

# ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ :ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ :ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

**Τίτλος Εργασίας** : **Ανάπτυξη ηλεκτρονικού portal ενημέρωσης και εκπαίδευσης για τις τεχνολογίες IoT και τις εφαρμογές τους**

**Όνομα φοιτητή** :**ΜΑΥΡΟΥΔΗΣ ΤΡΥΦΩΝΑΣ**

Αθήνα,2022



# HAROKOPIO UNIVERSITY

SCHOOL : HAROKOPIO UNIVERSITY

DEPARTMENT : INFORMATICS AND TELEMATICS

**Title : Developing an information portal for IoT technologies and applications**

**Student's Name: MAVROUDIS TRYFONAS**

Athens,2022

Ανάπτυξη ηλεκτρονικού portal ενημέρωσης και εκπαίδευσης για τις τεχνολογίες IoT και τις εφαρμογές τους./ΜΑΥΡΟΥΔΗΣ ΤΡΥΦΩΝΑΣ



# ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ :ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ :ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

**Τριμελής Εξεταστική Επιτροπή**


**ΚΛΕΟΠΑΤΡΑ ΜΠΑΡΔΑΚΗ**

Επίκουρη Καθηγήτρια στο γνωστικό αντικείμενο Πληροφοριακά Συστήματα Διάχυτου Υπολογισμού και Συστήματα Εφοδιαστικής Αλυσίδας

**ΜΙΧΑΛΑΚΕΛΗΣ ΧΡΗΣΤΟΣ**

Αναπληρωτής Καθηγητής στο γνωστικό αντικείμενο Τεχνοοικονομική Ανάλυση Δικτύων Επικοινωνιών και Πληροφοριακών Συστημάτων

**ΤΣΑΔΗΜΑΣ ΑΝΑΡΓΥΡΟΣ**

Ε.ΔΙ.Π. του Τμήματος Πληροφορικής και Τηλεματικής



Ανάπτυξη ηλεκτρονικού portal ενημέρωσης και εκπαίδευσης για τις τεχνολογίες IoT και τις εφαρμογές τους./ΜΑΥΡΟΥΔΗΣ ΤΡΥΦΩΝΑΣ

Ο ΜΑΥΡΟΥΔΗΣ ΤΡΥΦΩΝΑΣ

δηλώνω υπεύθυνα ότι:

**1)** Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

**2)** Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

**3)** Όπου υφίστανται δικαιώματα άλλων δημιουργών έχουν διασφαλιστεί όλες οι αναγκαίες άδειες χρήσης ενώ το αντίστοιχο υλικό είναι ευδιάκριτο στην υποβληθείσα εργασία.

# ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω όλους του καθηγητές που γνώρισα και συναναστράφηκα στην πορεία μου στο Χαροκόπειο Πανεπιστήμιο, καθώς ο καθένας ξεχωριστά βοήθησε με τον δικό του μοναδικό τρόπο, είτε μέσα από απαιτητικά projects, είτε με την αυστηρή βαθμολόγηση, να οριοθετηθεί ο δρόμος που θέλω να ακολουθήσω στην επαγγελματική μου πορεία που τώρα ξεκινά.

Ιδιαίτερες ευχαριστίες στην κυρία Μπαρδάκη κάθως πέρα από τη βαθιά γνώση του αντικειμένου που διδάσκει, έχει το χάρισμα να μεταλαμπαδεύει αυτή τη γνώση στους φοιτητές της, χρησιμοποιώντας μεθόδους που μεταβάλλονται με βάση την προσωπικότητα του καθενός μας, με στόχο πάντα, το βέλτιστο αποτέλεσμα. Πέρα από τον συμβουλευτικό της ρόλο στην αποπεράτωση της πτυχιακής μου, με έμαθε να διαχειρίζομαι με σύνεση καταστάσεις και κρίσεις που θα συναντήσω στην επαγγελματική μου ζωή, είτε στο πεδίο της πληροφορικής ή σε οποιονδήποτε επαγγελματικό χώρο επιλέξω να εργαστώ.

# ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ


**ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ** 5

**Εισαγωγή** 9

**1.ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ** 10

**1.1 Portals** 10

**1.2 Internet Of Things** 11

**1.3 Σύντομη Ιστορία Internet of Things** 13

Πραγματοποίηση της Ιδέας 13

Αρχές της δεκαετίας του 2000 14

IoT Getting Smarter 14

Το Industrial Internet of Things (IIoT) 15

Το Διαδίκτυο των Πραγμάτων γίνεται μέρος της ζωής 15

Το IoT πάει Mobile – 2015 16

**1.4 Εργαλεία Ανοιχτού Λογισμικού και Wordpress** 16

**2. ΔΙΑΔΙΚΑΣΙΑ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΑΝΑΠΤΥΞΗΣ** 19

**2.1 Εγκατάσταση Wordpress σε localhost.** 19

**2.2 Μεταφορά σε online host.** 22

**2.3Σχεδίαση Βασικής Δομής και Περιεχομένου.** 24

**2.4 Προσαρμογή Εμφάνισης.** 26

**2.5 Προσθήκη Περιεχομένου.** 28

2.5.1Ελαχιστοποίηση ρίσκου και απορρήτου εφαρμογών στο IoT 29

2.5.2 Hardware και projects στο IoT 45

2.5.3 Οδηγός GDPR και IoT 56

2.5.4 IoT και edge computing 69

2.5.5 Απόρρητο εφαρμογής και IoT 74

**2.6 Πρόσθετες δυνατότητες.** 89

**2.7 Βάση δεδομένων.** 92

**3. Αξιολόγηση.** 96

**3.1 Βελτίωση.** 98

**4.Συμπερασματα Περιορισμοί και Επόμενα βήματα** **103**

# Περίληψη στα Ελληνικά

Ο σκοπός της παραπάνω πτυχιακής είναι να δημιουργηθεί ένα e-portal απο το οποίο ο χρήστης θα μπορεί να αντλήσει πληροφορίες για το IoT ανεξαρτήτως απο το επίπεδο εμπειρίας του.Αυτό που προσπαθούμε να πετύχουμε με την παραπάνω υλοποίηση είναι να συγκεντρώσουμε οσο το δυνατόν περισσότερες πληροφορίες σε ενα σημείο αλλα παραλληλα να παρέχουμε την δυνατότητα στον χρήστη μέσω υπερ-συνδέσμων να μπορεί να εμβαθύνει οσο επιθυμεί στο θέμα που τον ενδιαφέρει.Επιπρόσθετα θα προσπαθήσουμε να κρατήσουμε τον χρήστη ενεργό στο site δινοντάς του την δυνατότητα να αλληλεπιδρά με άλλους χρήστες γύρω απο κοινα θέματα αλλά δίνοντας του την ευκαιρία να παρακολουθήσει σημαντικά events στο χώρο του IoT καθώς και την ευελιξία να δηλώσει ενδιαφέρον για θέσεις εργασίας, όλα στον ίδιο χώρο.Η διαδικασία που θα ακολουθήσουμε αποτελείται από 3 βασικά στοιχεία.Θα πραγματοποιηθεί έρευνα γύρω από τις ήδη υπάρχον ιστοσελίδες που προσφέρουν παρόμοια πληροφορία ,μετά θα δημιουργηθεί ένα site ‘σκελετός’ με βασικές πληροφορίες και δυνατότητες που θεωρούμε ότι πρέπει να διέπουν ενα portal και έπειτα θα σταλεί για αξιολόγηση σε στοχευμένο κοινό.Τέλος θα δράσουμε πάνω στις απαντήσεις των χρηστών βελτιωνοντας την εμπειρία χρήστη και την ευρυτερη λειτουργία του portal. Το αποτέλεσμα θα είναι ένα portal το οποίο θα παρέχει δυνατότητες που δεν υπάρχουν αυτην την στιγμη συγκεντρωμένες σε παρόμοια site και θα παρέχει την δυνατότητα για περαιτέρω εξέλιξη.

**Λέξεις κλειδιά:** IoT,υπερ-συνδέσμοι,portal,θέσεις εργασίας , events.

# Abstract ή Περίληψη στα Αγγλικά

The purpose of the above thesis is to create an e-portal from which the userinformation about IoT regardless of the user's level of experience.What we are trying to achieve with the above implementation is to gather as much information as possible in one place but at the same time provide the possibility for the user through hyperlinks to be able to go as deep as he wishes into the subject In addition, we will try to keep the user active in the site by giving him the opportunity to interact with other users around common topics but also giving him the opportunity to follow important events in the IoT field as well as the flexibility to register interest in jobs, all in the same place.The process we will follow consists of 3 main elements.existing websites that offer similar information ,then a site 'skeleton' with basic information and features that we believe should govern a portal and then it will be sent out for evaluation to a targeted audience.Finally we will act on user responses to improve the user experience and the broader functionality of the portal.portal. The result will be a portal that provides capabilities that do not exist.currently available on similar sites and will provide the opportunity for further development.

**Keywords**: IoT, informational research, electronic portal.

**ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ**

Εικόνα 1. Αρχεία Wp 17
Εικόνα 2. Σύνδεση στην βάση 18
Εικόνα 3. Σύνδεση Wp 19
Εικόνα 4 Πρώτες εικόνες 20
Εικόνα 5. Online host 21
Εικόνα 6. Ενεργοποιήση Maintenance Mode 22
Εικόνα 7. Αρχική σχεδίαση δομής 24
Εικόνα 8. Προσαμογή εμφάνισής 25
Εικόνα 9. Δημιουργία Slide Show 25
Εικόνα 10. Δομή πληροφοριών 26
Εικόνα 11. Προσθήκη άρθρων 26
Εικόνα 12. Άρθρα 27
Εικόνα 14. Παράδειγμα αλγορίθμου ανωνυμοποίησης αντικατάστασης.....29
Εικόνα 15. Παράδειγμα τυχαίας αναπαραγωγής δεδομένων.....32
Εικόνα 16. Ψευδωνυμοποίηση.....43
Εικόνα 17. Κατακερματισμός κωδικού πρόσβασης.....54
Εικόνα 18. Κατακερματισμός αλατισμένου κωδικού πρόσβασης.....55
Εικόνα 19. Συμμετρική κρυπτογράφηση.....57
Εικόνα 20. Raspberry Pi single-board-computer.....61
Εικόνα 21. Παράδειγμα ροής δεδομένων εφαρμογής.....63
Εικόνα 22. Χρήση τεχνικών προσωπικών δεδομένων εφαρμογής.....64
Εικόνα 23. Μητρώο κινδύνου.....65
Εικόνα 24. Πρωιμη μορφή .....72
Εικόνα 25. Θέσεις εργασίας.....75
Εικόνα 26. Φόρμα επικοινωνίας.....81
Εικόνα 27. Events.....85
Εικόνα 28. Σύνδεση στην online βάση.....89
Εικόνα 29. Πίνακες Wp.....91
Εικόνα 30. Πρώτο μέρος αποτελεσμάτων ερωτηματολογίου.....93
Εικόνα 31. Δεύτερο μέρος ερωτηματολογίου.....94
Εικόνα 32. Εικόνα εξωτερικού με συνδεδεμένου χρήστη.....95
Εικόνα 33. Εικονα εσωτερικού συνδεδεμένου χρήστη.....96

# ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

| | |
|---|---|
| IoT | Internet of things |
| Wp | Wordpress |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| RFID | Radio Frequency Identification |

# Εισαγωγή

Το θέμα της παρακάτω πτυχίακής εργασίας είναι Ανάπτυξη Internet portal σε Wordpress για την ενημέρωση γύρω από το Internet of Things.Συνοπτικά ο βασικός σκοπός της εγασίας ειναι η δημιουργία ενός portal ευκολο προς την χρήση το οποίο θα έχει συγκεντωμένη οσο περισσοτερο δυνατόν πληροφορία την οποία ενας νέος αλλα και ενα έμπειρος χρήστης μπορεί να αξιοποιήσει.Επέλεξα το παραπάνω θέμα επειδή ως νέος φοιτητής έκανα τις πρώτες μου ερευνες τα μονα site που κατεληγα να βρίσκω με πλυμμήριζαν με πληροφορίες χωρίς κανέναν διαδραστικό τρόπο και ουσιαστικά με αποθάρρυναν να συνεχίσω την έρευνα μου.Στοχος λοιπόν ειναι να συγκεντρωσουμε απο αξιοπιστες πηγες οσο το δυνατον περισσοτερες πληροφορίες γυρω απο το IoT και να τις παρουσιάσουμε με τον οσο πιο δυνατό προσιτο τρόπο μπορούμε.

Αρχικά πραγματοποιήθηκε έρευνα για να χτίσουμε ενα θεωριτικό υπόβαθρο το οποίο θα θέσει τα θεμέλια για να ξεκινήσουμε την διαδικασία υλοποιήσης του portal.Αφου ολοκληρωθηκε το πρώτο στάδιο , ξεκινήσε η υλοποίηση του portal.Αφου τελειώσει το λειτουργικό κομματι και είμαστε σε ενα πρωιμο σταδιο αναπτυξης προσθέσαμε βασικα πληροφοριακα περιεχομενα οπως γενικές πληροφορίες και βασικες λειτουργίες για το portal πριν εμβαθύνουμε και προσθέσαμε αρθρα και πληροφορίες σε μεγαλύτερη εκταση.

Αφου ολοκληρώθηκε αυτο το στάδιο μοιράστηκε το site σε ενα επιλεγμένο group απο το οποιο συλλέξαμε πληροφοριές τοσο για την λειτουργια οσο και για τις βελτιώσεις που

μπορεί να χρειάζεται το site.Έπειτα δράσαμε πανω σε αυτα τα στοιχεία που ειχαμε συλλέξει και αναλύσει και καταλήξαμε στο τελικό portal.

Σε όλο αυτο τον ενχείρημα δύο ηταν τα μεγαλύτερα εμπόδια.Ένα ειναι ο χρόνος καθώς υπηρχει πεπερασμένο διαστημα για την υλοποιήση και παρουσίαση του portal αλλα και η προσβασιμότητα σε πόρους καθως οπως και θα δούμε παρακάτω δεν υπηρχε πρόσβαση σε premium συνδρομη σε Host με αποτελεσμα περιορισμενα χαρακτηριστικά οσον αφορα την ταχυτητα και τον χώρο αποθήκευσης.

Τέλος παρουσιάστηκαν επόμενες πιθανές ενέργειες και ιδέες για την βελτίωση και διαχείρηση του portal.

# 1.ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

## 1.1 Portals

Portal είναι μία ιστοσελίδα - πύλη που έχει ένα συγκεκριμένο χαρακτήρα: περιέχει μεγάλη γκάμα περιεχομένου και θεματολογίας για κάτι συγκεκριμένο.Σε αυτού του τύπου την ιστοσελίδα, συγκεντρώνεται και προβάλλεται υλικό είτε από άλλες ιστοσελίδες - πηγές, είτε από τους ιδιοκτήτες του.Το portal έχει γενικά τη φιλοσοφία να παρέχει τα πάντα στους επισκέπτες και δεν επικεντρώνεται σε έναν "συγκεκριμένο χαρακτήρα" θεματολογίας και προβολής περιεχομένου όμως εξυπηρετεί μία συγκεκριμένη μερίδα του κόσμου.Για παράδειγμα μπορεί ένας Δήμος να κάνει ένα τέτοιο ώστε να ενημερώνει τους δημότες του για τον καιρό, τα events, την πορεία των έργων στο Δήμο, τα νέα του, κλπ.Επίσης προτείνει, παραπέμπει και χρησιμοποιεί πολλές φορές άλλες ιστοσελίδες ή υπηρεσίες άλλων, ώστε να έχει μέσα του συγκεντρωμένα τα πάντα.

Με μια απλή αναζήτηση στο Internet μπορούμε εύκολα να εντοπίσουμε ήδη υπάρχοντα portals που αφορούν το θέμα το οποίο θέλουμε να πλαισιώσουμε, δηλαδή portals γύρω απο το IoT.Μερικά απο τα πρώτα που θα αντικρίσουμε είναι το https://theiotportal.com/ το οποίο εμφανίζεται και πρώτο σε μια απλή αναζήτηση.Αν αφιερώσουμε λίγο χρόνο να περιηγηθούμε στον χάρτη του site αμέσως θα παρατηρήσουμε την πληθώρα πληροφοριών που έχει προστεθεί απο τους δημιουργους αλλά και την μεγάλη ποσότητα πληροφορίας που παρέχεται σε υπερ-συνδέσεις.Υπάρχει ένα πλούσιο μενου που καλυπτει οτιδήποτε θα χρειαστει καποιος εμπειρος χρηστης ωστε να βρεί αυτό που ψάχνει.Παραυτα το μεγαλύτερο πλεονέκτημα του είναι επίσης και το μειονέκτημα του.Ένας άπειρος χρήστης μπαίνοντας σε ενα τετοιο portal, βομβαρδίζεται απο πληροφορία και αμέσως

αποθαρρύνεται απο την πλοήγηση σε ένα τέτοιο site καθώς δεν παρέχεται ενα μονοπάτι συνεχως αυξανόμενο ετσι ωστε να μυηει τον χρήστη σταδιακά στην αναζήτηση της πληροφορίας.

Μιας και είναι το μόνο αντιπροσωπευτικό site που μπορέσαμε να βρούμε το οποίο είναι ενα ολοκληρωμένο portal αφιερωμένο στο IoT και οχι απλα μια συλλογή αρθρων όπως τα υπόλοιπα link που εμφανίζονται , αποφασίσαμε να δημιουργήσουμε ενα παρομοιο portal βελτιώνοντας τα προβλήματα τα οποία εντοπίσαμε.

## 1.2 Internet Of Things

Ο όρος Internet of Things αναφέρεται σε ένα δίκτυο διασυνδεδεμένων συσκευών, με τη διασύνδεση να επιτυγχάνεται μέσω της αξιοποίηση τεχνολογίας αισθητήρων, διαδικτύου και cloud. Οι αισθητήρες συλλέγουν δεδομένα τα οποία στη συνέχεια αναλύονται χρησιμοποιώντας μια εφαρμογή που βασίζεται σε cloud για τη λήψη αποφάσεων σε πραγματικό χρόνο. Το IoT έχει δείξει μεγάλες δυνατότητες τόσο για καταναλωτικές όσο και για βιομηχανικές εφαρμογές. Αν και ο όρος Internet Of Things θεωρείται σχετικά πρόσφατος, στην πραγματικότητα η ιδέα του συνδυασμού υπολογιστών και δικτύων για την παρακολούθηση διαφόρων συσκευών δεν ήταν νέα και υπήρχε ήδη πριν από την εμφάνιση της δημοφιλούς ορολογίας. Στην πραγματικότητα, η πρώτη συσκευή που ήταν συνδεδεμένη στο Διαδίκτυο γνωστοποιήθηκε στο κοινό σε ένα συνέδριο που πραγματοποιήθηκε το 1989 και ήταν μια τοστιέρα, συνδεδεμένη στο διαδίκτυο χρησιμοποιώντας μια στοίβα πρωτοκόλλων επικοινωνίας TCP/IP.

Σύμφωνα με τον κοινά αποδεκτό ορισμό το IoT, είναι μια παγκόσμια υποδομή δικτύου, που συνδέει φυσικά και εικονικά αντικείμενα μέσω της εκμετάλλευσης των δυνατοτήτων λήψης δεδομένων και επικοινωνίας. Προσφέρει συγκεκριμένη δυνατότητα αναγνώρισης αντικειμένων, αισθητήρων και διασύνδεσης ως βάση για την ανάπτυξη ανεξάρτητων συνεργαζόμενων υπηρεσιών και εφαρμογών. Στον κόσμο του IoT, έχουμε μια εγγενή προδιάθεση για επαφή με το εξωτερικό περιβάλλον και πολύ γρήγορη επεξεργασία και μετάδοση των σχετικών δεδομένων, που παρέχονται από το περιβάλλον. Στην πραγματικότητα, δεν είναι μόνο ο αυξανόμενος αριθμός συνδεδεμένων συσκευών που μπορεί να αποδειχθεί ότι φτάνει σε εντυπωσιακούς αριθμούς, αλλά και η ίδια η έννοια του IoT που εξελίσσεται λόγω της ικανότητας του IoT να προκαλεί αλλαγές

και να «συγχωνεύεται» με έναν σημαντικό αριθμό περιοχών που αξιοποιούν την τεχνολογία IoT, για παράδειγμα:

- Internet of Mobile Things (IoMT)

- Autonomous Internet of Things (A-IoT)

- Internet of Things Clouds (IoT- C)

- The Internet of Robotics (IoRT)

Όπως γίνεται φανερό, το IoT αποτελεί πλέον μεγάλο κομμάτι τόσο της βιομηχανίας όσο και της καθημερινής ζωής, καθώς βοηθά τους ανθρώπους να ζουν και να εργάζονται πιο έξυπνα και να αποκτούν τον απόλυτο έλεγχο της ζωής τους. Εκτός από την προσφορά έξυπνων συσκευών για την αυτοματοποίηση των σπιτιών, το IoT είναι απαραίτητο για τις επιχειρήσεις. Για το σκοπό αυτό, η ανάπτυξη του ενημερωτικού portal της παρούσας εργασίας κρίνεται απαραίτητη και θα σχεδιαστεί με κατάλληλο τρόπο, ώστε να προσφέρει στους επισκέπτες όλες τις παραπάνω πληροφορίες

## 1.3 Σύντομη Ιστορία Internet of Things

Με απλά λόγια, το Internet of Things αποτελείται από οποιαδήποτε συσκευή με διακόπτη ενεργοποίησης/απενεργοποίησης που είναι συνδεδεμένη στο Διαδίκτυο. Το Internet of Things (IoT) περιλαμβάνει μηχανές που επικοινωνούν πληροφορίες μέσω του Διαδικτύου και είναι σχετικά καινούργια έννοια.
Οι μηχανές παρέχουν άμεσες επικοινωνίες από τότε που αναπτύχθηκε ο τηλέγραφος (το πρώτο σταθερό τηλέφωνο) τη δεκαετία του 1830 και του 1840. Περιγραφόμενη ως «ασύρματη τηλεγραφία», η πρώτη ραδιοφωνική μετάδοση φωνής πραγματοποιήθηκε στις 3 Ιουνίου 1900, παρέχοντας ένα απαραίτητο στοιχείο για την ανάπτυξη του IoT. Η ανάπτυξη των υπολογιστών ξεκίνησε τη δεκαετία του 1950.
Το Διαδίκτυο το ίδιο είναι σημαντικό συστατικό του IoT, ξεκίνησε ως μέρος του DARPA (Defense Advanced Research Projects Agency) το 1962 και εξελίχθηκε σε ARPANET (Advanced Research Projects Agency Network) το 1969.
Στη δεκαετία του 1980, οι πάροχοι εμπορικών υπηρεσιών άρχισαν να υποστηρίζουν τη δημόσια χρήση του ARPANET, επιτρέποντάς του να εξελιχθεί στο σύγχρονο Διαδίκτυό μας. Οι δορυφόροι και τα σταθερά τηλέφωνα παρέχουν βασικές επικοινωνίες για μεγάλο μέρος του IoT.

Οι Παγκόσμιοι Δορυφόροι Εντοπισμού Θέσης (GPS) έγιναν πραγματικότητα στις αρχές του 1993, με το Υπουργείο Άμυνας να παρέχει ένα σταθερό, εξαιρετικά λειτουργικό σύστημα 24 δορυφόρων. Αυτό ακολούθησε γρήγορα από ιδιωτικούς, εμπορικούς δορυφόρους που τοποθετήθηκαν σε τροχιά, καθιστώντας το IIoT (Industrial Internet of Things) πολύ πιο λειτουργικό.

