft στην Ευρώπη.
- Παρέχονται ξεκάθαρες πληροφορίες για τη «χαρτογράφηση» και τα γεωγραφικά όρια των δεδομένων.
- Δέσμευση για τα δεδομένα σε αδράνεια (data at rest) να παραμένουν στην Ευρώπη.

Ασφάλεια υποδομών

Οι υποδομές του Azure περιλαμβάνουν υλικό, λογισμικό, δίκτυα, διοικητικό και λειτουργικό προσωπικό, και τα φυσικά κέντρα δεδομένων (data centers) που τα στεγάζουν όλα.

Φυσική ασφάλεια. Το Azure τρέχει σε γεωγραφικά κατανεμημένες εγκαταστάσεις της Microsoft, που μοιράζονται χώρο και λειτουργίες με άλλες online υπηρεσίες της Microsoft**.** Κάθε εγκατάσταση έχει σχεδιαστεί για να τρέχει 24x7x365 και χρησιμοποιεί διάφορα μέτρα για την προστασία από διακοπές ενέργειας, φυσικές εισβολές και διακοπές του δικτύου. Αυτά τα κέντρα δεδομένων συμμορφώνονται με βιομηχανικά πρότυπα (όπως ISO 27001) για τη σωματική ασφάλεια και τη διαθεσιμότητα.

Παρακολούθηση και καταγραφή. Με κεντρική παρακολούθηση καθώς και με συστήματα συσχέτισης και ανάλυσης γίνεται η διαχείριση του μεγάλου όγκου των

πληροφοριών που παράγονται από συσκευές μέσα στο περιβάλλον του Azure, παρέχοντας συνεχή προβολή και έγκαιρες προειδοποιήσεις προς τις ομάδες που διαχειρίζονται την υπηρεσία. Πρόσθετη παρακολούθηση, δυνατότητες καταγραφής και αναφοράς παρέχουν ορατότητα προς τους πελάτες.

Περίμετρος	**Κτήρια**	**Αίθουσες Υπολογιστών**
Προσωπικό ασφαλείας όλο το 24ωρο.	Συναγερμοί	Έλεγχος πρόσβασης δύο παραγόντων: βιομετρικός και καρτών ανάγνωσης (card readers)
Εγκαταστάσεις με προδιαγραφές για οπουδήποτε υποτροπή	Κέντρο λειτουργιών ασφαλείας	Κάμερες
Εμπόδια	Σεισμική αντιστήριξη	Εφεδρική ενέργεια πολλών ημερών
Περίφραξη	Κάμερες ασφαλείας	

- **Ποιος έχει πρόσβαση και τι είδους;**

Πρόσβαση μόνο για λόγους επίλυσης προβλημάτων (troubleshooting) και πρόληψης κατά ιών (malware).
Πρόσβαση περιορισμένη μόνο στο αναγκαίο προσωπικό (key personnel) σε εξαιρετικές περιπτώσεις.

Backup Δεδομένων

Τα backup δεδομένα σας αποθηκεύονται σε γεωγραφικά κατανεμημένα δίκτυα (geo-replicated) αποθήκευσης, τα οποία διατηρούν αντίγραφα των δεδομένων σας σε δύο Azure datacenters.

Προστασία Δεδομένων

Το Azure διασφαλίζει τα δεδομένα των πελατών χρησιμοποιώντας τρεις συγκεκριμένες μεθόδους: Κρυπτογράφηση, διαχωρισμό και καταστροφή.

Απομόνωση Δεδομένων. Το Azure είναι μια υπηρεσία ενοικίασης, πράγμα που σημαίνει ότι τα δεδομένα πολλών πελατών αλλά και εικονικών μηχανών είναι αποθηκευμένα στον ίδιο εξοπλισμό.

Data redundancy. Οι πελάτες έχουν την δυνατότητα να επιλέξουν την αποθήκευση εντός της χώρας for compliance or latency considerations ή την αποθήκευση εκτός της χώρας με σκοπό την ανάκτηση δεδομένων για ασφάλεια ή σε περιπτώσεις καταστροφής. Τα δεδομένα μπορούν να αντιγραφούν μέσα σε μια επιλεγμένη γεωγραφική περιοχή για πλεονασμό.

Καταστροφή Δεδομένων. Όταν οι πελάτες διαγράφουν δεδομένα ή φύγουν από το Azure, η Microsoft ακολουθεί αυστηρά πρότυπα για την αντικατάσταση των πόρων αποθήκευσης πριν επαναχρησιμοποιηθούν. Ως μέρος της συμφωνίας μας για την cloud υπηρεσία μας, είμαστε δεσμευμένοι σε συγκεκριμένες διαδικασίες για τη διαγραφή των δεδομένων.

Διαχείριση αναβαθμίσεων. Η ασφάλεια διαχείρισης αναβαθμίσεων βοηθά στην προστασία των συστημάτων από γνωστές αδυναμίες. Το Azure χρησιμοποιεί ολοκληρωμένα συστήματα ανάπτυξης για τη διαχείριση τη διανομή και την εγκατάσταση των ενημερώσεων ασφαλείας για το λογισμικό της Microsoft. Το Azure χρησιμοποιεί έναν συνδυασμό εργαλείων σάρωσης της Microsoft αλλά και τρίτων κατασκευαστών, για να σαρώνει λειτουργικά, διαδικτυακές εφαρμογές αλλά και βάσεις δεδομένων σε όλο το περιβάλλον του Azure.
Antivirus και Antimalware. Τα στοιχεία του λογισμικού του Azure θα περάσουν από μια σάρωση για ιούς πριν αναπτυχθούν. Ο κώδικας δεν προχωράει στην παραγωγή αν δεν γίνει πρώτα μια καθαρή και πετυχημένη σάρωση

DDoS προστασία. Το Azure έχει ένα σύστημα άμυνας κατά των Distributed Denial-of-Service επιθέσεων στις υπηρεσίες του. Χρησιμοποιεί πρότυπα ανίχνευσης και τεχνικές άμβλυνσης. Το αμυντικό σύστημα Azure DDoS είναι σχεδιασμένο να αντέχει τις επιθέσεις που παράγονται μέσα και έξω από την πλατφόρμα.

Υπεργολάβοι

Επωνυμία Υπεργολάβου	**Διεύθυνση δραστηριότητας υπεργολάβου**	**Ημερομηνία Σύμβασης με Υπεργολάβο**	**Δραστηριότητα που έχει ανατεθεί**	**Υπεύθυνος Επικοινωνίας για θέματα προσωπικών δεδομένων**

Mirosoft			Microsoft Azure Data Center (εντός της Ε.Ε.)	