Πραγματοποίηση της Ιδέας

Το Internet of Things, ως έννοια, δεν ονομάστηκε επίσημα μέχρι το 1999, αλλά ένα από τα πρώτα παραδείγματα IoT είναι από τις αρχές της δεκαετίας του 1980 και ήταν μια μηχανή Coca Cola, που βρισκόταν στο Πανεπιστήμιο Carnegie Mellon. Οι τοπικοί προγραμματιστές συνδέονταν μέσω του Διαδικτύου στη συσκευή ψύξης και έλεγχαν αν υπήρχε διαθέσιμο ποτό και αν ήταν κρύο, πριν πραγματοποιήσουν την διαδρομή για να αγοράσουν ένα.
Ο Kevin Ashton, Εκτελεστικός Διευθυντής των Εργαστηρίων Auto-ID του MIT, επινόησε τη φράση «Internet of Things» το 1999. Ήταν ο πρώτος που περιέγραψε το IoT, ενώ έκανε μια παρουσίαση για την Procter & Gamble, αλλά ο ορισμός του IoT έχει εξελιχθεί ανά τα χρόνια. Ο κ. Ashton δήλωσε:

> «Σήμερα οι υπολογιστές, και επομένως το Διαδίκτυο, εξαρτώνται σχεδόν εξ ολοκλήρου από τους ανθρώπους για πληροφορίες. Σχεδόν όλα τα περίπου 50 petabytes δεδομένων που είναι διαθέσιμα στο Διαδίκτυο καταγράφηκαν και δημιουργήθηκαν αρχικά από ανθρώπους πληκτρολογώντας, πατώντας ένα κουμπί εγγραφής, τραβώντας μια ψηφιακή φωτογραφία ή σαρώνοντας ένα barcode. Το πρόβλημα είναι ότι οι άνθρωποι έχουν περιορισμένο χρόνο, προσοχή και ακρίβεια. Όλα αυτά σημαίνουν ότι δεν είναι πολύ καλοί στη συλλογή δεδομένων για πράγματα στον πραγματικό κόσμο. Εάν είχαμε υπολογιστές που ήξεραν τα πάντα για τα πάντα, χρησιμοποιώντας δεδομένα που συγκέντρωσαν χωρίς καμία βοήθεια από εμάς, θα μπορούσαμε να παρακολουθούμε και να μετράμε τα πάντα και να μειώνουμε σημαντικά τη σπατάλη, την απώλεια και το κόστος. Θα ξέραμε πότε χρειάζονταν αντικατάσταση, επισκευή ή απόσυρση και αν ήταν φρέσκα ή περασμένα από το καλύτερό τους».

Αρχές της δεκαετίας του 2000

Ο Kevin Ashton (ο τύπος που επινόησε το όνομα «Internet of Things») πίστευε ότι η Αναγνώριση με Ραδιοφωνική Συχνότητα (RFID) ήταν απαραίτητη προϋπόθεση για το Διαδίκτυο των πραγμάτων — κυρίως ως λύση παρακολούθησης αποθέματος.
Εκ των υστέρων, η παρακολούθηση αποθέματος έχει γίνει ένα από τα πιο προφανή πλεονεκτήματα του IoT.
Κατέληξε στο συμπέρασμα ότι εάν όλες οι συσκευές είχαν «επισήμανση», οι υπολογιστές θα μπορούσαν να τις διαχειρίζονται, να τις παρακολουθούν και να τις καταγράφουν. Σε κάποιο βαθμό, η επισήμανση πραγμάτων έχει επιτευχθεί μέσω τεχνολογιών όπως η ψηφιακή υδατοσήμανση, οι γραμμικοί κώδικες και οι κωδικοί QR.

Το 2002-2003, η Walmart και το Υπουργείο Άμυνας των ΗΠΑ ήταν οι πρώτοι μεγάλοι οργανισμοί που υιοθέτησαν το μοντέλο της Ashton για την παρακολούθηση του αποθέματος με χρήση ετικετών, RFID και Internet of Things.
Ring, ένα κουδούνι που συνδέεται με το smartphone σας, αποτελεί ένα εξαιρετικό παράδειγμα χρήσης του Internet of Things στο σπίτι. Το κουδούνι σάς σηματοδοτεί όταν πατήσετε το κουδούνι της πόρτας και σας επιτρέπει να δείτε ποιος είναι και να μιλήσετε μαζί τους.
Το Ring doorbell αναπτύχθηκε το 2011 από τον Jamie Siminoff επειδή ήθελε να δει ποιος ήταν στην πόρτα του ενώ ήταν στο γκαράζ και εργαζόταν. Δεν μπορούσε να ακούσει το κουδούνι της πόρτας από το γκαράζ και συνέχιζε να χάνει τις παραδόσεις.
Ένα πρόσθετο και σημαντικό στοιχείο για την ανάπτυξη ενός λειτουργικού IoT έλαβε χώρα τον Ιούνιο του 2012, όταν οι μεγάλοι πάροχοι υπηρεσιών Διαδικτύου και εταιρείες web συμφώνησαν να αυξήσουν τον χώρο διευθύνσεων στο παγκόσμιο Διαδίκτυο ενεργοποιώντας το IPV6 για τις υπηρεσίες και τα προϊόντα τους. Ο Steve Leibson, του Μουσείου Ιστορίας Υπολογιστών, δήλωσε:

> "Η επέκταση του χώρου διευθύνσεων σημαίνει ότι θα μπορούσαμε να εκχωρήσουμε μια διεύθυνση IPV6 σε κάθε άτομο στην επιφάνεια της γης και να έχουμε ακόμα αρκετές διευθύνσεις για να κάνουμε άλλες 100+ γειώσεις."

Με άλλα λόγια, δεν πρόκειται να ξεμείνουμε από διευθύνσεις διαδικτύου σύντομα.

IoT Getting Smarter

Οι «Έξυπνες πόλεις» μπορούν να χρησιμοποιήσουν το IoT για να μειώσουν τα απόβλητα και να μεγιστοποιήσουν την αποτελεσματική χρήση της ενέργειας. Το IoT μπορεί επίσης να χρησιμοποιηθεί για τον εξορθολογισμό των ροών κυκλοφορίας και τον εντοπισμό του διαθέσιμου χώρου στάθμευσης
Το 2012, το Ομοσπονδιακό Γραφείο Ενέργειας της Ελβετίας ξεκίνησε ένα πιλοτικό πρόγραμμα με την ονομασία «Smart City Switzerland». Έφεραν μαζί εκπροσώπους από πανεπιστήμια, επιχειρήσεις και δημόσια διοίκηση για να συζητήσουν νέες ιδέες για το αστικό περιβάλλον. Η Smart City Switzerland έχει πάνω από εξήντα έργα σε εξέλιξη και υποστηρίζει νέες επιστημονικές συνεργασίες και καινοτομία. (Η Smart City Switzerland έχει εξελιχθεί σε κάτι αρκετά εντυπωσιακό.)
Μια καλά σχεδιασμένη έξυπνη πόλη υποστηρίζει όλα τα είδη αισθητήρων που είναι συνδεδεμένοι στο διαδίκτυο και παρέχει:

- Παρακολούθηση κυκλοφορίας – Παρακολούθηση και αναφορά κυκλοφορίας σε πραγματικό χρόνο.
- Παρακολούθηση ποιότητας αέρα – Οι ενσωματωμένοι αισθητήρες IoT μπορούν να εντοπίσουν τους ρυπαίνοντες.
- Έξυπνες μεταφορές- Τα έξυπνα φανάρια βελτιστοποιούν την αποτελεσματικότητα της κυκλοφορίας και τα μέσα μαζικής μεταφοράς.

- Έξυπνη στάθμευση – Αισθητήρες τοποθετημένοι στο πεζοδρόμιο κ.λπ. για τον προσδιορισμό της πληρότητας του χώρου στάθμευσης, οι οποίοι κοινοποιούνται στους οδηγούς.
- Έξυπνος δημόσιος φωτισμός- Φωτισμός χαμηλής ενέργειας σε συνδυασμό με χρονισμό και αισθητήρες.
- Έξυπνα κτίρια- Όταν συνδέεται με την έξυπνη πόλη μέσω Διαδικτύου, γίνεται μέρος της υποδομής της πόλης.

Ένα έξυπνο κτίριο, από μόνο του, χρησιμοποιεί αισθητήρες και αυτοματοποιημένες διαδικασίες για τον έλεγχο των λειτουργιών του κτιρίου, οι οποίες περιλαμβάνουν κλιματισμό, θέρμανση, εξαερισμό, ασφάλεια, φωτισμό και άλλα συστήματα. Τα έξυπνα κτίρια είναι ολοκληρωμένα συστήματα και μοιράζονται ζωτικές πληροφορίες.

Το Industrial Internet of Things (IIoT)

Το Industrial Internet of Things (IIoT) είναι μια επέκταση του IoT και χρησιμοποιεί ενεργοποιητές και έξυπνους αισθητήρες, οι οποίοι είναι δικτυωμένοι μαζί με τις βιομηχανικές εφαρμογές μιας εταιρείας. Στόχος είναι να δοθεί στις βιομηχανίες μεγαλύτερη αποτελεσματικότητα και αξιοπιστία. Το IIoT περιλαμβάνει ρομποτική και διαδικασίες παραγωγής που καθορίζονται από λογισμικό.
Η τεράστια χωρητικότητα αποθήκευσης του cloud (2002) ήταν απαραίτητη για να γίνει πραγματικότητα η σύγχρονη έκδοση του IIot.
Το IIoT δημιουργήθηκε περίπου το 2010, με αρκετές μεγάλες εταιρείες να αναπτύσσουν τα δικά τους συστήματα. Η GE έλαβε τα εύσημα για τη δημιουργία του όρου «Tndustrial Tnternet of Things», το 2012.

Το Διαδίκτυο των Πραγμάτων γίνεται μέρος της ζωής

Μέχρι το 2013, το IoT είχε γίνει ένα σύστημα που χρησιμοποιεί πολλαπλές τεχνολογίες, που κυμαίνονται από το Διαδίκτυο έως την ασύρματη επικοινωνία και από τα μικροηλεκτρομηχανικά συστήματα (MEMS) έως τα ενσωματωμένα συστήματα.
Αυτό περιλαμβάνει σχεδόν οτιδήποτε μπορείτε να σκεφτείτε, από κινητά τηλέφωνα έως συντήρηση κτιρίου έως τον κινητήρα τζετ ενός αεροπλάνου. Οι ιατρικές συσκευές, όπως ένα εμφύτευμα παρακολούθησης καρδιάς ή ένας αναμεταδότης βιοτσιπ σε ένα ζώο φάρμας, μπορούν να μεταφέρουν δεδομένα μέσω δικτύου και είναι μέλη του IoT.

Το IoT πάει Mobile – 2015

Τα smartphone αποτελούν μέρος του IoT και έχουν γίνει ένα σημαντικό εργαλείο επικοινωνίας για πολλά άτομα. Το 2015, εντάχθηκαν στο IoT με υψηλό βαθμό ενθουσιασμού από τους εμπόρους. Οι αισθητήρες σε αυτές τις συσκευές παρακολουθούνται από τμήματα μάρκετινγκ, τα οποία στέλνουν ορισμένες προσφορές με βάση τον πελάτη και την τοποθεσία του προϊόντος.

Ο κλάδος της υγείας έχει επίσης εκμεταλλευτεί αυτή την τάση. Συσκευές, όπως έξυπνα ρολόγια, smartphone και οθόνες που μπορούν να καταποθούν μπορούν να παρακολουθούν τα δεδομένα ενός ασθενούς σχετικά με την αρτηριακή πίεση, τον καρδιακό ρυθμό και άλλες ανησυχίες σε πραγματικό χρόνο.
Τα αυτοκίνητα και τα φορτηγά έχουν γίνει μέλη του IoT. Ένα συνδεδεμένο όχημα λειτουργεί με άλλες συσκευές μέσω ασύρματων δικτύων. Αυτή η τεχνολογία επιτρέπει σε διάφορα «συνδεδεμένα δίκτυα» να έχουν πρόσβαση και να επικοινωνούν με τα οχήματα.
Τα αυτοκίνητα και τα φορτηγά είναι ήδη φορτωμένα με αισθητήρες και τεχνολογία, συμπεριλαμβανομένου του OBD (on-board diagnostics) και του GPS. Μεγιστοποιώντας τη χρήση αυτών των τεχνολογιών, οι επιχειρήσεις μπορούν να εξάγουν πληροφορίες από τους στόλους τους σχετικά με τις απαιτήσεις συντήρησης, τις συνθήκες οδήγησης και τις διαδρομές σε πραγματικό χρόνο.
Τα αυτοοδηγούμενα αυτοκίνητα χρησιμοποιούν το σύννεφο για να ανταποκρίνονται σε παρακείμενα αυτοκίνητα, δεδομένα κυκλοφορίας, χάρτες, καιρικές συνθήκες, επιφανειακές συνθήκες κ.λπ. Η χρήση του cloud βοηθά τα οχήματα να παρακολουθούν το περιβάλλον τους και να λαμβάνουν καλύτερες αποφάσεις.
Τα αυτόνομα αυτοκίνητα είναι νέα μέλη του IOT. Το πρώτο πραγματικά αυτοοδηγούμενο όχημα εμφανίστηκε τη δεκαετία του 1980. Τον Οκτώβριο του 2021, η May Mobility κυκλοφόρησε ένα πιλοτικό πρόγραμμα για να δοκιμάσει το λογισμικό αυτοοδήγησης.
Οι ανθρώπινες γειτονιές γίνονται πλέον μέρος της διασυνδεδεμένης κοινότητας που ονομάζεται Internet of Things.

## 1.4 Εργαλεία Ανοιχτού Λογισμικού και Wordpress

Το WordPress αποτελεί ένα από τα πιο δημοφιλή συστήματα διαχείρισης περιεχομένου (CMS), λόγω των πολλών δυνατοτήτων και του εύχρηστου περιβάλλοντος. Τα CMS αποτελούν εφαρμογές μέσω των οποίων είναι δυνατή η δημιουργία και διαχείριση ιστοτόπων δυναμικού περιεχομένου. Ένα CMS διαχωρίζει τα διάφορα μέρη ενός ιστότοπου (περιεχόμενο, σχεδιασμός, λειτουργικότητα) με αποτέλεσμα να καθιστά ευκολότερη τη διαχείρισή του. Επιτρέπουν επίσης την ανάθεση ρόλων για την κατανομή ευθυνών διαχείρισης διαφορετικών τμημάτων του ιστοτόπου σε διαφορετικούς χρήστες. Για παράδειγμα, άτομα που δεν έχουν τεχνικές γνώσεις μπορούν να έχουν πρόσβαση μόνο στην επεξεργασία περιεχομένου του ιστότοπου, ενώ οι administrators άτομα μπορούν να εργαστούν στη σχεδίαση και τη λειτουργικότητα του ιστότοπου. Μέσω της προσθήκης plug-ins που αναπτύσσονται από την κοινότητα του και προσφέρονται ως επί τω πλείστων δωρεάν, η λειτουργικότητα του μπορεί να τροποποιηθεί

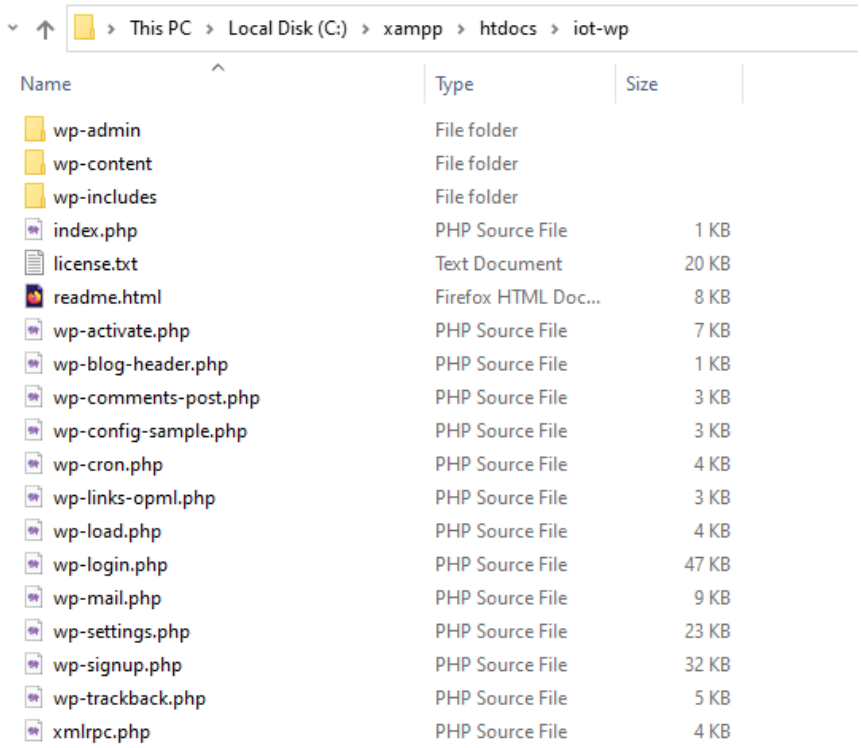
ανάλογα με τις ανάγκες του εκάστοτε portal. Το Wordrpess είναι γραμμένο σε PHP, παρέχει έναν φιλικό προς τον χρήστη πίνακα διαχείρισης και τα παρακάτω σημαντικά πλεονεκτήματα έναντι των αντίστοιχων CMS ανοιχτού λογισμικού:

- Βελτιστοποίηση για το Search Engine Optimization (SEO), καθώς δημιουργούν δυναμικά απλές και φιλικές διευθύνσεις URL. Επιπλέον, παρέχεται η δυνατότητα εγκατάστασης πρόσθετων για βελτίωση SEO. Χάρη στη βελτιστοποίηση SEO οι ιστοσελίδες είναι ευκολότερο να ανέβουν σε κατάταξη στις μηχανές αναζήτησης.
- Μεγάλη κοινότητα από προγραμματιστές και χρήστες, κάτι που σημαίνει πως παρέχονται πολλά και διαφορετικά πρόσθετα και θέματα καθώς και υποστήριξη. Χάρη στην κοινότητα του Wordpress, παρέχονται δωρεάν πολλά δωρεάν εργαλεία και η δημιουργία αισθητικά άρτιων ιστοσελίδων είναι πιο εύκολη από ποτέ.
- Δυνατότητα τροποποίησης κώδικα, δεδομένου του ότι πρόκειται για μία πλατφόρμα ανοιχτού κώδικα, με βασικές γνώσεις PHP μπορεί κανείς να κάνει τροποποιήσεις και να δημιουργήσει ακόμη και δικά του πρόσθετα ή θέματα για το Wordpress.
- Προστασία δεδομένων και ασφάλεια, μέσω της χρήσης συγκεκριμένων πρόσθετων και κατάλληλων ρυθμίσεων, όπως για παράδειγμα το πρόσθετο Really Simple SSL ή το firewall του πρόσθετου WPCerber και ρύθμιση για αυτόματο block σε IP που κάνουν πολλές αποτυχημένες ποσπάθειες σύνδεσης, μπορεί να εξασφαλιστεί με ευκολία η απαραίτητη ασφάλεια των δεδομένων των χρηστών.
- Ευκολία χρήσης. Το WordPress αποτελεί μία εξαιρετική πλατφόρμα για τον έλεγχο πρόσβασης στις πληροφορίες. Ειδικά στην περίπτωση των portals, η χρήση και η πρόσβαση στις πληροφορίες από τους επισκέπτες πρέπει να γίνεται με τη μεγαλύτερη ευκολία. Οι πληροφορίες πρέπει να παρουσιάζονται με σαφήνεια και κάθε καρτέλα ή επιλογή πρέπει να βρίσκεται αποτελεί μία ξεχωριστή ενότητα για να είναι εύκολη η εύρεση και η εξερεύνηση του portal.

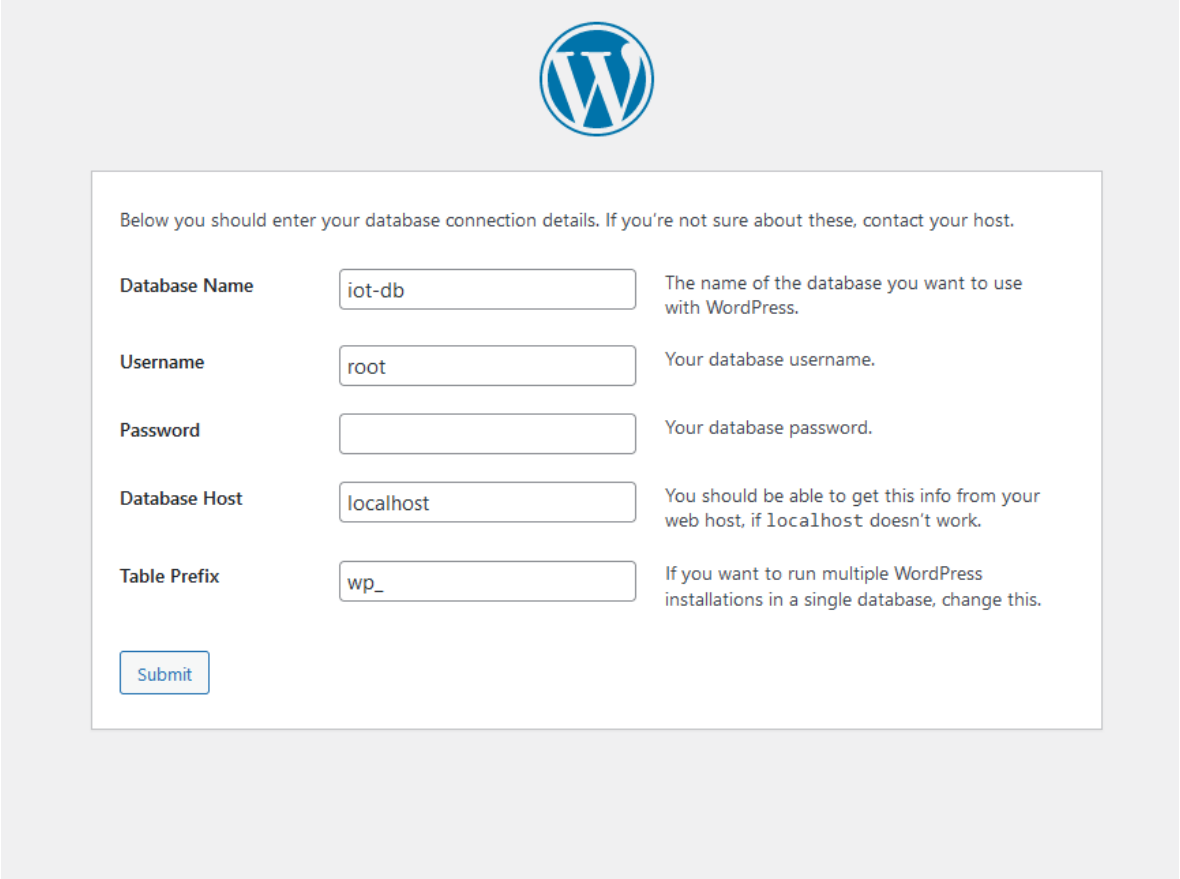
# 2. ΔΙΑΔΙΚΑΣΙΑ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΑΝΑΠΤΥΞΗΣ

## 2.1 Εγκατάσταση Wordpress σε localhost.

Για την υλοποίηση του portal της παρούσας εργασίας χρησιμοποιήθηκε η τελευταία έκδοση του Wordpress, 5.9.1, σε συνδυασμό με το θέμα “Hello Elementor”, που πρακτικά αποτελεί έναν λευκό καμβά προς σχεδίαση, και το πρόσθετο Elementor, που επιτρέπει τον οπτικό σχεδιασμό των σελίδων. Αξίζει να σημειωθεί το Wordpress διαθέτει δικό του visual editor, αλλά η επιλογή του Elementor έγινε επειδή παρέχει περισσότερες επιλογές και οπτικά πρότυπα. Αρχικά, κατεβάσαμε από το wordpress.org το σύνολο των αρχείων από τα οποία αποτελείται η πλατφόρμα και με χρήση της εφαρμογής XAMPP και phpMyAdmin δημιουργήσαμε μία βάση δεδομένων. Έπειτα, επισκεφθήκαμε από έναν φυλλομετρητή τη διεύθυνση localhost/iot-wp (αφού κάναμε extract τα αρχεία στον φάκελο C:/XAMPP/htdocs/iot-wp) και ακολουθήσαμε με επιτυχία τα βήματα εγκατάστασης.




Εικόνα 1. Αρχεία Wp

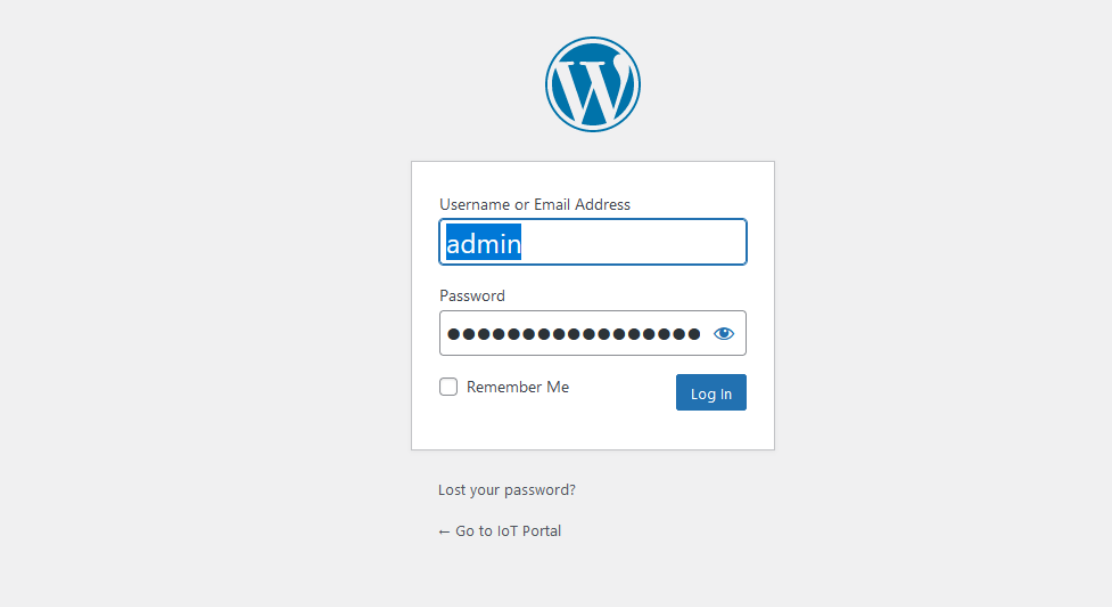



Εικόνα 2. Σύνδεση στην βάση

Μετά την ολοκλήρωση της εγκατάστασης, μεταβήκαμε στη διεύθυνση localhost/iot-wp/wp-admin (το wp-admin είναι η προεπιλεγμένη σελίδα διαχείρισης του Wordpress) και συνδεθήκαμε με τους κωδικούς που δηλώσαμε κατά την εγκατάσταση:

**Username:** admin

**Password:** Cr*9w(q5K*Cikx5R9@




Εικόνα 3. Σύνδεση Wp

Το επόμενο βήμα, ήταν η εγκατάσταση και ενεργοποίηση των βασικών πρόσθετων και του θέματος που θα χρησιμοποιηθούν από τις αντίστοιχες καρτέλες στο διαχειριστικό:

**Θέμα:** Hello Elementor

**Plug-ins:**

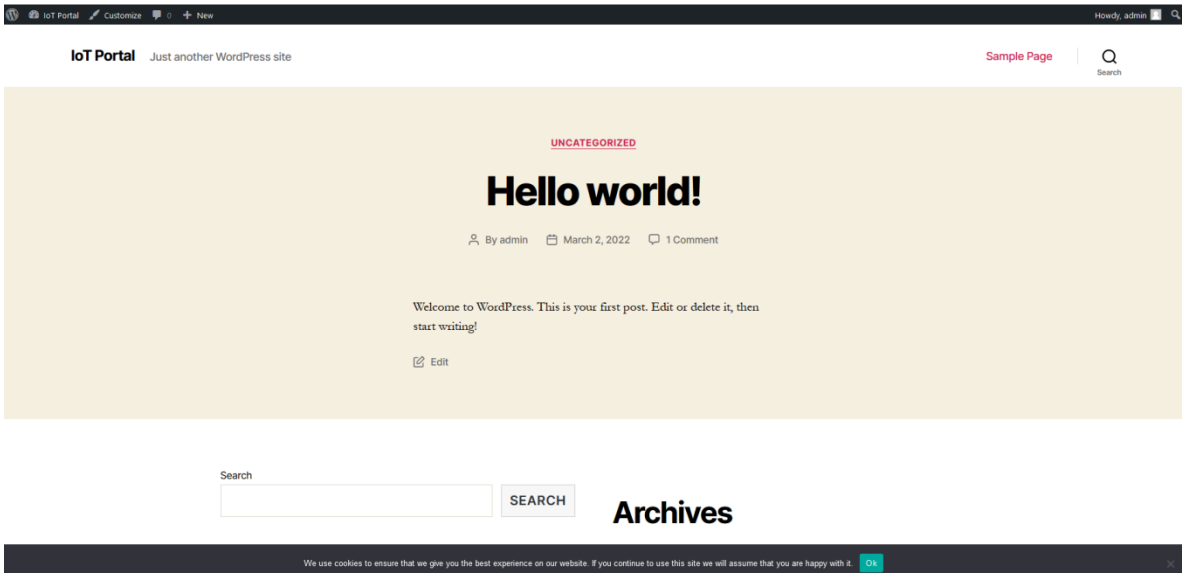
***Elementor-***για την εύκολη οπτική σχεδίαση.

***Elementor Header & Footer Builder***

***Essential Addons for Elementor***- για περισσότερα modules όπως Slideshows,Flipbox κ.ά.

***Post Grid-***για εύκολη προβολή άρθρων σε πλέγμα με ρύθμιση κατηγορίας.

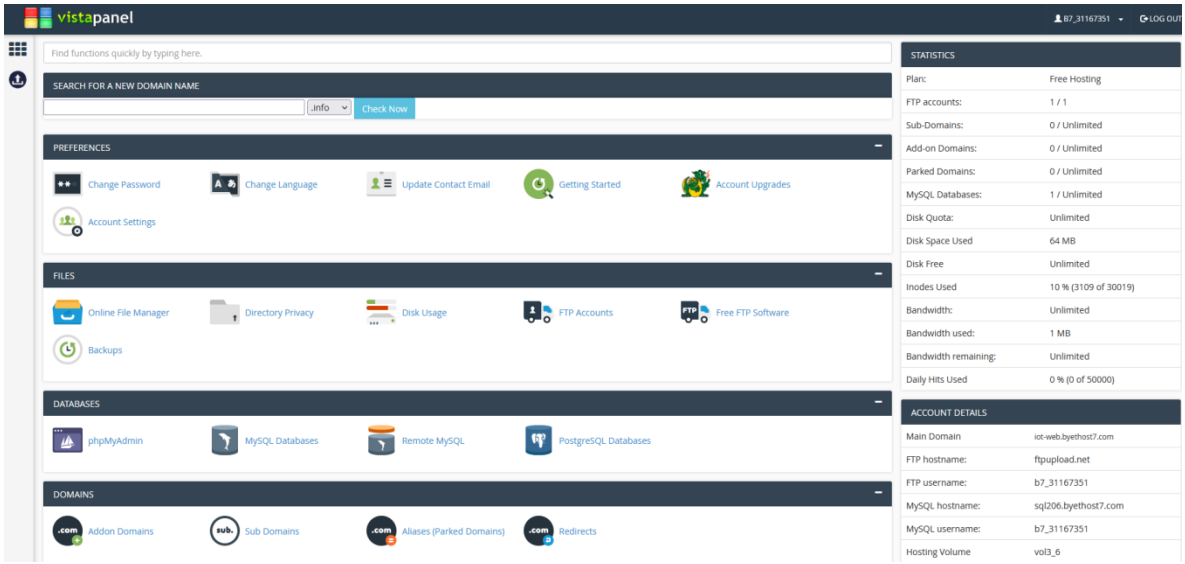
***Cookie Notice & Compliance for GDPR / CCPA-***για ενημέρωση των επισκεπτών σχετικά με την χρήση cookies μέσω αναδυόμενου πλαισίου.




Εικόνα 4 Πρώτες εικόνες

## 2.2 Μεταφορά σε online host.

Σε αυτό το σημείο, κρίθηκε ορθή η μεταφορά του portal σε online πάροχο φιλοξενίας ώστε να είναι δυνατή η επίσκεψη του από οποιονδήποτε στο διαδίκτυο. Αυτή η διαδικασία θα μπορούσε να γίνει και κατόπιν της τελικής ολοκλήρωσης του portal, αλλά η μεταφορά του σε online server εξυπηρετεί καθώς δεν μας περιορίζει ως προς την τοποθεσία από την οποία θα πρέπει να εργαζόμαστε. Είναι online, άρα μπορούμε να συνδεθούμε οποιαδήποτε στιγμή, από οποιονδήποτε υπολογιστή! Επιλέχθηκε ο δωρεάν πάροχος φιλοξενίας byethost όπου δημιουργήθηκε λογαριασμός και το domain www.iot-web.byethost7.com και ανεβάσαμε τα αρχεία εγκατάστασης μέσω ftp και τη βάση δεδομένων μέσω του PHPMyAdmin.

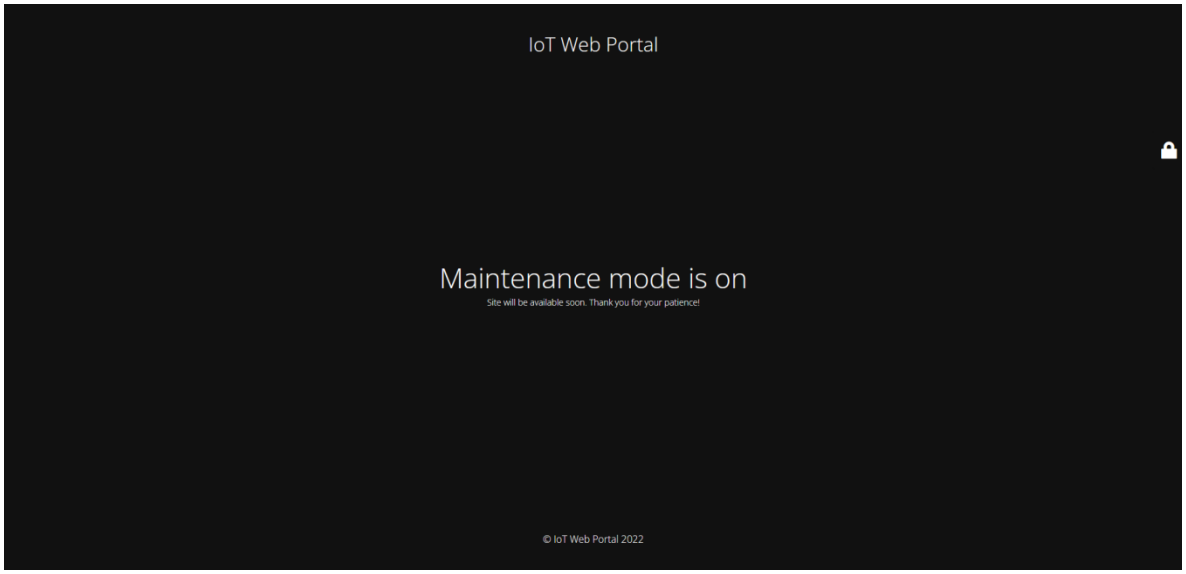



Εικόνα 5. Online host

Αφού ολοκληρώθηκε η μεταφορά, συνδεθήκαμε στην online διεύθυνση του διαχειριστικού:

iot-web.byethost7.com/wp-admin

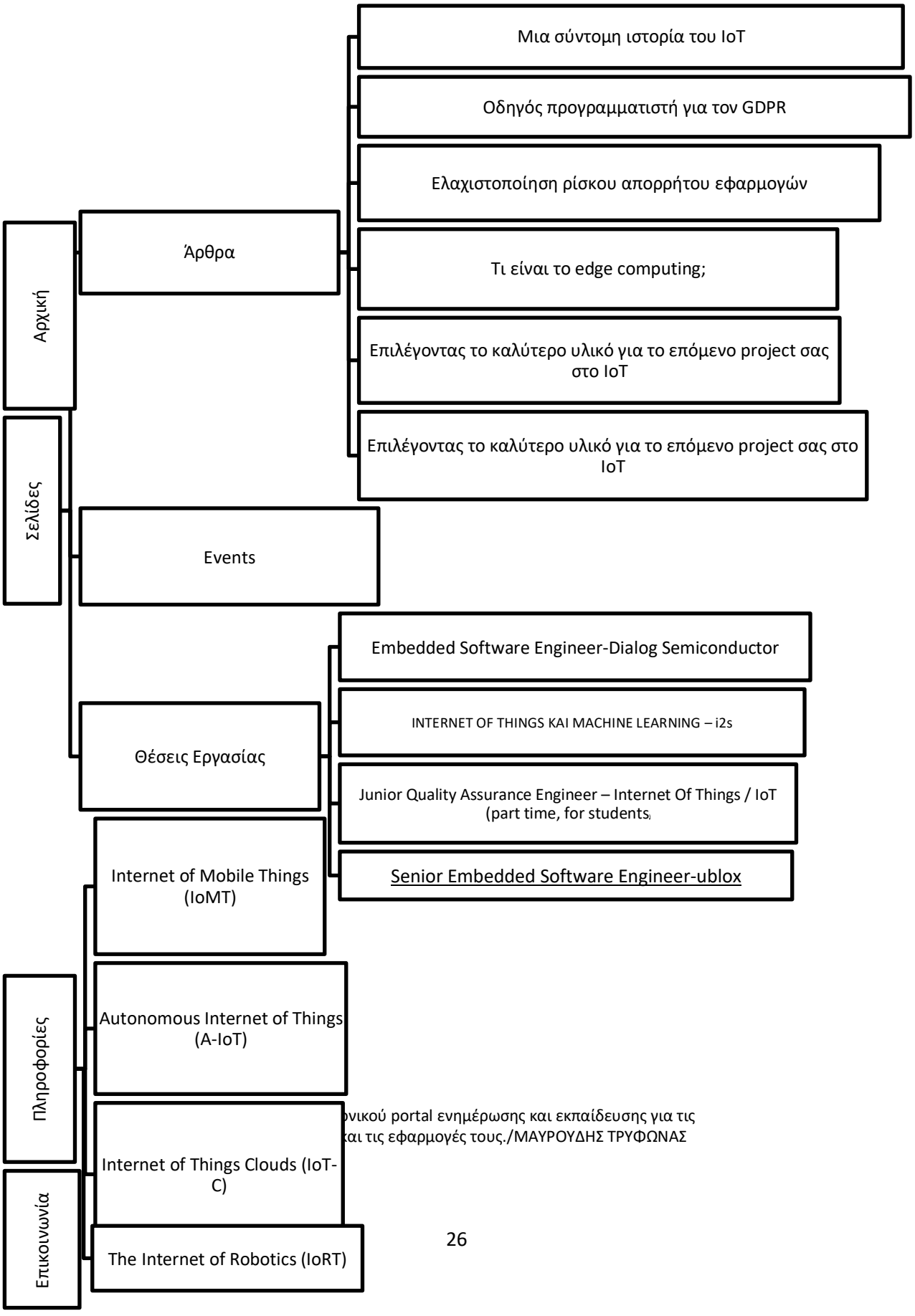
και εγκαταστήσαμε και ενεργοποιήσαμε το πρόσθετο Maintenance έτσι ώστε οι επισκέπτες να περιορίζονται κατά την επίσκεψη σε μία σελίδα που τους ενημερώνει πως το portal είναι υπό κατασκευή. Η σύνδεση στο διαχειριστικό γίνεται κανονικά από το παραπάνω link, συνεπώς εμείς μπορούμε να έχουμε πρόσβαση στον ιστότοπο και να εργαζόμαστε στο περιεχόμενο του, χωρίς οι επισκέπτες να βλέπουν τις αλλαγές.




Εικόνα 6. Ενεργοποιήση Maintenance Mode

## 2.3Σχεδίαση Βασικής Δομής και Περιεχομένου.

Δεδομένου του μεγάλου όγκου πληροφοριών που φιλοξενεί ένα portal, αλλά και της αρκετά σύνθετης φύσης που έχει ο τομέας του Internet Of Things, για τη δημιουργία ενός ιστοτόπου φιλικού προς τους επισκέπτες είναι απαραίτητη η σωστή οργάνωση και σχεδίαση του περιεχομένου του. Για το σκοπό αυτό, δημιουργήθηκε το παρακάτω διάγραμμα που περιγράφει τη δομή των σελίδων και του βασικού μενού:



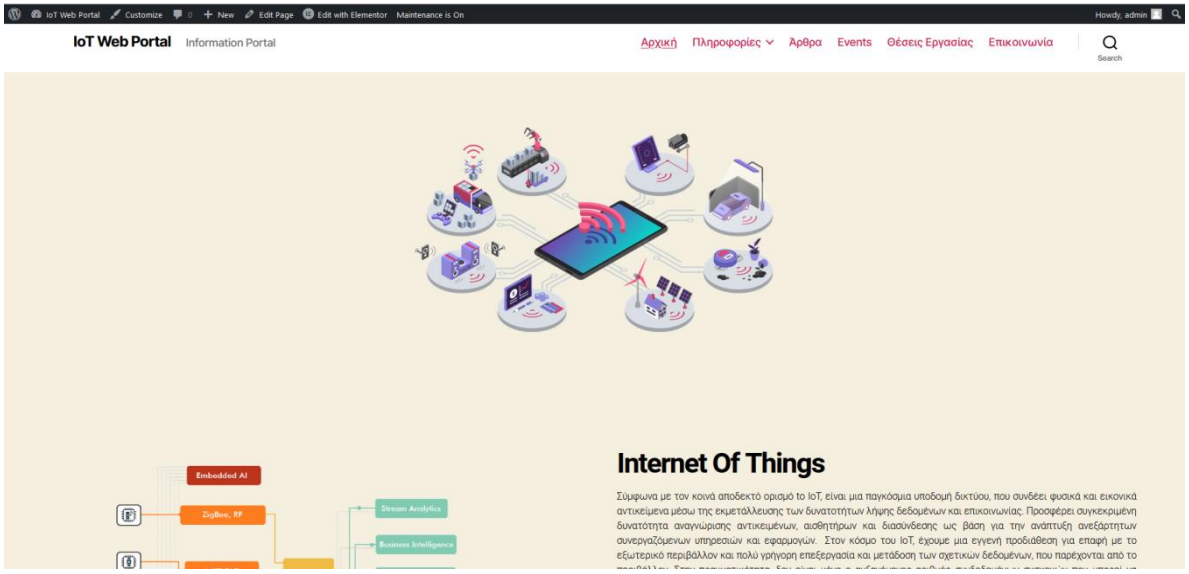

ονικού portal ενημέρωσης και εκπαίδευσης για τις
και τις εφαρμογές τους./ΜΑΥΡΟΥΔΗΣ ΤΡΥΦΩΝΑΣ

Εικόνα 7. Αρχική σχεδίαση δομής

Η Αρχική σελίδα θα περιέχει τις βασικές πληροφορίες σχετικά με τον σκοπό της σελίδας αλλά και το τι είναι το Internet of Things, καθώς και κουμπιά για γρήγορη πρόσβαση στις σελίδες πληροφοριών. Η σελίδα Άρθρα θα περιλαμβάνει ένα πλέγμα με άρθρα σχετικά με το Internet of Things με φθίνουσα ταξινόμηση έτσι ώστε τα πιο πρόσφατα να εμφανίζονται πρώτα.Τα άρθρα τα οποία αποτελόθν μερος του portal εκτός απο την εκτενής περιγραφη του θέματος του οποίου αναφέρονται περιέχουν Hyper links σε όρους που τυχόν ο αναγνωστης να μην καταλαβαίνει σε εξωτερικές σελίδες όπου και μπορούν να εμβαθύνουν στο θεμα.Η σελίδα events θα φιλοξενεί όλες τις εκδηλώσεις ή συνέδρια σχετικά με το Internet of Things, η σελίδα Θέσεις Εργασίας θα περιέχει αγγελίες εργασιών με απευθείας συνδέσμους στις εταιρείες, ενώ η σελίδα Επικοινωνία θα περιλαμβάνει φόρμα γρήγορης επικοινωνίας.

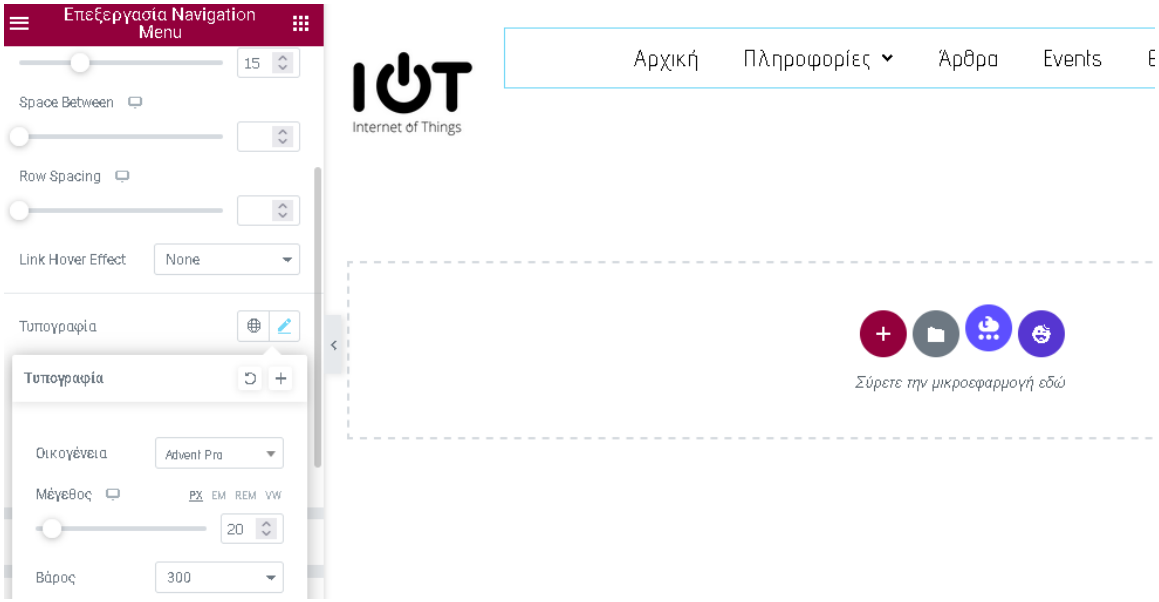
## 2.4 Προσαρμογή Εμφάνισης.

Το επόμενο στάδιο ήταν αυτό της οπτικής προσαρμογής. Μέσω του διαχειριστικού και της επιλογής Εμφάνιση->Προσαρμογή κάναμε τις απαραίτητες ρυθμίσεις για να αποκτήσει το portal μία ομοιόμορφη οπτική ταυτότητα. Μέσω των Μικροεφαρμογών, προσαρμόστηκε το Footer του portal για όλες τις σελίδες.



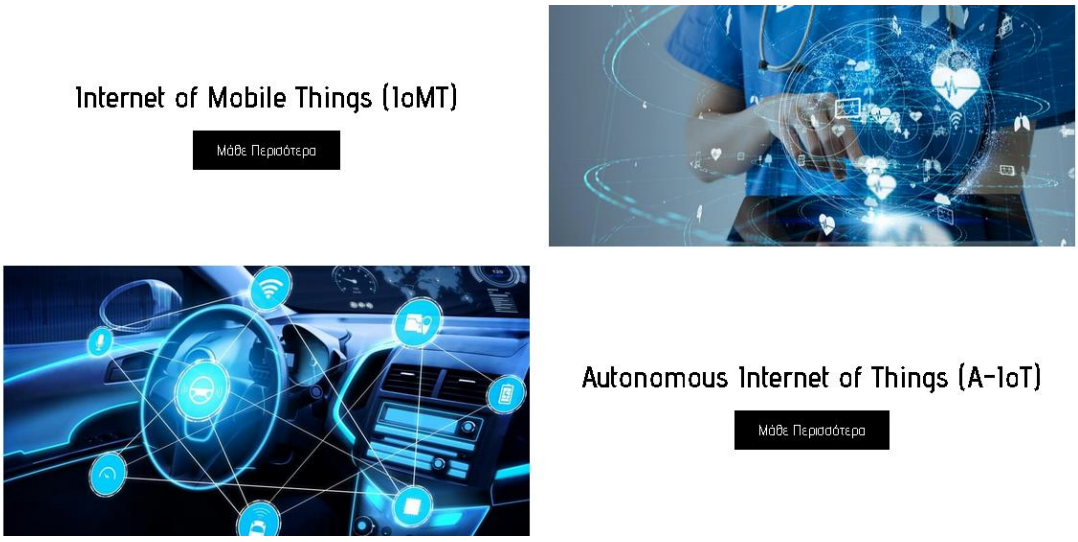

Εικόνα 8. Προσαμογή εμφάνισής

Με χρήση του plugin Elementor Header & Footer Builder δημιουργήσαμε το μενού στην κορυφή της σελίδας. Επιλέξαμε τη γραμματοσειρά Advent Pro με μέγεθος 20px και βάρος (weight) 300.




Εικόνα 9. Δημιουργία Slide Show

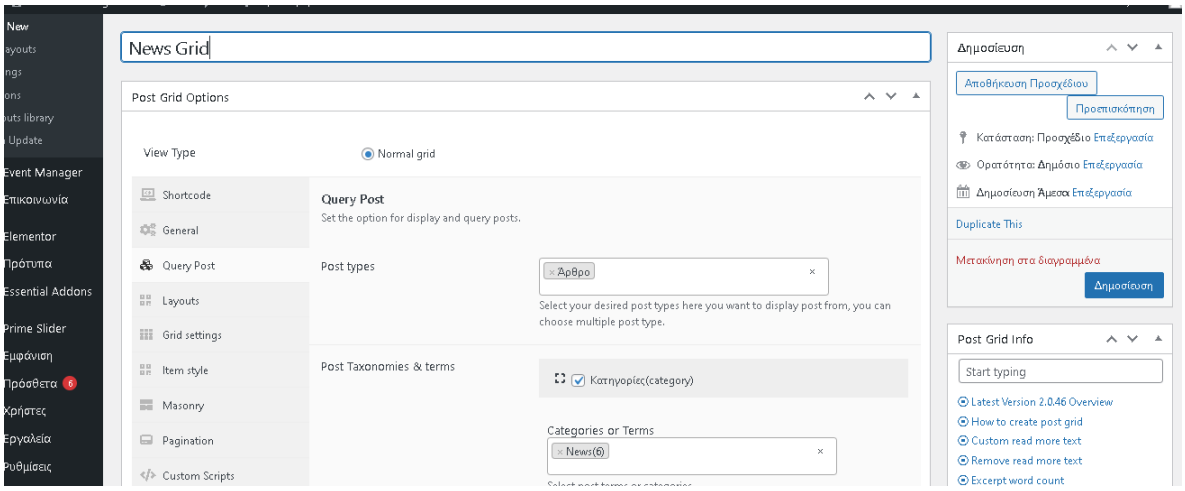
Δημιουργήθηκαν 4 sections με κουμπί και υπερσύνδεσμο προς κάθε μία από τις υποσελίδες του «Πληροφορίες». Κατόπιν, εγκαταστήσαμε το plugin "Slider Prime" και δημιουργήσαμε ένα slideshow για την αρχική με δύο εικόνες και υπερσυνδέσμους προς τις σελίδες «Θέσεις εργασίας» και «Άρθρα» Μετά από αρκετές δοκιμές και αλλαγές, καταλήξαμε στην παρακάτω δομή:




Εικόνα 10. Δομή πληροφοριών

## 2.5 Προσθήκη Περιεχομένου.

Οι θέσεις εργασίας και τα νέα προστέθηκαν ως άρθρα από το διαχειριστικό. Έπειτα δημιουργήθηκαν από το plugin PostGrid δύο πλέγματα για την προβολή των άρθρων ανά κατηγορία και με χρήση του shortcode τα προβάλαμε στις αντίστοιχες σελίδες.




Εικόνα 11. Προσθήκη άρθρων

**Άρθρα**

News
A Brief History of Internet of Things
Read more

News
A developer's guide to the GDPR
Read more

News
Choosing the best hardware for your next IoT project
Read more

News
Application privacy by design
Read more

News
Minimizing application privacy risk
Read more

News
Whats is edge computing
Read more

Εικόνα 12. Άρθρα

Παρακάτω θα δούμε άρθρα τα οποιά προστέθηκαν στην σελίδα Άρθρα οπου και θα μας δώσουν μια πίο ολοκληρωμένη εικόνα γύρω απο το IoT

### 2.5.1Ελαχιστοποίηση ρίσκου και απορρήτου εφαρμογών στο IoT

Υπάρχει μια σειρά από τεχνικές λύσεις που μπορούν να χρησιμοποιηθούν από εφαρμογές για να ενισχύσουν σημαντικά την προστασία των προσωπικών δεδομένων. Ενώ ο GDPR δεν απαιτεί τη χρήση ανωνυμοποίησης, ψευδωνυμοποίησης ή κρυπτογράφησης προσωπικών δεδομένων, τέτοιες τεχνικές λύσεις αναφέρονται στο GDPR ως μέθοδοι για τον μετριασμό του κινδύνου απορρήτου ενός υποκειμένου των δεδομένων. Αυτές οι τεχνικές μπορούν επίσης να μειώσουν σημαντικά το εύρος της συμμόρφωσης με το GDPR και τον κίνδυνο για τους οργανισμούς παροχής εφαρμογών, όπου είναι υπεύθυνοι ως υπεύθυνος επεξεργασίας ή επεξεργαστής (φιλοξενίας). Επομένως, οι προγραμματιστές εφαρμογών θα πρέπει να κατανοήσουν και να εξετάσουν το ενδεχόμενο εφαρμογής καθεμιάς από τις τεχνικές προστασίας προσωπικών δεδομένων που αναφέρονται από τον GDPR.

Ο GDPR δεν παρέχει ένα περιγραφικό σύνολο τεχνικών απαιτήσεων ασφάλειας, αλλά η ασφάλεια εφαρμογών βέλτιστων πρακτικών θεωρείται θεμελιώδης υποχρέωση προστασίας της ιδιωτικής ζωής δεδομένων. Η αδύναμη ασφάλεια εφαρμογών μπορεί να οδηγήσει σε παραβίαση προσωπικών δεδομένων που θα μπορούσε να προκαλέσει ανησυχία και βλάβη σε μεγάλο αριθμό ατόμων. Σύμφωνα με το άρθρο (5) στ) του GDPR, μια εφαρμογή μπορεί να θεωρηθεί παράνομη σε περίπτωση που τα προσωπικά δεδομένα παραβιαστούν είτε κακόβουλα είτε κατά λάθος, επειδή η ασφάλεια της εφαρμογής δεν πληροί τα κατάλληλα πρότυπα.

*Άρθρο (5)Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει (στ) να υποβάλλονται σε επεξεργασία με τρόπο που να διασφαλίζει την κατάλληλη ασφάλεια των προσωπικών δεδομένων, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή ζημιά, χρησιμοποιώντας κατάλληλα τεχνικά ή οργανωτικά μέτρα («ακεραιότητα και εμπιστευτικότητα»).*

Οι μαζικές παραβιάσεις προσωπικών δεδομένων που προκαλούνται από αδύναμη ασφάλεια εφαρμογών, αποτελούν σημαντικό κίνδυνο για τον οργανισμό που αναπτύσσει και παρέχει την εφαρμογή (ελεγκτής). Καθώς τέτοια περιστατικά είναι πιθανό να επικαλούνται σημαντικές οικονομικές κυρώσεις από τις εποπτικές αρχές προστασίας της ιδιωτικής ζωής δεδομένων και να προκαλέσουν σημαντικές βλάβες στη φήμη λόγω της υποχρέωσης αποκάλυψης παραβίασης δεδομένων του GDPR.

Αυτή η καθοδήγηση παρέχει στους προγραμματιστές μια επεξήγηση των τεχνικών μετριασμού του απορρήτου των δεδομένων της εφαρμογής που αναφέρονται στον GDPR. Η καθοδήγηση παρέχει επίσης μια επισκόπηση των κατάλληλων πρακτικών ασφάλειας ανάπτυξης εφαρμογών, όπως αναμένεται από τις εποπτικές αρχές που επιβλέπουν τη συμμόρφωση με τον GDPR.

Ανωνυμοποίηση

Η ανωνυμοποίηση είναι μια διαδικασία αποχέτευσης προσωπικών δεδομένων που αλλάζει τα προσωπικά δεδομένα, επομένως δεν είναι πλέον δυνατή η ταυτοποίηση οποιωνδήποτε ατόμων (υποκείμενα δεδομένων). Η ανωνυμοποίηση δεδομένων είναι μια μονόδρομη διαδικασία. Όταν ένα

σύνολο δεδομένων έχει ανωνυμοποιηθεί, θα πρέπει να είναι αδύνατο να αντιστραφεί η διαδικασία και να μετατραπεί ξανά το σύνολο δεδομένων σε προσωπικά δεδομένα.

Τα προσωπικά δεδομένα που έχουν επαρκώς ανωνυμοποιηθεί δεν ταξινομούνται πλέον ως προσωπικά δεδομένα, γεγονός που όχι μόνο προστατεύει το απόρρητο του χρήστη της εφαρμογής, αλλά αφαιρεί τα δεδομένα από το πεδίο εφαρμογής όλων των νομικών υποχρεώσεων απορρήτου του GDPR. Αυτό επιβεβαιώνεται στην αιτιολογική σκέψη 26, η οποία αναφέρει ότι οι αρχές της προστασίας δεδομένων δεν ισχύουν εάν τα δεδομένα προσωπικού χαρακτήρα καθίστανται ανώνυμα με τέτοιο τρόπο ώστε το υποκείμενο των δεδομένων να μην είναι πλέον αναγνωρίσιμο.

*Αιτιολογική σκέψη 26Επομένως, οι αρχές της προστασίας δεδομένων δεν θα πρέπει να ισχύουν για ανώνυμες πληροφορίες, δηλαδή πληροφορίες που δεν σχετίζονται με ταυτοποιημένο ή αναγνωρίσιμο φυσικό πρόσωπο ή προσωπικά δεδομένα που παρέχονται ανώνυμα με τέτοιο τρόπο ώστε το υποκείμενο των δεδομένων να μην είναι ή να μην είναι πλέον αναγνωρίσιμο.*

Οι διαδικασίες εφαρμογών, τα εργαλεία τρίτων και οι άμεσες εντολές βάσης δεδομένων SQL μπορούν να παρέχουν αποτελεσματική ανωνυμοποίηση προσωπικών δεδομένων. Για να θεωρηθεί επιτυχής η ανωνυμοποίηση προσωπικών δεδομένων, η διαδικασία ανωνυμοποίησης πρέπει να ακυρώσει ή να αφαιρέσει όλα τα άμεσα και έμμεσα αναγνωριστικά προσωπικών δεδομένων, τα οποία περιλαμβάνουν:

Όνομα του υποκειμένου των δεδομένων

Λογαριασμός εφαρμογής και αναγνωριστικά χρήστη

Διευθύνσεις ηλεκτρονικού ταχυδρομείου, συμπεριλαμβανομένων εκείνων χωρίς ονόματα υποκειμένων δεδομένων

Ψευδώνυμα, συμπεριλαμβανομένου του φόρουμ και των διαδικτυακών λαβών

Αναγνωριστικά που μπορούν να αναζητηθούν για την αναγνώριση ενός ατόμου αλλού, όπως αριθμοί λογαριασμού και αριθμοί αναφοράς. βιομετρικά δεδομένα, συμπεριλαμβανομένων των γενετικών δεδομένων

Δεδομένα τοποθεσίας και παρακολούθησης, συμπεριλαμβανομένων της διεύθυνσης οδού, των τεταγμένων ετικετών γεωγραφικών ετικετών, των διευθύνσεων IP και των cookie εφαρμογών

Πεδία κειμένου που ενδέχεται να περιέχουν προσωπικά δεδομένα (για παράδειγμα, σχόλια χρηστών)

### Μέθοδοι ανωνυμοποίησης δεδομένων

Υπάρχουν διαφορετικά πλεονεκτήματα και κίνδυνοι απορρήτου με τους διάφορους τύπους μεθόδων ανωνυμοποίησης δεδομένων. Οι πιο συνηθισμένες μέθοδοι ανωνυμοποίησης προσωπικών δεδομένων περιγράφονται παρακάτω.

### Ακύρωση, διαγραφή και διόρθωση

Η ανωνυμοποίηση επιτυγχάνεται διαγράφοντας ή ακυρώνοντας (μηδενίζοντας) όλα τα άμεσα και έμμεσα πεδία προσωπικών αναγνωριστικών.

Εικόνα 13. Παράδειγμα μηδενικής ανωνυμοποίησης

| Data Subject Name (personal data identifier) | Disabilities |
|---|---|
| Alice Smith | Vision impairment |
| Bob Johnson | None |
| Dave Doe | deaf or hard of hearing |
| Eve Jackson | None |
| Grace Chan | Mental health |

**Personal Data**



| Data Subject Name (personal data identifier) | Disabilities |
|---|---|
| <null> | Vision impairment |
| <null> | None |
| <null> | deaf or hard of hearing |
| <null> | None |
| <null> | Mental health |

**Anonymized Data**

Πλεονεκτήματα: Υπάρχει μικρός κίνδυνος αποανωνυμοποίησης (η διαδικασία αναστρέφεται και μετατρέπεται σε προσωπικά δεδομένα.

Μειονεκτήματα: Η απώλεια της δομής δεδομένων μπορεί να προκληθεί για προγραμματιστές που επιδιώκουν να δημιουργήσουν δοκιμαστικά σύνολα δεδομένων από δεδομένα παραγωγής, καθώς τα μηδενικά ή κενά πεδία δεδομένων εμποδίζουν σημαντικά τις δυνατότητες δοκιμής εφαρμογών και μπορεί να προκαλέσουν σφάλματα εφαρμογής.

### Αντικατάσταση

Η ανωνυμοποίηση επιτυγχάνεται με την αντικατάσταση των πεδίων αναγνώρισης προσωπικών δεδομένων με πλαστά προσωπικά δεδομένα. Η ανωνυμοποίηση αντικατάστασης περιλαμβάνει είτε την εναλλαγή προσαρμοσμένων διαμορφωμένων δεδομένων από έναν πίνακα είτε τη χρήση αλγορίθμου για τη δημιουργία τυχαίων δεδομένων που ταιριάζουν με την αναμενόμενη τιμή για τον τύπο πεδίου.

Εικόνα 14. Παράδειγμα αλγορίθμου ανωνυμοποίησης αντικατάστασης

| Data Subject Name (personal data identifier) | Disabilities |
|---|---|
| Alice Smith | Vision impairment |
| Bob Johnson | None |
| Dave Doe | deaf or hard of hearing |
| Eve Jackson | None |
| Grace Chan | Mental health |

**Personal Data**



| Data Subject Name (personal data identifier) | Disabilities |
|---|---|
| Rgwko Bkgoeoe | Vision impairment |
| Ekgogks Gbkoskfso | None |
| Gege Wuiwgb | deaf or hard of hearing |
| Boxoe Bolw | None |
| Pogiw Bikskwekm | Mental health |

**Anonymized Data**

Πλεονεκτήματα: Το ανωνυμοποιημένο σύνολο δεδομένων διατηρεί τη δομή του, επομένως είναι μια κατάλληλη τεχνική ανωνυμοποίησης για τη δημιουργία δεδομένων δοκιμής ποιότητας παραγωγής για χρήση στη φάση δοκιμής του Κύκλου Ζωής Ανάπτυξης Λογισμικού (SDLC) και για την αναπαραγωγή θεμάτων εφαρμογής ως μέρος της υποστήριξης.</ li>

Μειονεκτήματα: Υπάρχει πιθανότητα να χαθούν άμεσα ή έμμεσα πεδία αναγνώρισης προσωπικών δεδομένων και να παραμείνουν μη ανακαλυφθέντα μέσα στο σύνολο δεδομένων. Καθώς τα πραγματικά προσωπικά δεδομένα εντός του ανωνυμοποιημένου δεδομένων μπορεί να είναι δύσκολο να παρατηρηθούν και να επαληθευτούν.

### Απόκρυψη δεδομένων

Η κάλυψη δεδομένων είναι ένα υβρίδιο των τεχνικών ανωνυμοποίησης αντικατάστασης και μηδενισμού και ανωνυμοποιεί τα προσωπικά δεδομένα αντικαθιστώντας χαρακτήρες πεδίου με χαρακτήρα «μάσκα». Η κάλυψη δεδομένων χρησιμοποιείται ευρέως στον κλάδο των καρτών πληρωμής, για να επιτρέψει την αναγνώριση των καρτών πληρωμής χωρίς κίνδυνο απάτης, με τη χρήση κάλυψης για την μερική αποκάλυψη του κύριου αριθμού λογαριασμού μιας κάρτας πληρωμής, π.χ. 1234 56 XX XXXX 1234. Μπορεί να είστε εξοικειωμένοι με αυτήν τη συγκεκριμένη χρήση της κάλυψης σε αποδείξεις πληρωμής, αντίγραφα κίνησης και σε εφαρμογές ηλεκτρονικής τραπεζικής.

Πλεονεκτήματα: Η κάλυψη μπορεί να μειώσει τον κίνδυνο απορρήτου όταν απαιτείται κοινή χρήση, εμφάνιση ή εκτύπωση προσωπικών δεδομένων.

Μειονεκτήματα: Αν και η κάλυψη προσωπικών δεδομένων είναι κατάλληλη για πεδία αναγνωριστικού λογαριασμού και αριθμού αναφοράς, μπορεί να είναι μια αδύναμη μορφή ανωνυμοποίησης δεδομένων με άλλους τύπους πεδίων, καθώς τα καλυμμένα προσωπικά δεδομένα ενδέχεται να εξακολουθούν να είναι είτε αναγνωρίσιμα είτε αναστρέψιμα, π.χ. Ο Τζον Σμιθ, με μάσκα σε J *Sm** θα μπορούσε ακόμα να είναι αρκετός για την αναγνώριση ενός υποκειμένου δεδομένων.

### Scrambling \ shuffling

Η σύγχυση ή η ανακάτεμα δεδομένων είναι μια μέθοδος αντικατάστασης όπου το προσωπικό σύνολο δεδομένων χρησιμοποιείται αποκλειστικά για την εναλλαγή «στήλων» δεδομένων. Στο απλό παράδειγμα που φαίνεται στο Σχήμα 3, τα επώνυμα έχουν ανακατευτεί για να δημιουργηθεί ένα ανώνυμο σύνολο δεδομένων.

Εικόνα 15. Παράδειγμα τυχαίας αναπαραγωγής δεδομένων

| First Name | Surname | Age |
|---|---|---|
| Alice | Smith | 42 |
| Bob | Johnson | 21 |
| Dave | Doe | 74 |
| Eve | Jackson | 44 |
| Grace | Chang | 32 |

**Personal Data**




| First Name | Surname | Age |
|---|---|---|
| Alice | Doe | 42 |
| Bob | Jackson | 21 |
| Dave | Chang | 74 |
| Eve | Smith | 44 |
| Grace | Johnson | 32 |

**Anonymized Data**

Πλεονεκτήματα: Το ανώνυμο σύνολο δεδομένων διατηρεί τη δομή του, επομένως παραμένει κατάλληλο για χρήση ως δεδομένα δοκιμής.

Μειονεκτήματα: Η ανακάτεμα δεδομένων ενέχει σημαντικό κίνδυνο αποανωνυμοποίησης, δεδομένου ότι το ανώνυμα σύνολο δεδομένων θα μπορούσε να συγκεντρωθεί ξανά μαζί για την αναγνώριση ατόμων. Ο αλγόριθμος ανακάτεμα κινδυνεύει επίσης να αποκρυπτογραφηθεί. Στο παράδειγμα που φαίνεται στο Σχήμα 3, τα ανώνυμα δεδομένα θα μπορούσαν να αντιστραφούν μηχανικά με διασταύρωση των πεδίων ονόματος και ηλικίας μιας εγγραφής με ένα σύνολο δεδομένων τρίτου μέρους ή αποκρυπτογραφώντας τον αλγόριθμο τυχαίας αναπαραγωγής, ο οποίος αντικαθιστά το πεδίο επωνύμου που είχε δύο εγγραφές μπροστά κάθε φορά.

### Συγκέντρωση \ γενίκευση

Η συγκέντρωση ή η γενίκευση δεδομένων είναι μια τεχνική ανωνυμοποίησης δεδομένων όπου τα προσωπικά δεδομένα αναλύονται και στη συνέχεια αποδίδονται σε μια στατιστική ή συνοπτική μορφή, αφαιρώντας τα αναγνωριστικά προσωπικών δεδομένων ως μέρος της διαδικασίας.

Πλεονεκτήματα: Η συγκέντρωση μπορεί να μειώσει τον κίνδυνο απορρήτου για ορισμένους τύπους συνόλων δεδομένων, όπως τα δεδομένα έρευνας και τα αποτελέσματα των αναλυτικών στοιχείων μεγάλων δεδομένων. Για παράδειγμα, εάν μια εφαρμογή Ιστού έχει την απαίτηση να παρακολουθεί τη γενική τοποθεσία των χρηστών της, μια διαδικασία εφαρμογής θα μπορούσε να γενικεύσει την καταγεγραμμένη διεύθυνση IP κάθε χρήστη σε μια χώρα προέλευσης. Αυτή η διαδικασία ανωνυμοποιεί το αναγνωριστικό προσωπικών δεδομένων, δηλαδή τη διεύθυνση IP του χρήστη, ενώ παράλληλα επιτυγχάνει την απαίτηση της εφαρμογής να συνοψίζει τη γενική τοποθεσία των χρηστών.

Μειονεκτήματα: Η συγκέντρωση και η γενίκευση των προσωπικών δεδομένων έχει αξία μόνο όταν υπάρχει απαίτηση συλλογής στατιστικών ή συνοπτικών πληροφοριών για ομάδες ατόμων.

**Επαναναγνώριση**

Προκειμένου τα προσωπικά δεδομένα να θεωρούνται ανώνυμα, δεν πρέπει να υπάρχει δυνατότητα επαναπροσδιορισμού, σύμφωνα με την οποία τα άτομα μπορούν να εξακολουθήσουν να αναγνωρίζονται αντιστοιχίζοντας τα ανώνυμα δεδομένα με άλλα εξωτερικά δεδομένα, όπως δημόσια διαθέσιμες πληροφορίες σε μέσα κοινωνικής δικτύωσης και ιστότοπους ή από άλλα σύνολα δεδομένων.

Η πρόοδος στις τεχνικές εξόρυξης δεδομένων και στην ανάλυση δεδομένων σημαίνει ότι υπάρχει μεγαλύτερη πιθανότητα επαναπροσδιορισμού ανώνυμων προσωπικών δεδομένων. Για παράδειγμα, ως μέρος ενός διαγωνισμού εξόρυξης δεδομένων το 2006, το Netflix κυκλοφόρησε δημόσια 100 εκατομμύρια δίσκους με βαθμολογίες ταινιών από 500.000 πελάτες του. Το σύνολο δεδομένων ανωνυμοποιήθηκε αντικαθιστώντας τα ονόματα χρήστη του Netflix με τυχαίους αριθμούς. Δεκαέξι ημέρες μετά την κυκλοφορία, δύο ερευνητές στο Πανεπιστήμιο του Τέξας ανέφεραν ότι κατάφεραν

να προσδιορίσουν τα υποκείμενα των δεδομένων στο σύνολο δεδομένων, όχι αντιστρέφοντας τη διαδικασία ανωνυμοποίησης, αλλά διασταυρώνοντας ταξινομήσεις ταινιών και χρονικές σημάνσεις με πληροφορίες δημόσιας χρήσης στον ιστότοπο της βάσης δεδομένων ταινιών στο Διαδίκτυο , IMDb.com. Χρησιμοποιώντας αυτήν την τεχνική επαναπροσδιορισμού, οι ερευνητές μπόρεσαν να αναγνωρίσουν σημαντικό αριθμό χρηστών του Netflix. Οι ερευνητές διαπίστωσαν επίσης ότι ήταν δυνατό να αποκαλυφθεί το ιστορικό παρακολούθησης μεμονωμένων χρηστών του Netflix, το οποίο θεωρείται σοβαρή παραβίαση της ιδιωτικής ζωής, καθώς οι συνήθειες παρακολούθησης ταινιών ενός ατόμου θα μπορούσαν να αποκαλύψουν τον σεξουαλικό του προσανατολισμό.

**Δοκιμή επαναναγνώρισης**

Οι προγραμματιστές θα πρέπει να επιδιώξουν να επαληθεύσουν ότι όλες οι διαδικασίες ανωνυμοποίησης προσωπικών δεδομένων είναι επαρκείς, κανονίζοντας τα ανώνυμα σύνολα δεδομένων να ελέγχονται από έναν κατάλληλα καταρτισμένο ελεγκτή διείσδυσης. Αποτελεί βέλτιστη πρακτική ασφάλειας για τις εφαρμογές να ελέγχονται διείσδυσης εντός της φάσης δοκιμής του SDLC. Οι προγραμματιστές θα πρέπει να διασφαλίζουν ότι η δοκιμή επαναπροσδιορισμού όλων των ανώνυμων συνόλων δεδομένων περιλαμβάνεται στο πεδίο της δοκιμής διείσδυσης. Συμπεριλαμβανομένης της διαδικασίας εφαρμογής και της δημιουργίας ανώνυμων συνόλων δεδομένων από τον προγραμματιστή. δηλαδή τη δημιουργία δεδομένων δοκιμής.

Η δοκιμή επαναπροσδιορισμού ανώνυμων δεδομένων θα πρέπει να περιλαμβάνει:

Προσπάθεια ταυτοποίησης ατόμων με ένα ή περισσότερα προσωπικά δεδομένα

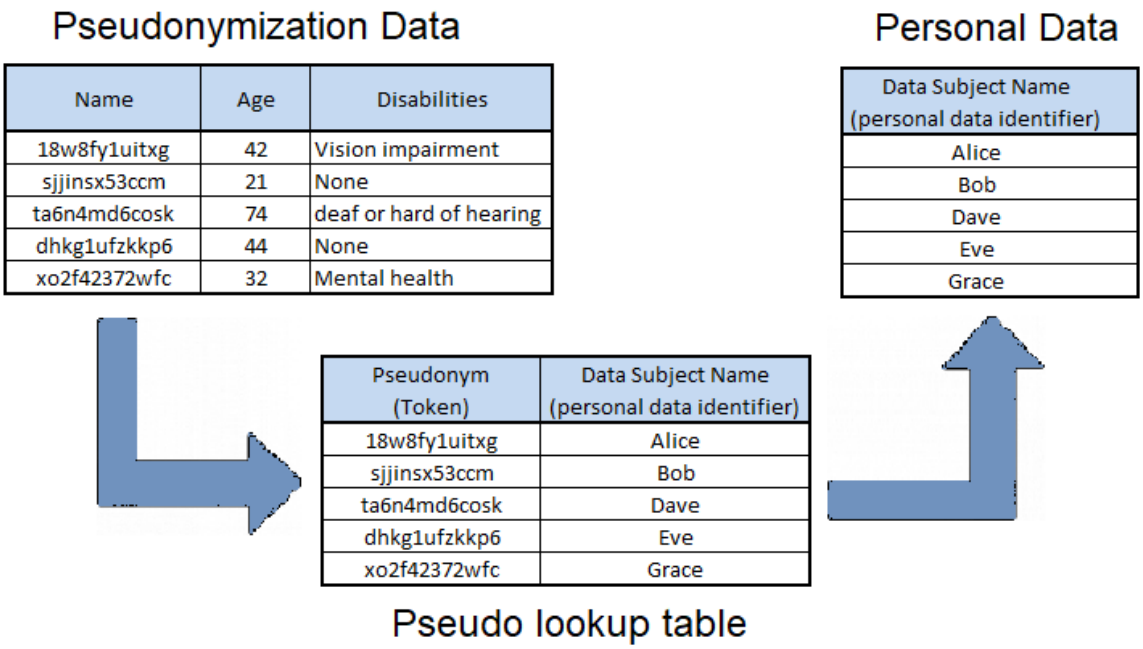
Προσπάθεια αναστροφής της διαδικασίας ανωνυμοποίησης

Χρήση δημοσίως διαθέσιμων και νομίμως αποκτηθέντων δεδομένων για την αναγνώριση ατόμων εντός του συνόλου ανώνυμων δεδομένων

**Ψευδωνυμοποίηση**

Η ψευδωνυμοποίηση αναφέρεται στο άρθρο 4 του ΓΚΠΔ και είναι μια διαδικασία που αντικαθιστά τα αναγνωριστικά προσωπικών δεδομένων με ρεαλιστικά φανταστικά δεδομένα, γνωστά ως ψευδώνυμο ή διακριτικό. Σε αντίθεση με την ανωνυμοποίηση, η ψευδωνυμοποίηση των προσωπικών δεδομένων έχει σκοπό να επιτρέψει την εκ νέου αναγνώριση των προσωπικών δεδομένων όταν απαιτείται. Μια τιμή ψευδωνύμου αντικαθιστά τα πεδία προσωπικών δεδομένων στο σύνολο δεδομένων της εφαρμογής. Αυτή η αντικατάσταση δεδομένων παρακολουθείται σε έναν ξεχωριστό πίνακα αναζήτησης, ο οποίος στη συνέχεια μπορεί να χρησιμοποιηθεί για την εκ νέου αναγνώριση των προσωπικών δεδομένων.

**Εικόνα 16. Ψευδωνυμοποίηση**




Η ψευδωνυμοποίηση μειώνει τον κίνδυνο απορρήτου της εφαρμογής μετακινώντας τα αναγνωριστικά προσωπικών δεδομένων σε έναν ξεχωριστό διακομιστή βάσης δεδομένων, ο οποίος είναι συνήθως απομονωμένος από το περιβάλλον δικτύου της εφαρμογής. Εάν το σύνολο δεδομένων εφαρμογής που περιέχει δεδομένα ψευδωνυμοποίησης έχει παραβιαστεί, ένας εισβολέας ή τρίτο μέρος δεν έχει τη δυνατότητα να αναζητήσει την ψευδοτιμή και να εντοπίσει τα υποκείμενα των προσωπικών δεδομένων.

*Άρθρο 4 παράγραφος 5«ψευδώνυμος» σημαίνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών, υπό την προϋπόθεση ότι αυτές οι πρόσθετες πληροφορίες τηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα για να διασφαλιστεί ότι τα προσωπικά δεδομένα δεν αποδίδονται σε αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο.*

Η ψευδωνυμοποίηση είναι επίσης γνωστή ως tokenization και μπορεί να ρυθμιστεί ώστε να παρέχει δεδομένα διακριτικού που ταιριάζουν με τον τύπο του πεδίου και την αναμενόμενη τιμή δεδομένων, επιτρέποντας ακόμη και σε βάσεις δεδομένων παλαιού τύπου να διατηρήσουν τη δομή. Οι λύσεις Tokenization χρησιμοποιούνται από το Apple Pay, το Samsung Pay και το Android Pay για την αποφυγή απάτης με κάρτες πληρωμών, αποθηκεύοντας μια συμβολική αξία σε κάθε έξυπνο τηλέφωνο αντί για έναν αριθμό κάρτας πληρωμής. Όταν ζητείται πληρωμή με κάρτα έξυπνου τηλεφώνου, το διακριτικό που διατηρείται στο έξυπνο τηλέφωνο αποστέλλεται και αντιστοιχίζεται με τα αποθηκευμένα στοιχεία της κάρτας πληρωμής που βρίσκονται σε ένα ασφαλές κέντρο δεδομένων, όπου γίνεται η επεξεργασία της πληρωμής. Οι λύσεις Tokenization έχουν αποδειχθεί δημοφιλείς στον κλάδο των καρτών πληρωμής (PCI), καθώς μειώνουν τον κίνδυνο απάτης με κάρτες

πληρωμών και παραβιάσεων δεδομένων και μειώνουν σημαντικά το οργανωτικό κόστος μειώνοντας σημαντικά τον αριθμό των απαιτήσεων των προτύπων ασφάλειας δεδομένων PCI με τις οποίες πρέπει να συμμορφώνεται ένας οργανισμός.

Συμπερασματικά, η χρήση του tokenization από εφαρμογές θα πρέπει να θεωρείται ως αποδεδειγμένη τεχνολογία για τη μείωση των γενικών εξόδων και του κόστους συμμόρφωσης με τον GDPR, ενώ ταυτόχρονα μετριάζεται ο κίνδυνος απορρήτου του υποκειμένου των δεδομένων, με την ψευδωνυμοποίηση να αναφέρεται ειδικά ως επιλογή μετριασμού του κινδύνου στο άρθρο 32 παράγραφος 1.

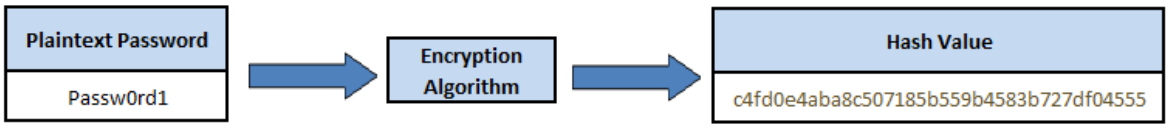
*Άρθρο 32 παράγραφος 1…ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσουν ένα επίπεδο ασφάλειας κατάλληλο για τον κίνδυνο, συμπεριλαμβανομένων άλλως κατά περίπτωση (α) την ψευδωνυμοποίηση και την κρυπτογράφηση των προσωπικών δεδομένων,*

**Κατακερματισμός**

Ο κατακερματισμός είναι μια μορφή ψευδωνυμοποίησης που χρησιμοποιεί έναν μαθηματικό αλγόριθμο για να μετατρέψει τα πεδία προσωπικών δεδομένων σε σκοτεινές αλφαριθμητικές συμβολοσειρές σταθερού μήκους, γνωστές ως τιμές κατακερματισμού ή αναλύσεις μηνυμάτων. Ο κατακερματισμός πεδίων απλού κειμένου σε τιμές κατακερματισμού προορίζεται να είναι μια μονόδρομη διαδικασία μετασχηματισμού δεδομένων, καθώς ένας αλγόριθμος κατακερματισμού δεν είναι αναστρέψιμος. δηλαδή, μπορεί να μετατρέψει μια τιμή κατακερματισμού ξανά σε απλό κείμενο. Ο κατακερματισμός χρησιμοποιείται συνήθως από εφαρμογές για την επαλήθευση εισόδων απλού κειμένου κατακερματίζοντας μια τιμή εισόδου απλού κειμένου χρησιμοποιώντας έναν καθορισμένο αλγόριθμο κατακερματισμού. η προκύπτουσα τιμή κατακερματισμού μπορεί να ελεγχθεί έναντι μιας προηγουμένως υπολογισμένης και αποθηκευμένης τιμής κατακερματισμού. Εάν οι τιμές κατακερματισμού είναι οι ίδιες, είναι εξαιρετικά πιθανό η εισαγωγή απλού κειμένου και το αρχικό κατακερματισμένο κείμενο να είναι ίδια. Ο μετριασμός του κινδύνου απορρήτου είναι ότι οι τιμές απλού κειμένου δεν διατηρούνται στο σύνολο δεδομένων.

Οι εφαρμογές θα πρέπει να χρησιμοποιούν κατακερματισμό για να προστατεύουν τους κωδικούς πρόσβασης που βρίσκονται σε βάσεις δεδομένων, αποθηκεύοντας τιμές κατακερματισμού κωδικών πρόσβασης αντί για κωδικούς πρόσβασης απλού κειμένου. Όταν ένας χρήστης εισάγει έναν κωδικό πρόσβασης απλού κειμένου κατά τη διαδικασία ελέγχου ταυτότητας, η εφαρμογή μετατρέπει τον κωδικό πρόσβασης απλού κειμένου χρησιμοποιώντας τον καθορισμένο αλγόριθμο κατακερματισμού σε τιμή κατακερματισμού και, στη συνέχεια, ελέγχει εάν ταιριάζει με τον κατακερματισμό κωδικού πρόσβασης που διατηρείται στη βάση δεδομένων. Σε περίπτωση παραβίασης της βάσης δεδομένων της εφαρμογής, αν και οι τιμές κατακερματισμού κωδικού πρόσβασης είναι ορατές και προσβάσιμες, δεν μπορούν να χρησιμοποιηθούν για έλεγχο ταυτότητας λογαριασμού και είναι σχεδόν αδύνατο να αντιστραφούν οι τιμές κατακερματισμού σε κωδικούς πρόσβασης απλού κειμένου.

Εικόνα 17. Κατακερματισμός κωδικού πρόσβασης

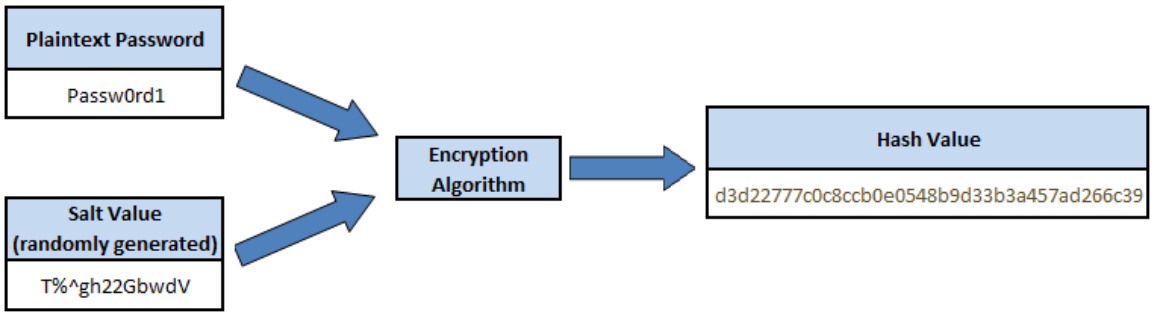



| Username | Password (hashed) |
|---|---|
| Alice | c4fd0e4aba8c507185b559b4583b727df04555 |
| Bob | 1809c34c89e13c9f056d461f5e252d1d24f188eb |
| Dave | 317db6ad17e98c88c064debdc5ae8d274b6b2433 |
| Eve | c051dfe501477eadeae8d14340123ac9f25b9b6a |
| Grace | 41882e3b02d38b11bf6fc739b2a07bf321c7 |

**Application Table**

Ενώ ο κατακερματισμός προορίζεται να είναι μη αναστρέψιμος, είναι δυνατό να επιχειρήσετε να σπάσετε τις τιμές κατακερματισμού χρησιμοποιώντας έναν πίνακα ουράνιου τόξου, ο οποίος είναι μια μεγάλη προ-υπολογισμένη λίστα όλων των πιθανών τιμών κατακερματισμού σε τιμές απλού κειμένου. Ωστόσο, «αλατώνοντας» τον τύπο κατακερματισμού προσθέτοντας μια μοναδική παράμετρο εγγραφής και χρησιμοποιώντας ισχυρούς αλγόριθμους κατακερματισμού όπως ο SHA-512, μειώνει σημαντικά την πιθανότητα επαναφοράς των τιμών κατακερματισμού αντίστροφης μηχανικής στην τιμή απλού κειμένου. Δεδομένης της χρήσης ενός αλατιού, ένας εισβολέας θα έπρεπε να υπολογίσει εκ των προτέρων έναν μοναδικό πίνακα ουράνιου τόξου, ενώ η χρήση ενός ισχυρού αλγορίθμου κατακερματισμού όπως ο SHA-512, ο οποίος χρησιμοποιεί 512 bit, σημαίνει ότι θα χρειαζόταν τεράστια ποσότητα ισχύος υπολογιστή και ώρα για τη δημιουργία του πίνακα ουράνιου τόξου, καθιστώντας τη μέθοδο επίθεσης μη βιώσιμη.

Εικόνα 18. Κατακερματισμός αλατισμένου κωδικού πρόσβασης




| Username | Password (hashed) | Unique Salt |
|---|---|---|
| Alice | d3d22777c0c8ccb0e0548b9d33b3a457ad266c39 | T%^gh22GbwdV |
| Bob | 5ef0000cb4f7f7d62dad6924e9a55012f9fa578 | caca71a46aeb |
| Dave | 91d12a6eca1784fef394ad7f265bd122fbe07daa | e31f31d9761f |
| Eve | 017f545cfcba28d9121b18d1656fd41f30190ac8 | 7524acf2458c |
| Grace | 19b5e89fa2e871fe6c0ec3ac194b4682471c56b6 | 8c540bd11008 |

**Application Table**

Η επιβεβλημένη ισχύς κωδικού πρόσβασης χρήστη της εφαρμογής είναι ένα άλλο βασικό στοιχείο για την προστασία των κατακερματισμένων κωδικών πρόσβασης σε παραβιασμένα σύνολα δεδομένων. Ο κίνδυνος από επιθέσεις λεξικών και ωμής βίας, οι οποίες μπορούν να χρησιμοποιήσουν παραβιασμένες τιμές κατακερματισμού για την επαλήθευση της επιτυχίας, μπορεί να μειωθεί σημαντικά με την επιβολή σύνθετων κωδικών πρόσβασης χρηστών 8 ή περισσότερων χαρακτήρων.

Ένας πολύπλοκος κωδικός πρόσβασης θεωρείται ότι περιλαμβάνει τουλάχιστον ένα από τα ακόλουθα:

Κεφάλαιο γράμμα

Πεζό γράμμα

Αριθμητικό ψηφίο

Ειδικός χαρακτήρας (#, $, *, %)

Ενώ ο κατακερματισμός αποφεύγει την επιβάρυνση διαχείρισης της κρυπτογράφησης και μπορεί να διαδραματίσει ρόλο στον μετριασμό του κινδύνου απορρήτου στην προστασία των κωδικών πρόσβασης, τα περισσότερα πεδία προσωπικών δεδομένων που απαιτούνται από τις εφαρμογές συνήθως δεν ταιριάζουν με την προσέγγιση κατακερματισμού ψευδωνυμοποίησης.

**Κρυπτογράφηση προσωπικών δεδομένων**

Η κρυπτογράφηση δεδομένων είναι η μέθοδος που μπορεί να μειώσει σημαντικά τον κίνδυνο απορρήτου και θα πρέπει να λαμβάνεται υπόψη όταν η ανωνυμοποίηση και η ψευδωνυμοποίηση δεν είναι βιώσιμες επιλογές για την προστασία των προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία από μια εφαρμογή. Ωστόσο, η κρυπτογράφηση προσωπικών δεδομένων έχει ένα βασικό κόστος διαχείρισης και πιθανές αδυναμίες ασφάλειας που πρέπει να εκτιμήσουν οι προγραμματιστές πριν σχεδιάσουν και εφαρμόσουν κρυπτογράφηση προσωπικών δεδομένων.

Ο GDPR δεν απαιτεί ρητά την κρυπτογράφηση των προσωπικών δεδομένων, αλλά αναφέρεται στη χρήση κρυπτογράφησης στα άρθρα 6, 32 και 34 και στην αιτιολογική σκέψη 83. Σύμφωνα με το άρθρο 34, εάν τα δεδομένα της εφαρμογής είναι κρυπτογραφημένα και στη συνέχεια χαθούν ή κλαπούν χωρίς μέσα (το ιδιωτικό κλειδί) για την αποκρυπτογράφηση του, η απώλεια δεδομένων δεν θα συνιστούσε υψηλό κίνδυνο για τους χρήστες (υποκείμενα των δεδομένων) και ως εκ τούτου δεν χρειάζεται να αναφέρεται. Αυτό σημαίνει ότι τα κρυπτογραφημένα προσωπικά δεδομένα χωρίς τα μέσα για την αποκρυπτογράφηση τους, δεν μπορούν πλέον να θεωρούνται προσωπικά δεδομένα.

*Άρθρο 6 παράγραφος 4Όταν η επεξεργασία για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή σε Το δίκαιο της Ένωσης ή του κράτους μέλους που συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των στόχων που αναφέρονται στο*

*άρθρο 23 παράγραφος 1, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβώσει εάν η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο η συλλέγονται αρχικά προσωπικά δεδομένα, λάβετε υπόψη, μεταξύ άλλων: (ε) την ύπαρξη κατάλληλων διασφαλίσεων, οι οποίες μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.*

*Άρθρο 32 παράγραφος 1… ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσουν ένα επίπεδο ασφάλειας κατάλληλο για τον κίνδυνο, συμπεριλαμβανομένων άλλωστε κατά περίπτωση (α) η ψευδωνυμοποίηση και η κρυπτογράφηση των προσωπικών δεδομένων,*

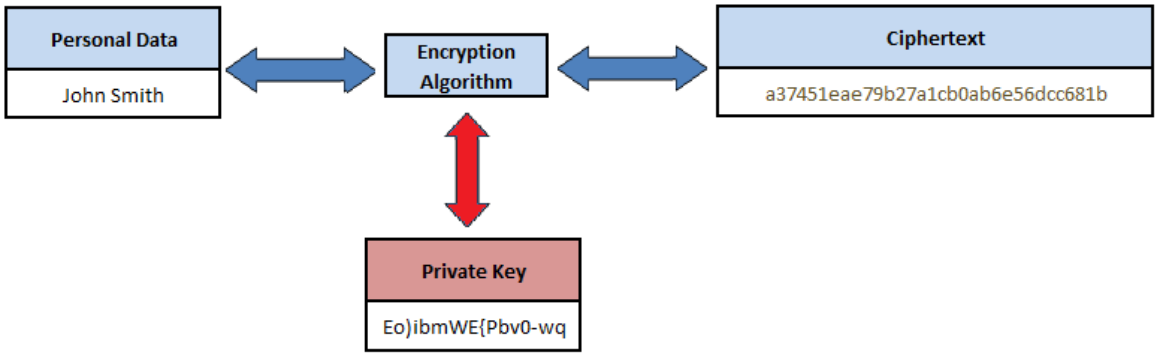
*Αιτιολογική σκέψη (83)(1) Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας κοινοποιεί η παραβίαση προσωπικών δεδομένων στο υποκείμενο των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση. (3) …δεν απαιτείται η επικοινωνία στο υποκείμενο των δεδομένων που αναφέρεται στην παράγραφο 1 εάν πληρούται οποιαδήποτε από τις ακόλουθες προϋποθέσεις: (α) ο υπεύθυνος επεξεργασίας έχει εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας και τα μέτρα αυτά εφαρμόστηκαν σε τα προσωπικά δεδομένα που επηρεάζονται από την παραβίαση προσωπικών δεδομένων, ιδίως εκείνα που καθιστούν τα προσωπικά δεδομένα ακατανόητα σε οποιοδήποτε άτομο που δεν έχει εξουσιοδότηση πρόσβασης σε αυτά, όπως η κρυπτογράφηση,*

*Άρθρο 34Για να διατηρηθεί η ασφάλεια και να αποτραπεί η επεξεργασία κατά παράβαση του παρόντος κανονισμού, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να αξιολογεί τους εγγενείς κινδύνους της επεξεργασίας και να εφαρμόζει μέτρα μετριάστε αυτούς τους κινδύνους, όπως η κρυπτογράφηση.*

**Επισκόπηση κρυπτογράφησης**

Η κρυπτογράφηση δεδομένων χρησιμοποιεί έναν μαθηματικό κρυπτογραφικό αλγόριθμο με έναν κωδικό μυστικού κλειδιού για τη μετατροπή προσωπικών δεδομένων από «απλό κείμενο» σε «κρυπτογραφημένο κείμενο» το οποίο δεν είναι αναγνώσιμο χωρίς τη γνώση του μυστικού κλειδιού για να αντιστρέψει τη διαδικασία κρυπτογράφησης, όπως απεικονίζεται στο Σχήμα 7. Οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι είναι θεωρείται ασφαλές έναντι επίθεσης, αλλά το μυστικό ή ιδιωτικό κλειδί είναι η Αχίλλειος πτέρνα με κρυπτογράφηση, δεδομένου ότι εάν το κλειδί παραβιαστεί από έναν εισβολέα, θα έχει τη δυνατότητα να αποκρυπτογραφήσει τα δεδομένα.

**Εικόνα 19. Συμμετρική κρυπτογράφηση**




Υπάρχουν διάφορες λύσεις κρυπτογράφησης λογισμικού και υλικού που μπορούν να χρησιμοποιηθούν από εφαρμογές για την κρυπτογράφηση προσωπικών δεδομένων. Η διαχείριση της κρυπτογράφησης μπορεί να γίνει πλήρως από την εφαρμογή, να εκτελεστεί απευθείας στον διακομιστή της βάσης δεδομένων ή να χρησιμοποιηθούν αποκλειστικές συσκευές διαχείρισης κρυπτογράφησης γνωστές ως Hardware Security Modules (HSM). Εκτός από την κρυπτογράφηση της βάσης δεδομένων, υπάρχει κρυπτογράφηση συστήματος αρχείων, για την προστασία προσωπικών δεδομένων σε προσωρινά αρχεία διακομιστή εφαρμογών, μέσα σε αρχεία καταγραφής ελέγχου και σε αντίγραφα ασφαλείας δεδομένων.

**Μέθοδοι κρυπτογράφησης**

Υπάρχουν δύο κύριοι τύποι μεθόδων κρυπτογράφησης: κρυπτογράφηση συμμετρικού κλειδιού και κρυπτογράφηση ασύμμετρου κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού χρησιμοποιεί ένα μόνο ιδιωτικό κλειδί, για παράδειγμα, το AES-256. Η κρυπτογράφηση ασύμμετρου κλειδιού χρησιμοποιεί έναν συνδυασμό δημόσιας κοινόχρηστων και ιδιωτικών κλειδιών για να επιτρέψει σε δύο μέρη να κρυπτογραφήσουν δεδομένα μέσω μιας μη αξιόπιστης σύνδεσης, για παράδειγμα, χρησιμοποιώντας ψηφιακά πιστοποιητικά, τον αλγόριθμο RSA. Η κρυπτογράφηση προσωπικών δεδομένων εφαρμογής χρησιμοποιεί συνήθως κρυπτογράφηση συμμετρικού κλειδιού, η οποία απαιτεί ένα μόνο ιδιωτικό κλειδί για προστασία και ασφαλή διαχείριση.

**Διαχείριση ιδιωτικού κλειδιού**

Υπάρχει ένας αριθμός διαδικασιών στη διαχείριση ιδιωτικών κλειδιών κρυπτογράφησης που πρέπει να ληφθούν υπόψη στο σχεδιασμό μιας εφαρμογής που σκοπεύει να χρησιμοποιήσει κρυπτογράφηση δεδομένων, συμπεριλαμβανομένων των περιπτώσεων όπου η εφαρμογή θα βασίζεται σε τρίτο μέρος για την παροχή ή τη διαχείριση της κρυπτογράφησης.

Δημιουργία κλειδιών: Τα ιδιωτικά κλειδιά που δημιουργήθηκαν πρόσφατα θα πρέπει να δημιουργούνται τυχαία. Δεν πρέπει να συγχέεται με τη δημιουργία κωδικού πρόσβασης ή φράσης πρόσβασης, τα μήκη ενός κλειδιού κρυπτογράφησης είναι συνήθως 128 bit ή μεγαλύτερα και θα πρέπει να δημιουργούνται χρησιμοποιώντας μια γεννήτρια τυχαίων αριθμών ή μια γεννήτρια

ψευδοτυχαίων αριθμών. Αυτό διασφαλίζει ότι τα ιδιωτικά κλειδιά σχηματίζονται εντελώς τυχαία, μειώνοντας τον κίνδυνο εικασίας ή αντιστροφής των κλειδιών.

Αποθήκευση κλειδιού: Τα ιδιωτικά κλειδιά πρέπει πάντα να αποθηκεύονται και να διατηρούνται με ασφάλεια, ακόμη και όταν χρησιμοποιούνται από την εφαρμογή για την κρυπτογράφηση και την αποκρυπτογράφηση προσωπικών δεδομένων. Ένα ιδιωτικό κλειδί δεν πρέπει ποτέ να είναι «hardcoded» της εφαρμογής, δηλαδή γραμμένο στον κώδικα της εφαρμογής, καθώς αυτό αυξάνει σημαντικά την πιθανότητα να τεθεί σε κίνδυνο η κρυπτογράφηση. Αυτό περιλαμβάνει κατακερματισμό ή κωδικοποίηση του κλειδιού κρυπτογράφησης για να συγκαλύψει την τιμή του ιδιωτικού κλειδιού μέσα στον κώδικα. Δεδομένου ότι το ιδιωτικό κλειδί πρέπει να είναι προσβάσιμο από την εφαρμογή για την εκτέλεση κρυπτογράφησης και αποκρυπτογράφησης, και η αποθήκευση αυτού του κλειδιού, έστω και προσωρινά, παρουσιάζει σημαντικό κίνδυνο για την ανατροπή της κρυπτογράφησης, η λύση είναι να κρυπτογραφηθεί και το ιδιωτικό κλειδί. Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας το κλειδί κρυπτογράφησης κλειδιού (KEK), μια διαδικασία που συνήθως υποστηρίζεται από ένα στοιχείο εκτός της εφαρμογής, όπως ένα HSM. Είναι σημαντικό η ισχύς του KEK να είναι τουλάχιστον τόσο ισχυρή όσο η ισχύς κρυπτογράφησης προσωπικών δεδομένων, διαφορετικά η ισχύς κρυπτογράφησης προσωπικών δεδομένων θεωρείται ότι έχει αποδυναμωθεί σε σχέση με την ισχύ του KEK. Τα ιδιωτικά κλειδιά μπορούν επίσης να κρατηθούν και να κληθούν από ένα ασφαλές θησαυροφυλάκιο κωδικών πρόσβασης, που προστατεύεται από μια ξεχωριστή διαδικασία κρυπτογράφησης. Τα ιδιωτικά κλειδιά θα πρέπει να αποθηκεύονται σε όσο το δυνατόν λιγότερες τοποθεσίες.

Διανομή κλειδιού: Τα ιδιωτικά κλειδιά πρέπει να μεταδίδονται με ασφάλεια προς και από την εφαρμογή. Η προσβασιμότητα στο ιδιωτικό κλειδί πρέπει να ελέγχεται αυστηρά με βάση την “ανάγκη να γνωρίζω” και η πρόσβαση στο κλειδί να κλειδώνεται ανάλογα.

Αλλαγή\περιστροφή κλειδιού (κρυπτογραφική περίοδος): Η τακτική αλλαγή του ιδιωτικού κλειδιού είναι μια συμμετρική βέλτιστη πρακτική κρυπτογράφησης, καθώς μειώνει την αξία του ιδιωτικού κλειδιού στους εισβολείς. Το χρονικό διάστημα κατά το οποίο απαιτείται αλλαγή στο ιδιωτικό κλειδί ονομάζεται κρυπτογραφική περίοδος και πρέπει να ορίζεται με βάση τον κίνδυνο. Τουλάχιστον δύο βασικές αλλαγές ανά έτος θεωρούνται βέλτιστη πρακτική για την προστασία ευαίσθητων δεδομένων. Οι εφαρμογές που διαχειρίζονται τη δική τους κρυπτογράφηση πρέπει να παρέχουν τη δυνατότητα στους διαχειριστές να αλλάζουν τακτικά τα ιδιωτικά κλειδιά.

Διαγραφή κλειδιού: Τα ιδιωτικά κλειδιά που δεν χρησιμοποιούνται πλέον ή χρειάζονται πρέπει να διαγραφούν για να διασφαλιστεί ότι δεν μπορούν να χρησιμοποιηθούν για την αποκρυπτογράφηση παλαιότερων εκδόσεων κρυπτογραφημένων προσωπικών δεδομένων που ενδέχεται να υπάρχουν. δηλαδή, όπως διατηρείται σε παλιά αντίγραφα ασφαλείας ή παλαιότερα άγνωστα χαμένα ή παραβιασμένα σύνολα δεδομένων.

**Απαιτήσεις ασφάλειας εφαρμογής GDPR**

Ο GDPR δεν παρέχει συγκεκριμένους και περιγραφικούς ελέγχους ασφάλειας πληροφορικής ή ασφάλειας εφαρμογών. Αντίθετα, στο άρθρο 32 ορίζει την «εφαρμογή κατάλληλου επιπέδου ασφάλειας πληροφοριών». Το κατάλληλο επίπεδο ασφάλειας για μια εφαρμογή καθορίζεται από το συνδυασμό της τήρησης των βέλτιστων πρακτικών ασφαλείας του κλάδου και με την υιοθέτηση μιας προσέγγισης αξιολόγησης κινδύνου. Το τελευταίο καλύπτεται από την Εκτίμηση Επιπτώσεων στην Ασφάλεια Δεδομένων, η οποία περιγράφεται λεπτομερώς στο δεύτερο μέρος αυτής της σειράς οδηγιών GDPR.

*Άρθρο 32 παράγραφος 1Λαμβάνοντας υπόψη την εξέλιξη της τεχνολογίας, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας καθώς και κίνδυνος ποικίλης πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίσουν ένα επίπεδο ασφάλειας κατάλληλο για τον κίνδυνο >, συμπεριλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:*

*(α) την ψευδωνυμοποίηση και την κρυπτογράφηση προσωπικών δεδομένων*

*(β) την ικανότητα να διασφαλίζεται η συνεχής εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών επεξεργασίας*

*(γ) δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε προσωπικά δεδομένα εγκαίρως σε περίπτωση φυσικού ή τεχνικού συμβάντος*

*(δ) μια διαδικασία τακτικής δοκιμής, αξιολόγησης και αξιολόγησης της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας*

**Βέλτιστη πρακτική για την ασφάλεια εφαρμογών**

Για να συμμορφωθούν με το άρθρο 32 παράγραφος 1γ), να διασφαλίσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των προσωπικών δεδομένων που διαχειρίζονται οι εφαρμογές, οι προγραμματιστές θα πρέπει να ακολουθούν βέλτιστες πρακτικές ασφάλειας εφαρμογών αναγνωρισμένες από τον κλάδο, όπως η ανάπτυξη της εφαρμογής σύμφωνα με τις δέκα κορυφαίες αρχές του Open Web Application Security Project (OWASP).

OWASP Top Ten 2017:

Ένεση

Αποτελέσματα ελέγχου ταυτότητας και διαχείριση περιόδου σύνδεσης

Έκθεση ευαίσθητων δεδομένων

Εξωτερική οντότητα XML (XXE)

Διακοπή ελέγχου πρόσβασης

Εσφαλμένη διαμόρφωση ασφαλείας

Σενάρια μεταξύ ιστοτόπων (XSS)

Ασφαλής αποζωνοποίηση

Χρήση στοιχείων με γνωστά τρωτά σημεία

Ανεπαρκής καταγραφή και παρακολούθηση

**Διασφάλιση της ασφάλειας των εφαρμογών της συμμόρφωσης GDPR με το IBM® Security AppScan**

Για να συμμορφωθούν με το άρθρο 33 παράγραφος 1δ), να διασφαλίσουν τη δοκιμή, την αξιολόγηση και την αξιολόγηση της αποτελεσματικότητας των τεχνικών μέτρων που διασφαλίζουν την επεξεργασία προσωπικών δεδομένων από την εφαρμογή, οι προγραμματιστές θα πρέπει να πραγματοποιούν διεξοδικές δοκιμές ασφάλειας εφαρμογών και σάρωση ευπάθειας κατά τη φάση δοκιμών SDLC. Το IBM Security AppScan είναι ένα εργαλείο σάρωσης ευπάθειας εφαρμογών Ιστού που μπορεί να χρησιμοποιηθεί για την επαλήθευση και την αναφορά της συμμόρφωσης με την ασφάλεια μιας εφαρμογής τόσο με το Top Ten του OWASP όσο και με τον GDPR.

**Συμμόρφωση GDPR για την ασφάλεια εφαρμογών IoT**

Οι εφαρμογές που αναπτύχθηκαν για τη διαχείριση συσκευών Internet of Things (IoT) επεξεργάζονται συχνά προσωπικά δεδομένα και επομένως εμπίπτουν στο πεδίο εφαρμογής της συμμόρφωσης με τον GDPR.

**Αποκάλυψη παραβίασης δεδομένων**

Τα άρθρα 33 και 34 του ΓΚΠΔ τονίζουν την ανάγκη για ισχυρή ασφάλεια της εφαρμογής, δεδομένου ότι οποιαδήποτε αστοχία στην ασφάλεια της εφαρμογής που προκαλεί παραβίαση προσωπικών δεδομένων πρέπει να αναφέρεται από τον υπεύθυνο επεξεργασίας σε μια εποπτική αρχή εντός 72 ωρών και στα υποκείμενα των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση.

*Άρθρο 33 παράγραφος 1Σε περίπτωση παραβίασης προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει χωρίς αδικαιολόγητη καθυστέρηση και, όπου είναι δυνατόν, το αργότερο 72 ώρες μετά την ενημερωθείτε για την παραβίαση προσωπικών δεδομένων στην εποπτική αρχή.*

*Άρθρο 34 παράγραφος 1Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας κοινοποιεί την προσωπική παραβίαση δεδομένων προς το υποκείμενο των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση.*

Όταν ένας οργανισμός ανάπτυξης εφαρμογών δεν έχει ρόλο ελεγκτή, ο αναπτυσσόμενος οργανισμός εξακολουθεί να διατρέχει τον κίνδυνο σημαντικής ζημιάς στη φήμη του κοινού και των πελατών,

ειδικά όπου η αδύναμη ασφάλεια εφαρμογών έχει προκαλέσει μεγάλης κλίμακας ή σοβαρές παραβιάσεις προσωπικών δεδομένων.

**Συμπέρασμα**

Υπάρχει ένας αριθμός διαφορετικών τεχνικών λύσεων που μπορούν να μειώσουν σημαντικά τον κίνδυνο απορρήτου μιας εφαρμογής και να διευκολύνουν τη συμμόρφωση ενός οργανισμού με τον GDPR. Κάθε λύση μετριασμού του κινδύνου απορρήτου έχει αδυναμίες ασφάλειας και συμβιβασμούς που πρέπει να γίνουν πλήρως κατανοητές και να ληφθούν υπόψη κατά τον σχεδιασμό της εφαρμογής. Για παράδειγμα, η ανωνυμοποίηση δεδομένων και η ψευδωνυμοποίηση έχουν τον κίνδυνο να υποστούν αντίστροφη μηχανική, ενώ η κρυπτογράφηση δεδομένων έχει το γενικό κόστος να απαιτεί ισχυρές διαδικασίες διαχείρισης κλειδιών. Αφού καθοριστούν στο σχεδιασμό, τα μέτρα μετριασμού της προστασίας της ιδιωτικής ζωής της εφαρμογής πρέπει να εξεταστούν για να διασφαλιστεί ότι η εφαρμογή έχει αναπτυχθεί για να παρέχει ένα πρότυπο προστασίας δεδομένων και ένα επίπεδο κινδύνου για την ιδιωτική ζωή, το οποίο θεωρείται κατάλληλο από τις εποπτικές αρχές του GDPR.

Ο GDPR δεν ορίζει ένα περιγραφικό σύνολο απαιτήσεων ασφάλειας πληροφορικής και εφαρμογών, αντίθετα, ο κανονισμός απαιτεί την υιοθέτηση «ενδεδειγμένου επιπέδου ασφάλειας πληροφοριών». Δεδομένου του σημαντικού κινδύνου ασθενούς ασφάλειας εφαρμογών που οδηγεί σε παραβιάσεις προσωπικών πληροφοριών με μεγάλο αντίκτυπο, συμπεριλαμβανομένων μαζικών παραβιάσεων δεδομένων, η ανάπτυξη και η δοκιμή εφαρμογών για αποδεδειγμένες πρακτικές ασφάλειας εφαρμογών θα πρέπει να θεωρείται ως σημείο αναφοράς για την επίτευξη μιας «συμβατής» εφαρμογής GDPR. Η ανάπτυξη εφαρμογών που συμμορφώνονται με τις αρχές του OWASP Top Ten και η δοκιμή εφαρμογών για τρωτά σημεία ασφαλείας χρησιμοποιώντας το IBM Security AppScan, αποτελούν βασικές πρακτικές SDLC για τη μείωση του οργανωτικού κινδύνου μη συμμόρφωσης με τον GDPR και, το πιο σημαντικό, για την προστασία του απορρήτου των χρηστών της εφαρμογής.

## 2.5.2 Hardware και projects στο IoT

Connected συσκευές είναι κεντρικές στο IoT. Οι συσκευές συλλέγουν δεδομένα και παρακολουθούν παραμέτρους. Βρίσκονται σε όλα, από βιομηχανικό εξοπλισμό, κτίρια και αυτοκίνητα, μέχρι ζώα, αποστολές φορτίου, αγωγούς και ανθρώπους.

Τα στοιχεία υλικού και λογισμικού έχουν σχεδιαστεί για εφαρμογές IoT μέσω ενός τυπικού πρωτοκόλλου σχεδίασης: ανάπτυξη προδιαγραφών, εννοιολογική σχεδίαση, πρωτότυπο, δοκιμή και, τελικά, διάθεση υλικού και λογισμικού ενσωματωμένου σε ένα δίκτυο. Ορισμένες πλατφόρμες, όπως το Arduino και το Raspberry Pi, ενδέχεται να επισπεύσουν τη σχεδίαση και να επιτρέψουν την

ταχεία δημιουργία πρωτοτύπων χωρίς να απαιτείται προσαρμογή, επιταχύνοντας έτσι τον χρόνο που απαιτείται για την υλοποίηση μιας διαμόρφωσης IoT.

Ο σχεδιασμός θα απαιτεί αναγνώριση των απαιτήσεων απόδοσης, του απαραίτητου υλικού και λογισμικού για την επίτευξη τέτοιων απαιτήσεων, ακολουθούμενες από προδιαγραφές για εξαρτήματα – είτε εμπορικά εκτός ραφιού (COTS) είτε προσαρμοσμένα σχέδια – με τη δέουσα προσοχή στο περιβάλλον λειτουργίας και την εφαρμογή που πρέπει να χρησιμοποιείται μέσα σε αυτό.

Στο πλαίσιο του IoT, μια συσκευή αναφέρεται σε οτιδήποτε αποκτά πληροφορίες και τις μεταδίδει. Για παράδειγμα, ένας αισθητήρας πίεσης μέσα σε έναν αγωγό, ένας αισθητήρας θερμοκρασίας μέσα σε βαγόνι ψύξης ή μικροσκοπικά τσιπ που εισάγονται κάτω από το δέρμα μιας αγελάδας σε μια διάσπαρτη ακοή – είναι όλα συσκευές. Οι συσκευές μπορεί να είναι μόνες τους ή να λειτουργούν σε συγχρονισμό με άλλες συσκευές.

Σε αυτό το άρθρο, θα εξετάσω ορισμένες επιλογές υλικού εκτός ραφιού και ορισμένους παράγοντες που πρέπει να λάβετε υπόψη κατά την επιλογή τους για την ανάπτυξη του επόμενου έργου IoT σας.

Χαρακτηριστικά συσκευής IoT

Καθώς αναπτύσσεται το τοπίο του IoT, θα παρουσιαστούν νέες συσκευές και πλατφόρμες. Υπάρχουν βασικά χαρακτηριστικά που είναι κοινά στις συσκευές IoT που παρέχουν μια βάση σύγκρισης κατά την επιλογή υλικού και λογισμικού για τη διαμόρφωση ενός νέου δικτύου IoT ή για την ανάπτυξη και επέκταση ενός υπάρχοντος.Οι συσκευές IoT μπορούν να χαρακτηρίζονται από δυνατότητες:

Απόκτηση και έλεγχος δεδομένων

Επεξεργασία και αποθήκευση δεδομένων

Συνδεσιμότητα

Διαχείριση ενέργειας

Απόκτηση και έλεγχος δεδομένων

Η Απόκτηση δεδομένων (***DAQ***) συλλέγει αναλογικές πληροφορίες σε ένα σταθερό χρονικό διάστημα (ο ρυθμός δειγματοληψίας δεδομένων) , και το μεταδίδει ως ψηφιακό σήμα σε μια απομακρυσμένη συσκευή εξόδου για ψηφιακή ανάγνωση. Το DAQ μπορεί να περιλαμβάνει ρύθμιση σήματος (για τον χειρισμό και την κλιμάκωση των ακατέργαστων μετρήσεων του αισθητήρα) και μετατροπείς αναλογικού σε ψηφιακό για τη μετατροπή των μετρήσεων του αναλογικού αισθητήρα σε ψηφιακές τιμές, ώστε να είναι δυνατή η επεξεργασία και η ανάλυσή τους.

Οι Αισθητήρες είναι στοιχεία που μετρούν φυσικές μεταβλητές και τις μετατρέπουν σε ηλεκτρικά σήματα (τάσεις). Οι αισθητήρες είναι διαθέσιμοι στο εμπόριο, εκτός αγοράς και έχουν καθοριστεί για τη μέτρηση μιας σειράς μεταβλητών που περιλαμβάνουν: θερμοκρασία, υγρασία, πίεση, καπνός,

αέριο, φως, ήχος, δόνηση, ροή αέρα, ροή νερού, ταχύτητα, επιτάχυνση , εγγύτητα, θέση GPS, υψόμετρο και πολλές άλλες μεταβλητές.

Οι αισθητήρες διαφέρουν ως προς τη λειτουργικότητά τους και μπορούν να χρησιμοποιηθούν για τη μέτρηση μιας μεγάλης ποικιλίας συνθηκών. Για παράδειγμα, αισθητήρες ιδιοδεκτικότητας παρακολουθούν την εσωτερική κατάσταση της συσκευής. Αισθητήρες όπως κουμπιά, συρόμενα χειριστήρια ή οθόνες αφής μπορούν να χρησιμοποιηθούν για άμεση αλληλεπίδραση με μια συσκευή (Διασύνδεση ανθρώπου-μηχανής).

Κάθε τύπος αισθητήρα έχει πολλές επιλογές. Οι κατασκευαστές και οι προδιαγραφές προϊόντων αισθητήρων τους ποικίλλουν. Η ακρίβεια, η ακρίβεια και η απαιτούμενη κατάσταση λειτουργίας του αισθητήρα μπορεί να διαφέρουν από κατάλογο σε κατάλογο και από κατασκευαστή σε κατασκευαστή. Οι αισθητήρες μπορούν να χρησιμοποιηθούν μέσα σε έναν κινητήρα, υποβρύχια, ενσωματωμένοι σε ανθρώπους ή ζώα, ακόμη και στο διάστημα. Τα περιβάλλοντα απαιτούν διαφορετικά χαρακτηριστικά αισθητήρα και είναι σχεδιασμένα για διαφορετικές χρήσεις ανάλογα.

Ένα σημαντικό χαρακτηριστικό των στοιχείων του αισθητήρα είναι η ανάλυση. Η ανάλυση ενός αισθητήρα αντιπροσωπεύει τη μικρότερη ποσότητα αλλαγής που μπορεί να διαβάσει αξιόπιστα ο αισθητήρας και σχετίζεται με το μέγεθος της αριθμητικής τιμής που χρησιμοποιείται για την αναπαράσταση των πρωτογενών μετρήσεων του αισθητήρα. Για παράδειγμα, ένας αναλογικός αισθητήρας θερμοκρασίας με ανάλυση 10 bit αντιπροσωπεύει μια ένδειξη θερμοκρασίας χρησιμοποιώντας μια αριθμητική τιμή μεταξύ 0 και 1023. Τα bit είναι δυαδικά, επομένως τα 10 bit παρέχουν δύο στην ισχύ του 10 ή 1024 πιθανές τιμές συνολικά. Ωστόσο, στην πράξη, οι αισθητήρες επηρεάζονται από ηλεκτρικό θόρυβο που μειώνει την πραγματική ανάλυση.

Ενώ οι αισθητήρες μετατρέπουν μια φυσική μεταβλητή όπως η θερμοκρασία σε ηλεκτρικό σήμα, οι συσκευές εξόδου είναι το αντίστροφο: μετατρέπουν ένα ηλεκτρικό σήμα σε φυσικό αποτέλεσμα. Οι συσκευές εξόδου περιλαμβάνουν LED, ηχεία και οθόνες. Αυτό μπορεί να απαιτεί ενεργοποιητές όπως κινητήρες, ρελέ και ηλεκτρομαγνητικές βαλβίδες που ενεργοποιούν φυσικά κάτι. Οι ενεργοποιητές είναι συνηθισμένοι σε βιομηχανικές εφαρμογές IoT. Για παράδειγμα, οι πνευματικοί γραμμικοί ενεργοποιητές υιοθετούνται ευρέως στην κατασκευή για να μετακινούν και να συγκρατούν προϊόντα κατά τη διάρκεια της διαδικασίας συναρμολόγησης. Ένας ενεργοποιητής σε έναν άξονα σχολικού λεωφορείου μπορεί να ενεργοποιήσει το φρενάρισμα όταν ανιχνευτεί δυσμενής κίνηση. Μια υψηλή θερμοκρασία σε ένα δοχείο ψύξης με προϊόντα μέσα, μπορεί να ενεργοποιήσει συναγερμό όταν μια θερμοκρασία ανεβαίνει σε ένα συγκεκριμένο απαράδεκτο επίπεδο.

Επεξεργασία και αποθήκευση δεδομένων

Οι συσκευές IoT απαιτούν συγκεκριμένη ικανότητα επεξεργασίας και αποθήκευσης δεδομένων. Αυτό βοηθά στην επίτευξη συγκέντρωσης, μετάδοσης και ανάλυσης δεδομένων. Ορισμένες συσκευές IoT ενδέχεται να επεξεργάζονται δεδομένα απευθείας, ενώ άλλες μεταδίδουν αυτά τα

δεδομένα σε άλλες συσκευές, συσκευές πύλης ή εφαρμογές cloud για περαιτέρω συγκέντρωση και ανάλυση.

Το Edge analytics εκτελεί ανάλυση δεδομένων στα άκρα ενός δικτύου και όχι σε μια κεντρική τοποθεσία. Τα δεδομένα μπορούν να αναλυθούν σε πραγματικό χρόνο στις ίδιες τις συσκευές ή μπορούν να αναλυθούν σε μια κοντινή συσκευή πύλης (όπως ένας δρομολογητής) που είναι συνδεδεμένη με τις συσκευές IoT, αντί για τη μετάδοση μεγάλου όγκου δεδομένων ανάντη σε διακομιστή cloud ή κέντρο δεδομένων για περαιτέρω ανάλυση. Η επεξεργασία δεδομένων στην άκρη συγκεντρώνει και φιλτράρει τα δεδομένα καθώς συλλέγονται, με μόνο τα πιο σημαντικά δεδομένα να αποστέλλονται ανάντη. Το Edge analytics μειώνει τις απαιτήσεις επεξεργασίας και αποθήκευσης μειώνει το φόρτο του δικτύου.

Η ισχύς επεξεργασίας και η αποθήκευση που χρησιμοποιούνται από μια εφαρμογή IoT εξαρτάται από την επεξεργασία που απαιτείται από τις υπηρεσίες ή τις εφαρμογές που καταναλώνουν τα δεδομένα. Διαθέσιμες προδιαγραφές μνήμης και επεξεργαστή, ταχύτητα ρολογιού και αριθμός πυρήνων, τα οποία καθορίζουν στη συνέχεια τον ρυθμό επεξεργασίας δεδομένων των συσκευών. Η χωρητικότητα του μη πτητικού φλας, το οποίο χρησιμοποιείται για τη διατήρηση δεδομένων έως ότου μεταδοθούν ανάντη, καθορίζει πόσα δεδομένα μπορούν να αποθηκευτούν στη συσκευή. Οι συσκευές που εκτελούν αναλύσεις άκρων απαιτούν σημαντικά περισσότερες δυνατότητες επεξεργασίας από τις συσκευές που εκτελούν μόνο βασική επεξεργασία δεδομένων όπως επικύρωση, κανονικοποίηση, κλιμάκωση ή μετατροπή μετρήσεων.

Συνδεσιμότητα

Η συνδεσιμότητα δικτύου είναι ένα καθοριστικό χαρακτηριστικό οποιασδήποτε συσκευής IoT. Οι συσκευές επικοινωνούν με άλλες συσκευές τοπικά. Στη συνέχεια δημοσιεύουν δεδομένα μέσω υπηρεσιών που βασίζονται σε σύννεφο. Ορισμένες συσκευές επικοινωνούν ασύρματα, χρησιμοποιώντας τεχνολογίες 802.11 (Wi-Fi), Bluetooth, RFID, δίκτυα κινητής τηλεφωνίας ή τεχνολογίες ευρείας περιοχής χαμηλής κατανάλωσης (LPWAN), όπως LoRa, SigFox ή NB-IoT. Η ενσύρματη επικοινωνία είναι κατάλληλη για σταθερές συσκευές. Τέτοιες συσκευές μπορούν να εγκατασταθούν σε έξυπνα κτίρια, οικιακούς αυτοματισμούς και εφαρμογές βιομηχανικού ελέγχου, για παράδειγμα, και να συνδεθούν με Ethernet ή να τοποθετηθούν εκ των υστέρων με Ethernet μέσω τροφοδοσίας. Η σειριακή επικοινωνία είναι μια μορφή ενσύρματης συνδεσιμότητας μεταξύ συσκευών, χρησιμοποιώντας τυπικά πρωτόκολλα όπως Universal Asynchronous Receiver Transmitter (UART) ή το πρωτόκολλο Controller Area Network (CAN), το οποίο διαθέτει προέλευση από την αυτοκινητοβιομηχανία.

Διαχείριση ενέργειας

Η διαχείριση ενέργειας είναι ένας κρίσιμος παράγοντας για φορητές και φορητές συσκευές IoT που βασίζονται σε ασύρματη πηγή ενέργειας, όπως μπαταρίες ή φωτοβολταϊκά στοιχεία (ηλιακή). Ανάλογα με τα μοτίβα χρήσης και τις απαιτήσεις ισχύος των συνδεδεμένων αισθητήρων, ενεργοποιητών ή ολοκληρωμένων κυκλωμάτων (IC), μια συσκευή μπορεί να τίθεται σε κατάσταση

αναστολής λειτουργίας ή σε λειτουργία χαμηλής κατανάλωσης περιοδικά για εξοικονόμηση ενέργειας.

Για παράδειγμα, ένας υπολογιστής μονής πλακέτας όπως ο Raspberry Pi 4 απαιτεί περίπου 700 – 1000 mA ρεύματος για να λειτουργήσει υπό τυπική χρήση. Εάν μεταδίδατε δεδομένα συνεχώς μέσω ενός δικτύου Wi-Fi ή εάν η συσκευή υπό βαρύ φορτίο εκτελούσε πολλή επεξεργασία δεδομένων, η κατανάλωση ενέργειας θα ήταν υψηλή, αλλά στη συνέχεια θα έπεφτε όταν η συσκευή έμενε σε αδράνεια. Εάν συνδέσετε μια μονάδα κάμερας, η απαιτούμενη ένταση ρεύματος αυξάνεται κατά περίπου 250 mA όταν η κάμερα χρησιμοποιείται. Επίσης, οι αισθητήρες συνήθως απαιτούν ρεύμα για να λειτουργήσουν. οι ακίδες GPIO στο Raspberry Pi τροφοδοτούν 3,3V ή 5V, έως ένα σύνολο ρεύματος 50mA σε όλες τις ακίδες. Η κατανάλωση ενέργειας της συσκευής αυξάνεται καθώς αυξάνετε τον αριθμό των εξαρτημάτων που είναι συνδεδεμένα στις ακίδες.

Τύποι standard υλικού για τη δημιουργία πρωτοτύπων του έργου IoT

Η ανάπτυξη εφαρμογών IoT είναι πιο προσιτή με την αυξανόμενη διαθεσιμότητα χαμηλού κόστους, εμπορικά διαθέσιμων πλακών ανάπτυξης υλικού, πλατφορμών και κιτ πρωτοτύπων. Τα αρθρωτά σχέδια υλικού παρέχουν μεγάλη ευελιξία. Με μεγαλύτερη επιλογή εξαρτημάτων, οι σχεδιαστές μπορούν να αντικαταστήσουν νέους αισθητήρες με διαφορετικές προδιαγραφές. Εναλλακτικά, μπορείτε να αναβαθμίσετε ανεξάρτητα τις μονάδες δικτύωσης, επεξεργασίας δεδομένων ή αποθήκευσης μιας συσκευής για τις εξελισσόμενες απαιτήσεις.

Πολλές εμπορικές standard συσκευές, συμπεριλαμβανομένων μικροελεγκτών και υπολογιστών με μία πλακέτα, έχουν σχεδιαστεί γύρω από ολοκληρωμένα κυκλώματα System-on-a-Chip (SoC). Τα SoC συνδυάζουν δυνατότητες όπως η επεξεργασία δεδομένων, η αποθήκευση και η δικτύωση σε ένα μόνο τσιπ. Αυτή η διαμόρφωση σημαίνει ότι θυσιάζεις κάποια ευελιξία για λόγους ευκολίας, αλλά, ευτυχώς, υπάρχει ένας τεράστιος αριθμός συσκευών εμπορευμάτων που διατίθενται με μια σειρά διαμορφώσεων για να διαλέξεις. Για παράδειγμα, ο Πίνακας 1 παραθέτει τις τεχνικές προδιαγραφές για μια επιλογή μικροελεγκτών που μπορούν να χρησιμοποιηθούν για τη δημιουργία πρωτοτύπων έργων IoT και παρέχει μια σύγκριση τριών δημοφιλών Single-board-Computers (SBC).

Πλακέτες ανάπτυξης μικροελεγκτών

Ένας μικροελεγκτής είναι ένα SoC που παρέχει δυνατότητες επεξεργασίας και αποθήκευσης δεδομένων. Οι μικροελεγκτές περιέχουν έναν πυρήνα (ή πυρήνες) επεξεργαστή, μνήμη (RAM) και διαγράψιμη προγραμματιζόμενη μνήμη μόνο για ανάγνωση (EPROM) για την αποθήκευση των προσαρμοσμένων προγραμμάτων που εκτελούνται στον μικροελεγκτή. Οι Οι πλακέτες ανάπτυξης μικροελεγκτών είναι PCB με πρόσθετο κύκλωμα για την υποστήριξη του μικροελεγκτή ώστε να είναι πιο βολικό το πρωτότυπο και ο προγραμματισμός του τσιπ.

Οι αισθητήρες και οι ενεργοποιητές συνδέονται με τον μικροελεγκτή μέσω ψηφιακών ή αναλογικών ακίδων Είσοδος/Έξοδος γενικής χρήσης (GPIO) ή μέσω διαύλου υλικού. Τυπικά πρωτόκολλα επικοινωνίας όπως ***I2C*** και ***SPI*** χρησιμοποιούνται για επικοινωνία εντός της συσκευής με τα στοιχεία

που είναι συνδεδεμένα με το δίαυλο. Η υιοθέτηση προτύπων διευκολύνει την προσθήκη ή την εναλλαγή στοιχείων που συνδέονται με το δίαυλο.

Το Arduino (***http://arduino.cc/en/Main/***) είναι μια πλατφόρμα συσκευών ανοιχτού κώδικα, με μια ενεργή κοινότητα που δημιουργούν συμβατούς πίνακες ανάπτυξης και εργαλεία. Οι δυνατότητες της συσκευής διαφέρουν στα επίσημα μοντέλα Arduino (***https://www.arduino.cc/en/Products/Compare)</a >), καθώς και μεταξύ των δεκάδων συμβατών πλακών τρίτων κατασκευαστών. Όλες οι συσκευές είναι συμβατοί με το Arduino μικροελεγκτές, συμπεριλαμβανομένου του απανταχού Arduino Uno, του Particle's Electron, το οποίο περιλαμβάνει ένα ενσωματωμένο κινητό μόντεμ και του Espressif Systems (https://espressif.com/en/products/hardware/esp8266ex/overview) ESP8266-01, ένας μικροελεγκτής χαμηλού κόστους και χαμηλής κατανάλωσης με ενσωματωμένο wifi.***

Όπως το Arduino, το ESP8266 έχει μια ενεργή κοινότητα υιοθετητών. Οι αξιοσημείωτες πλακέτες ανάπτυξης που βασίζονται στο ESP8266 περιλαμβάνουν τα ***NodeMCU***, ***WeMos D1*** και το Feather Huzzah του AdaFruit (***https://learn.adafruit.com/adafruit-feather-huzzah-esp8266/overview***). Ένας αριθμός εναλλακτικών επιλογών υλικολογισμικού για πλακέτες που βασίζονται σε ESP8266 έχουν αναπτυχθεί από την κοινότητα ανοιχτού κώδικα και κατασκευαστών, δίνοντας τη δυνατότητα στους προγραμματιστές IoT να προγραμματίζουν αυτές τις πλακέτες χρησιμοποιώντας Lua, Python και JavaScript και να υποστηρίζουν ενημερώσεις over-the-air (OTA) .

Η τυπική προσέγγιση για την ανάπτυξη του λογισμικού που θα λειτουργεί σε μικροελεγκτές συμβατούς με Arduino είναι η χρήση C ή C++ και το Arduino IDE, ωστόσο υπάρχουν επίσης δεσμεύσεις γλώσσας και οπτικά εργαλεία προγραμματισμού που έχουν αναπτυχθεί από την κοινότητα. Οι πλακέτες συμβατές με Arduino που μοιράζονται κοινές διατάξεις καρφίτσας μπορούν να επεκταθούν χρησιμοποιώντας προαιρετικές ασπίδες τρίτων, για παράδειγμα, για προσθήκη θύρας Ethernet ή Bluetooth σε ένα Arduino Uno. Το Arduino είναι το πιο ευρέως διαδεδομένο περιβάλλον ανάπτυξης μικροελεγκτών για χομπίστες, αλλά άλλα όπως το Tessel (***https://tessel.io/***) και το Particle.io (< a href="http://particle.io/">http://particle.io) υποστηρίζει εγγενώς JavaScript, ενώ η Python υποστηρίζεται για πίνακες όπως το PyBoard της MicroPython (***http://micropython.org***) και από το WeIO (***http://we-io.net/ υλικό/***).

Η επιλογή ενός μικροελεγκτή συμβατού με Arduino διευκολύνει τη μεταφορά προγραμμάτων που έχουν αναπτυχθεί χρησιμοποιώντας τις βιβλιοθήκες Arduino και το Arduino IDE μεταξύ πλατφορμών για εκτέλεση σε άλλες συσκευές συμβατές με Arduino. Απαιτείται ακόμα η επεξεργασία και γύρω από τη λεπτή διαφορά.

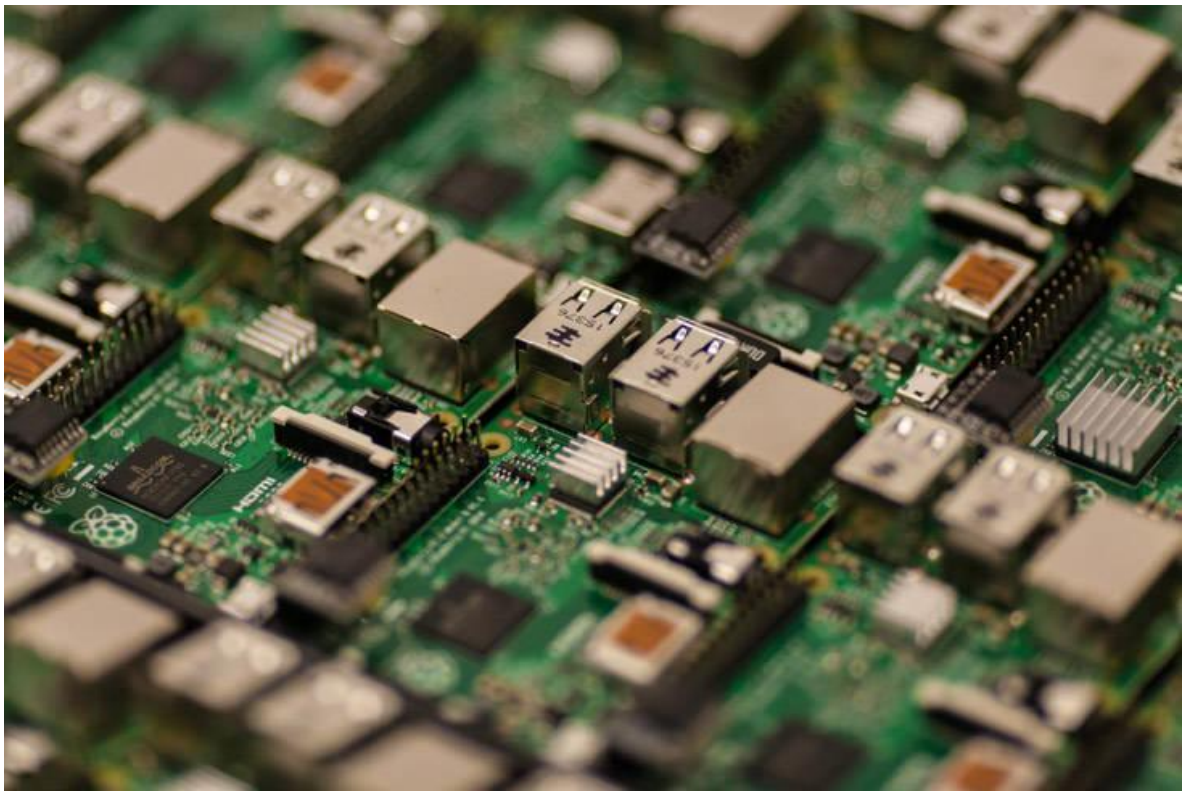
Για παράδειγμα, το Arduino Uno χρησιμοποιεί λογική 5V σε ψηφιακές ακίδες I/O (όπου 0 βολτ ισούται με LOW ή OFF και 5 volt ισούται με HIGH ή ON), αλλά οι πίνακες ESP8266 και Particle 3,3V χρησιμοποιούν λογική 3,3V (το ΥΨΗΛΟ είναι 3,3V). Αυτό μπορεί να επηρεάσει την επιλογή των εξαρτημάτων του αισθητήρα ή του ενεργοποιητή, καθώς ορισμένα εξαρτήματα λειτουργούν μόνο με

το ένα ή το άλλο. Η εναλλαγή αισθητήρων που έχουν σχεδιαστεί για λογική 5V σε 3,3V μπορεί να οδηγήσει σε απρόβλεπτα αποτελέσματα και πιθανώς να βλάψει τους ακροδέκτες που δεν είναι ανεκτικοί σε υψηλότερες τάσεις και επομένως θα χρειαστεί να προσθέσετε έναν μετατροπέα λογικού επιπέδου για να λειτουργήσει αυτό. Όταν αρχίσετε να εφαρμόζετε λειτουργίες υλικού χαμηλού επιπέδου, όπως η ενεργοποίηση της λειτουργίας βαθιάς ύπνου ή η ανάγνωση από συνδεδεμένους αισθητήρες χρησιμοποιώντας συγκεκριμένα πρωτόκολλα, πιθανότατα θα χρειαστεί να βασιστείτε σε βιβλιοθήκες για συγκεκριμένες συσκευές ή στοιχεία που θα κάνουν τον κώδικά σας λιγότερο φορητό.

Υπολογιστές μονής πλακέτας

Οι Οι υπολογιστές μιας πλακέτας (SBC) είναι ένα βήμα παραπάνω από τους μικροελεγκτές. Σας επιτρέπουν να προσαρτάτε περιφερειακές συσκευές όπως πληκτρολόγια, ποντίκια και οθόνες, καθώς και περισσότερη μνήμη και επεξεργαστική ισχύ (για παράδειγμα, μικροεπεξεργαστής ARM 32 bit 1,2 GHz σε σύγκριση με μικροελεγκτή 8 bit 16 KHz από ).

Εικόνα 20. Raspberry Pi single-board-computer



Η διάκριση μεταξύ μικροελεγκτών και υπολογιστών με μία πλακέτα είναι κάπως αυθαίρετη. Ορισμένες συσκευές, όπως το Onion Omega 2 (***https://docs.onion.io/omega2-docs/omega2.html#omega2***), βρίσκονται κάπου στο ενδιάμεσο, με σχεδόν τόση ενσωματωμένη μνήμη και ικανότητα επεξεργασίας όσο ένα SBC χαμηλού επιπέδου. Υπάρχει επίσης μια σειρά από υβριδικές

συσκευές, όπως το UDOO Quad (***http://www.udoo.org/docs/ Introduction/Introduction.html***) που ενσωματώνουν ένα σύστημα Linux που βασίζεται σε ARM με έναν μικροελεγκτή συμβατό με Arduino.

Όπως και με τους μικροελεγκτές, οι δυνατότητες της συσκευής SBC μπορούν να επεκταθούν με την προσθήκη στοιβαζόμενων πλακών επέκτασης γνωστών ως καπέλα στο Raspberry Pi και ακρωτήρια στο BeagleBone Black και με την προσθήκη εξωτερικών μονάδων , όπως ελεγκτές κινητήρα ή μετατροπείς αναλογικού σε ψηφιακό, για τον μετριασμό των περιορισμών με τις δυνατότητες της ενσωματωμένης συσκευής.

Πολλές συσκευές SBC μοιάζουν περισσότερο με mini-PC και τρέχουν ένα ενσωματωμένο λειτουργικό σύστημα, συνήθως μια βελτιωμένη διανομή Linux. Ως αποτέλεσμα, υπάρχουν πολλά περισσότερα εργαλεία ανάπτυξης και επιλογές γλώσσας που είναι διαθέσιμα για την ανάπτυξη ενσωματωμένων εφαρμογών που λειτουργούν με τους συνδεδεμένους αισθητήρες και ενεργοποιητές σε αυτές τις συσκευές παρά σε πλακέτες μικροελεγκτών. Ωστόσο, τα SBC είναι πιο περίπλοκα στη ρύθμιση, μεγαλύτερα, απαιτούν περισσότερη ενέργεια και πιο επιρρεπή σε προβλήματα όπως καταστροφή της κάρτας SD ή της μνήμης flash όπου αποθηκεύονται οι εφαρμογές.

Επιλογή μεταξύ πλακών ανάπτυξης μικροελεγκτών και υπολογιστών μονής πλακέτας

Παρόλο που οι πλακέτες ανάπτυξης μικροελεγκτών εκτός ραφιού και οι υπολογιστές με μία πλακέτα μπορεί να αποτελούν μόνο μέρος μιας λύσης IoT, είναι ιδανικοί για την εκκίνηση της ανάπτυξης μιας.

Ένας τρόπος για να ξεκινήσετε είναι να λάβετε υπόψη τα βασικά χαρακτηριστικά της συσκευής IoT υπό το φως των απαιτήσεων της εφαρμογής σας και, στη συνέχεια, να επεξεργαστείτε τις ακόλουθες αποφάσεις σχεδιασμού:

Προσδιορίστε τον τύπο και τον αριθμό των περιφερειακών αισθητήρων και των στοιχείων εξόδου που χρειάζεστε και, εάν είναι απαραίτητο, τυχόν κυκλώματα σχεδίασης για αυτά τα εξαρτήματα

Επιλέξτε έναν μικροελεγκτή ή μια συσκευή μονής πλακέτας για να συντονίσετε την ανάγνωση και τον έλεγχο των περιφερειακών στοιχείων

Αποφασίστε σχετικά με τα πρωτόκολλα επικοινωνίας δεδομένων που πρέπει να χρησιμοποιήσετε για επικοινωνία εντός της συσκευής (για παράδειγμα, χρησιμοποιώντας I2C για επικοινωνία μεταξύ του μικροελεγκτή και τυχόν συνδεδεμένων αισθητήρων)

Επιλέξτε το υλικό δικτύωσης και τα πρωτόκολλα που χρειάζεστε για να επικοινωνείτε με υπηρεσίες και εφαρμογές cloud

Για παράδειγμα, για να ρυθμίσετε ένα σύστημα οικιακού αυτοματισμού με προϋπολογισμό, μπορείτε να επιλέξετε το Raspberry Pi Zero W. Είναι μια μικρή και πολύ χαμηλού κόστους συσκευή SBC με άφθονη επεξεργαστική ισχύ και μνήμη (επεξεργαστής ARM6 1GHz και RAM 512 MB) για να εκτελούν επεξεργασία δεδομένων και αναλύσεις στη συσκευή. Υποστηρίζει επέκταση μνήμης flash με κάρτα microSD έως 64 GB για αποθήκευση προγραμμάτων και δεδομένων. Και, είναι εξοπλισμένο με μια πλήρη κεφαλίδα GPIO 40 ακίδων, ακριβώς όπως το Raspberry Pi 4, που επιτρέπει τη σύνδεση πολλών αισθητήρων και υποστηρίζει πρωτόκολλα SPI και I2C. Διαθέτει ενσωματωμένο wifi για σύνδεση με οικιακό δίκτυο και μπορεί να τροφοδοτηθεί με micro-USB από φορητό τροφοδοτικό ή τροφοδοτικό τοίχου.

Καθώς προχωράτε περαιτέρω με τη σχεδίαση τοπίου IoT, μπορείτε να σταματήσετε και να συγκρίνετε την αναμενόμενη απόδοσή σας με την πρόθεση σχεδίασης. Πραγματοποιήστε τη σχεδίαση και το πρωτότυπο της συσκευής, την επιλογή ενσωματωμένου λογισμικού και την επιλογή υπηρεσιών και εφαρμογών ανάντη, αλλά στη συνέχεια σταματήστε για να το αξιολογήσετε. Μπορείτε να αξιολογείτε περιοδικά τα πρωτότυπά σας σε σχέση με τις λειτουργικές και μη λειτουργικές σας απαιτήσεις, συμπεριλαμβανομένων των επιδόσεων, της αξιοπιστίας και της ασφάλειας, και να επανεξετάζετε αυτές τις επιλογές, όπως απαιτείται.

### Απαιτήσεις υλικού IoT για την ανάπτυξη του έργου σας IoT

Οι συσκευές IoT είναι εξαιρετικά εξειδικευμένες. Είναι σχεδιασμένα να λειτουργούν σε πολύ συγκεκριμένα περιβάλλοντα. Το υλικό για έργα IoT ποικίλλει ευρέως. Ενώ μπορείτε να δημιουργήσετε πρωτότυπο με γενικό υλικό εκτός ραφιού, μπορείτε τελικά να προχωρήσετε προς το σχεδιασμό και την ανάπτυξη προσαρμοσμένων PCB και εξαρτημάτων, προσαρμοσμένων στις απαιτήσεις των λύσεων IoT σας. Ως μέρος αυτής της διαδικασίας, θα πρέπει να λάβετε υπόψη αυτά τα είδη απαιτήσεων υλικού:

Απαιτήσεις ασφαλείας

Ευκολία ανάπτυξης

Απαιτήσεις απόκτησης, επεξεργασίας και αποθήκευσης δεδομένων

Απαιτήσεις συνδεσιμότητας

Απαιτήσεις ισχύος

Φυσική σχεδίαση συσκευής

Απαιτήσεις κόστους

Απαιτήσεις ασφαλείας

Η ασφάλεια είναι κρίσιμο στοιχείο στο IoT. Είναι επιτακτική ανάγκη να λαμβάνεται υπόψη σε όλα τα στάδια σχεδιασμού και ανάπτυξης. Η ακεραιότητα και η ασφάλεια των δεδομένων που

καταγράφονται από οποιαδήποτε συσκευή πρέπει να παραμείνουν ανέπαφα – ακόμη και κατά την κατασκευή πρωτοτύπων. Οι απαιτήσεις ασφαλείας ισχύουν για τις ίδιες τις συσκευές IoT, το δίκτυό σας και τις εφαρμογές cloud, κινητών και υπηρεσιών web.

Οι σχετικές απαιτήσεις ασφαλείας περιλαμβάνουν:

Διασφάλιση ότι κάθε συσκευή έχει αρκετή επεξεργαστική ισχύ και μνήμη για να μπορεί να κρυπτογραφεί και να αποκρυπτογραφεί δεδομένα και μηνύματα με τον ρυθμό αποστολής και λήψης τους

Διασφάλιση ότι οι βιβλιοθήκες ανάπτυξης ενσωματωμένου λογισμικού υποστηρίζουν οποιουσδήποτε μηχανισμούς εξουσιοδότησης και ελέγχου πρόσβασης χρησιμοποιούνται για τον έλεγχο ταυτότητας με υπηρεσίες και εφαρμογές upstream

Επιλογή υιοθέτησης συσκευών εκτός ραφιού που εφαρμόζουν πρωτόκολλα διαχείρισης συσκευών για την ασφαλή καταχώριση νέων συσκευών καθώς προστίθενται σε ένα δίκτυο για την αποφυγή πλαστογράφησης και εκείνων που περιλαμβάνουν δυνατότητες υλικολογισμικού για την υποστήριξη ασφαλών ενημερώσεων over the air για ενημερώσεις κώδικα ασφαλείας< /li>

Ευκολία ανάπτυξης

Κατά τη δημιουργία πρωτοτύπων, η ευκολία ανάπτυξης είναι μια άλλη απαίτηση υψηλής προτεραιότητας, ώστε να μπορείτε γρήγορα και εύκολα να θέσετε σε λειτουργία τη συσκευή σας IoT, να καταγράφετε δεδομένα και να επικοινωνείτε με άλλες συσκευές και το cloud.

Λάβετε υπόψη την προσβασιμότητα, τη διαθεσιμότητα και την ποιότητα της τεκμηρίωσης API, των εργαλείων ανάπτυξης και της υποστήριξης που προσφέρονται από τον κατασκευαστή υλικού ή από την κοινότητα ανάπτυξης. Επιλέξτε συσκευές που είναι γρήγορες και εύκολες στον προγραμματισμό και το αναβοσβήσιμο, καθώς και με χαμηλή αφή για ανάπτυξη, με μηδενική ή ελάχιστη διαμόρφωση ανά συσκευή που απαιτείται, για να μειώσετε την απογοήτευση και να εξοικονομήσετε χρόνο ενώ αναπτύσσετε τη λύση IoT.

Απαιτήσεις απόκτησης, επεξεργασίας και αποθήκευσης δεδομένων

Ο αριθμός των συνδεδεμένων αισθητήρων, η ανάλυση των δεδομένων που συλλέγονται και ο ρυθμός με τον οποίο γίνεται δειγματοληψία των δεδομένων καθορίζουν τον όγκο των δεδομένων προς επεξεργασία, γεγονός που επηρεάζει τις απαιτήσεις επεξεργασίας και αποθήκευσης δεδομένων.

Ο όγκος των δεδομένων που πρέπει να διατηρηθούν σε μια συσκευή εξαρτάται από το πόσο συχνά συνδέεται η συσκευή για τη μετάδοση δεδομένων ανάντη. Μια ενσύρματη, πάντα συνδεδεμένη συσκευή που είναι εγκατεστημένη σε ένα έξυπνο κτίριο, μια συσκευή που μεταδίδει χαμηλούς όγκους ακατέργαστων δεδομένων απευθείας σε έναν εξαιρετικά διαθέσιμο διακομιστή, θα απαιτεί λιγότερη ισχύ επεξεργασίας δεδομένων και αποθήκευση σε σύγκριση με μια συσκευή που

χρειάζεται να επεξεργαστεί μεγάλους όγκους δεδομένων σε εκρήξεις. Μια συσκευή που συνδέεται μόνο κάθε λίγες ώρες για εξοικονόμηση ενέργειας θα απαιτεί περισσότερο χώρο αποθήκευσης για την τοπική καταγραφή δεδομένων στο ενδιάμεσο.

Απαιτήσεις συνδεσιμότητας

Οι απαιτήσεις συνδεσιμότητας για ασύρματη δικτύωση περιλαμβάνουν το εύρος λειτουργίας, το πόσο μακριά θα πρέπει να μεταδοθεί το σήμα και τον αναμενόμενο όγκο και ρυθμό δεδομένων που θα μεταδοθούν. Εξετάστε την ανοχή σφαλμάτων και τη δυνατότητα μιας συσκευής να επανασυνδέεται και να προσπαθεί ξανά να στείλει δεδομένα, μετά την αποσύνδεσή της.

Το υλικό σας μπορεί να έχει ενσωματωμένη συνδεσιμότητα δικτύου όπως Bluetooth ή wifi ή αυτή η δυνατότητα μπορεί να χρειαστεί να προστεθεί με μια πλακέτα επέκτασης ή μια μονάδα. Μια εξωτερική μονάδα που μπορεί να αναβαθμιστεί μπορεί να προσφέρει μεγαλύτερη ευελιξία, καθώς έχετε την επιλογή να δοκιμάσετε διαφορετικές μονάδες για να αξιολογήσετε την εμβέλειά τους και την κατανάλωση ενέργειας.

Απαιτήσεις ενέργειας

Πολλές από τις άλλες απαιτήσεις, συμπεριλαμβανομένου του αριθμού των απαιτούμενων αισθητήρων και του ρυθμού μετάδοσης του δικτύου, θα επηρεάσουν τις απαιτήσεις ισχύος της συσκευής. Σκεφτείτε εάν η συσκευή σας θα είναι ενσύρματη για τροφοδοσία ή θα χρειάζεται μια φορητή πηγή ενέργειας όπως μπαταρία ή υπερπυκνωτής. Εάν απαιτεί φορητό τροφοδοτικό, όπως μπαταρία, πρέπει να γνωρίζετε το μέγεθος, το βάρος και τις απαιτήσεις χωρητικότητας για την μπαταρία, καθώς και εάν πρέπει να είναι επαναφορτιζόμενη, αντικαταστάσιμη ή να απορριφθεί μετά το τέλος της μπαταρίας. Εάν η συσκευή είναι επαναφορτιζόμενη, πόσο συχνά πρέπει να φορτίζεται και με ποια μέσα;

Απαιτήσεις σχεδιασμού φυσικών συσκευών

Οι απαιτήσεις σχεδιασμού φυσικής συσκευής περιλαμβάνουν την εμφάνιση και το μέγεθος της συσκευής.Πρέπει επίσης να ληφθούν υπόψη οι περιβαλλοντικές συνθήκες στις οποίες θα εγκατασταθεί η συσκευή, για παράδειγμα, θα χρειαστεί αδιάβροχο ή ανθεκτικό περίβλημα; Για παράδειγμα, μια συσκευή που είναι εγκατεστημένη στο κάτω μέρος ενός φορτηγού ως μέρος μιας εφαρμογής παρακολούθησης στόλου θα πρέπει να θωρακιστεί για να διασφαλιστεί ότι θα συνεχίσει να λειτουργεί υπό σκληρές συνθήκες. Θα πρέπει να είναι αδιάβροχο και ανθεκτικό στη βρωμιά, τους κραδασμούς και τους κραδασμούς.

Απαιτήσεις κόστους

Το κόστος του υλικού περιλαμβάνει την αρχική δαπάνη για το υλικό και τα σχετικά εξαρτήματα (όπως τυχόν αισθητήρες) καθώς και το τρέχον κόστος λειτουργίας τους, όπως το κόστος ισχύος και συντήρησης με τη μορφή αντικατάστασης φθαρμένων εξαρτημάτων ή ελαττωματικών εξαρτημάτων. Εξετάστε επίσης πιθανές χρεώσεις αδειοδότησης για ορισμένα εξαρτήματα ή προγράμματα

οδήγησης συσκευών. Η αγορά εμπορικά διαθέσιμων πλακών ανάπτυξης ή SBC μπορεί να είναι πιο οικονομική από την κατασκευή προσαρμοσμένων πλακών. Καθώς κλιμακώνετε το δίκτυό σας IoT με πολλές συσκευές, οι αποκλειστικές συσκευές υλικού μπορεί να γίνουν μια πιο σοφή εναλλακτική λύση.

Συμπέρασμα

Κάθε εφαρμογή και κατάσταση είναι διαφορετική. Δεν υπάρχει προσέγγιση «ενιαίου μεγέθους» για την επιλογή υλικού για έργα IoT. Η υιοθέτηση βασισμένου σε πρότυπα υλικού βασισμένου σε βασικά προϊόντα, όπως μικροελεγκτές ή υπολογιστές με μία πλακέτα, μπορεί να εξοικονομήσει χρόνο και έξοδα στα αρχικά στάδια ανάπτυξης, χωρίς να θυσιάζει την ευελιξία. Αυτό που μαθαίνετε στη φάση της δημιουργίας πρωτοτύπων μπορεί να σας βοηθήσει να λάβετε κρίσιμες αποφάσεις σχεδιασμού υλικού αργότερα κατά την ανάπτυξη της λύσης IoT.

## 2.5.3 Οδηγός GDPR και IoT

Εισαγωγή

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) δημιουργήθηκε από την Ευρωπαϊκή Επιτροπή και το Συμβούλιο για να ενισχύσει και να ενοποιήσει την ευρωπαϊκή νομοθεσία για την προστασία δεδομένων, αντικαθιστώντας την Ευρωπαϊκή Οδηγία για την Προστασία Δεδομένων του 1995. Παρόλο που ο GDPR είναι κανονισμός της Ευρωπαϊκής Ένωσης (ΕΕ), ισχύει για οποιουσδήποτε οργανισμούς εκτός Ευρώπης που χειρίζονται προσωπικά δεδομένα πολιτών της ΕΕ. Αυτό περιλαμβάνει την ανάπτυξη εφαρμογών που προορίζονται για την επεξεργασία προσωπικών πληροφοριών πολιτών της ΕΕ. Επομένως, οι οργανισμοί που παρέχουν εφαρμογές ιστού, εφαρμογές για κινητά ή παραδοσιακές εφαρμογές επιτραπέζιου υπολογιστή που μπορούν να επεξεργάζονται έμμεσα τα προσωπικά δεδομένα πολιτών της ΕΕ ή να επιτρέπουν τη σύνδεση πολιτών της ΕΕ υπόκεινται στις υποχρεώσεις απορρήτου του GDPR. Οι οργανισμοί αντιμετωπίζουν την προοπτική ισχυρών κυρώσεων σε περίπτωση που οι εφαρμογές δεν συμμορφωθούν με τον GDPR. Αυτό το άρθρο, το πρώτο μιας σειράς τριών μερών, συνοψίζει τον GDPR και εξηγεί πώς ο κανονισμός απορρήτου επηρεάζει και εφαρμόζεται στην ανάπτυξη και υποστήριξη εφαρμογών που προορίζονται να χρησιμοποιηθούν από πολίτες της Ευρωπαϊκής Ένωσης. Το Μέρος 2 διερευνά τον τρόπο ενσωμάτωσης της αξιολόγησης και του μετριασμού του κινδύνου απορρήτου στον κύκλο ζωής ανάπτυξης λογισμικού και Μέρος 3 παρέχει πρακτικές τεχνικές ανάπτυξης εφαρμογών που μπορούν να μετριάσουν τον κίνδυνο απορρήτου μιας εφαρμογής.

Συνέπειες της μη συμμόρφωσης με τον GDPR

Ο GDPR χορηγεί στη ρυθμιστική αρχή απορρήτου δεδομένων κάθε χώρας της ΕΕ, γνωστή ως εποπτική αρχή, διορθωτικές εξουσίες και οικονομικές κυρώσεις για να διασφαλίσει ότι οι οργανισμοί συμμορφώνονται με το δικαίωμα κάθε πολίτη της ΕΕ στο απόρρητο. Οι κυρώσεις για μη

συμμόρφωση περιλαμβάνουν πρόστιμα έως 20 εκατ. ευρώ ή 4 τοις εκατό του παγκόσμιου κύκλου εργασιών του οργανισμού και παροχή στους πολίτες της ΕΕ του νομικού δικαιώματος να διεκδικήσουν αποζημίωση για ζημίες μέσω ομαδικών αγωγών. Ο GDPR επιβάλλει επίσης την αποκάλυψη παραβιάσεων προσωπικών δεδομένων εντός 72 ωρών, η οποία μπορεί επίσης να οδηγήσει σε σημαντικές βλάβες στη φήμη και στην απώλεια της εμπιστοσύνης των καταναλωτών λόγω της αρνητικής προσοχής των μέσων ενημέρωσης.

Οι στόχοι και η επισκόπηση του GDPR

Η Οδηγία της ΕΕ για την Προστασία Δεδομένων του 1995 (95/46/ΕΚ) βασίστηκε στην ερμηνεία των απαιτήσεων κάθε εθνικής κυβέρνησης της ΕΕ, αλλά ο GDPR ισχύει ακριβώς όπως έχει διατυπωθεί, σε κάθε οργανισμό στον κόσμο που επεξεργάζεται τα προσωπικά στοιχεία των πολιτών της ΕΕ. Ο ίδιος ο κανονισμός αποτελείται από 99 άρθρα και 173 αιτιολογικές σκέψεις. Τα Άρθρα είναι οι υποχρεώσεις (απαιτήσεις), ενώ οι αιτιολογικές σκέψεις υποστηρίζουν και εξηγούν πώς πρέπει να λαμβάνονται υπόψη και να εφαρμόζονται τα Άρθρα. Μπορείτε να δείτε τα άρθρα και αιτιολογικές σκέψεις του GDPR, ωστόσο, μπορεί να είναι προκλητικά για μη νομικοί και μη επαγγελματίες απορρήτου να κατανοήσουν. Σε όλη αυτή τη σειρά, αναφέρομαι στα άρθρα και τις αιτιολογικές σκέψεις GDPR με τον αριθμό αναφοράς GDPR και ο αριθμός παραγράφου του άρθρου ακολουθεί εντός παρενθέσεων.

Βασικοί όροι και ορισμοί GDPR

Για να διασφαλίσετε ότι οι εφαρμογές αναπτύσσονται για να συμμορφώνονται με τον GDPR και να μετριάζουν τον κίνδυνο απορρήτου, θα πρέπει να κατανοήσετε καλά το δικαίωμα στην ιδιωτικότητα, τις απαιτήσεις GDPR και τους βασικούς όρους απορρήτου δεδομένων. Αυτή η γνώση μπορεί να σας βοηθήσει στο χειρισμό ερωτημάτων απορρήτου από χορηγούς έργων ανάπτυξης, Υπεύθυνους Προστασίας Δεδομένων και τους χρήστες της εφαρμογής.

Το θεμελιώδες δικαίωμα στην ιδιωτικότητα

Η ιδιωτική ζωή είναι ένα θεμελιώδες ανθρώπινο δικαίωμα που αναγνωρίζεται από τα Ηνωμένα Έθνη, στο πλαίσιο διεθνών συνθηκών και σε περισσότερα από 150 εθνικά συντάγματα. Το δικαίωμα στην ιδιωτική ζωή με την ευρεία έννοια είναι το δικαίωμα ενός ατόμου να μένει μόνο του από ανεπιθύμητη εισβολή και παρατήρηση από άλλα άτομα. Αυτό περιλαμβάνει τη μη αποκάλυψη ιδιωτικών γεγονότων για το άτομο σε τρίτους ή δημόσια χωρίς την άδειά τους. Στο ψηφιακό πλαίσιο, το δικαίωμα ενός ατόμου στην ιδιωτική ζωή συχνά παρεξηγείται ή παραμελείται. ίσως αυτό οφείλεται στον μαζικό πολλαπλασιασμό της κοινής χρήσης προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης ή στην τακτική αναφορά μεγάλων παραβιάσεων προσωπικών δεδομένων από τα μέσα ενημέρωσης. Ωστόσο, το θεμελιώδες ανθρώπινο δικαίωμα στην ιδιωτική ζωή εξακολουθεί να ισχύει τόσο στο ψηφιακό πλαίσιο όσο και στον φυσικό κόσμο. Οι κοινές παραβιάσεις του ψηφιακού απορρήτου από οργανισμούς περιλαμβάνουν:

Μη λήψη συναίνεσης από άτομα πριν από τη συλλογή και επεξεργασία των προσωπικών τους στοιχείων (με άλλα λόγια, τα προσωπικά τους δεδομένα)

Μη σαφής ενημέρωση των ατόμων σχετικά με τον τρόπο με τον οποίο θα χρησιμοποιηθούν και θα κοινοποιηθούν τα προσωπικά τους στοιχεία με άλλα μέρη

Συλλογή υπερβολικών προσωπικών πληροφοριών από άτομα χωρίς λόγο

Δεν παρέχεται σε άτομα ορατότητα και έλεγχος των προσωπικών τους στοιχείων

Δεν επιτρέπεται σε άτομα να ασκούν τα δικαιώματα απορρήτου τους

Δεν προστατεύονται επαρκώς τα προσωπικά στοιχεία (για παράδειγμα, παρέχουν κακή ασφάλεια)

Μη ενημέρωση ατόμων όταν παραβιάζονται τα προσωπικά τους στοιχεία

Ο GDPR έχει επινοηθεί για να αντιμετωπίσει αυτές τις ελλείψεις στο ψηφιακό απόρρητο, διασφαλίζοντας ότι οι οργανισμοί συμμορφώνονται πλήρως με το δικαίωμα ενός ατόμου στο ψηφιακό απόρρητο, μέσω του ορισμού ενός περιγραφικού συνόλου υποχρεώσεων απορρήτου που πρέπει να ακολουθήσουν οι οργανισμοί.

Θέμα δεδομένων

Υποκείμενο δεδομένων είναι το άτομο με το οποίο σχετίζονται τα προσωπικά δεδομένα.

Προσωπικά δεδομένα

Ως προσωπικά δεδομένα ορίζεται κάθε πληροφορία που μπορεί να χρησιμοποιηθεί για την ταυτοποίηση ενός ατόμου, συμπεριλαμβανομένου έμμεσα μέσω ψευδωνύμου ή αριθμού αναφοράς. Τα παραδείγματα προσωπικών δεδομένων περιλαμβάνουν τα εξής:

Όνομα

Αναγνωριστικό χρήστη εφαρμογής

Διεύθυνση ηλεκτρονικού ταχυδρομείου (ακόμη και σε αυτές που δεν περιλαμβάνουν όνομα)

Αριθμός λογαριασμού

Φόρουμ και διαδικτυακές λαβές

Οποιοδήποτε άλλο αναγνωριστικό που μπορεί να αναζητηθεί σε μια βάση δεδομένων για την αναγνώριση ενός ατόμου

Βιομετρικά δεδομένα, συμπεριλαμβανομένων των γενετικών δεδομένων

Δεδομένα τοποθεσίας

Δεδομένα τοποθεσίας

Τα δεδομένα τοποθεσίας θεωρούνται προσωπικά δεδομένα σύμφωνα με τον GDPR και είναι οποιαδήποτε δεδομένα μπορούν να χρησιμοποιηθούν για τον προσδιορισμό του τόπου που ζει, εργάζεται ή παίζει ένα άτομο. Οι προγραμματιστές θα πρέπει να γνωρίζουν ότι οι συμβολοσειρές cookie, οι διευθύνσεις IP, τα δεδομένα γεωγραφικών ετικετών και τα αναγνωριστικά κινητής συσκευής θεωρούνται όλα προσωπικά δεδομένα, δεδομένου ότι αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για τον εντοπισμό και την αναγνώριση ενός ατόμου.

Πιθανά κρυφά προσωπικά δεδομένα εντός εφαρμογών

Οι προγραμματιστές θα πρέπει να αναγνωρίσουν ότι τα πεδία πληροφοριών που από μόνα τους δεν ταξινομούνται ως προσωπικά δεδομένα μπορούν να γίνουν προσωπικά δεδομένα όταν συνδυάζονται με άλλα πεδία σε ένα αρχείο. Οι προγραμματιστές θα πρέπει να ελέγχουν την πιθανή χρήση οποιωνδήποτε πεδίων ελεύθερου κειμένου από την εφαρμογή, όπου υπάρχει εύλογη πιθανότητα ότι τα πεδία κειμένου θα μπορούσαν να περιέχουν προσωπικά δεδομένα (για παράδειγμα, μέσω εισαγωγής χρήστη), τέτοια πεδία κειμένου θα πρέπει να θεωρούνται προσωπικά δεδομένα. *Άρθρο 4 παράγραφος 1 "προσωπικά δεδομένα" σημαίνει κάθε πληροφορία που σχετίζεται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο δεδομένων»). ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο που μπορεί να αναγνωριστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε ένα αναγνωριστικό όπως ένα όνομα, ένας αριθμός αναγνώρισης, δεδομένα τοποθεσίας, ένα διαδικτυακό αναγνωριστικό ή σε έναν ή περισσότερους παράγοντες ειδικούς για το φυσικό, φυσιολογικό, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα ενός φυσικού προσώπου.* Τα προσωπικά δεδομένα που έχουν ψευδωνυμοποιηθεί (με άλλα λόγια, μέθοδοι κωδικοποίησης κλειδιού, όπως η κωδικοποίηση και η κρυπτογράφηση) εξακολουθούν να θεωρούνται προσωπικά δεδομένα, ανάλογα με το πόσο δύσκολο είναι να αποδοθεί το ψευδώνυμο στην ταυτοποίηση ενός ατόμου. Ανατρέξτε στο Μέρος 3 αυτής της σειράς για περισσότερες λεπτομέρειες σχετικά με την ψευδωνυμοποίηση. Όταν ένα ή περισσότερα πεδία σε μια εγγραφή μπορούν να προσδιορίσουν ένα άτομο, τα άλλα πεδία της ίδιας εγγραφής που περιέχουν προσωπικά στοιχεία για το αναγνωρισμένο άτομο θεωρούνται επίσης προσωπικά δεδομένα. Τα προσωπικά δεδομένα δεν μπορούν να υποβληθούν σε επεξεργασία από εφαρμογές χωρίς να υπάρχει νόμιμη βάση για κάτι τέτοιο σύμφωνα με το άρθρο 6 παράγραφος 1, το οποίο περιλαμβάνει τη λήψη της συναίνεσης του χρήστη. *Άρθρο 6 παράγραφος 1Η επεξεργασία είναι νόμιμη μόνο εάν και στον βαθμό που ισχύει τουλάχιστον ένα από τα ακόλουθα: (α) το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους συγκεκριμένους σκοπούς· ανατρέξτε στο άρθρο: 7, 8 & 9 και αιτιολογική σκέψη: 32, 42, 43 & 171 (β) η επεξεργασία είναι απαραίτητη για την εκτέλεση μιας σύμβασης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατόπιν αιτήματος του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης· ανατρέξτε στο άρθρο: 20 (γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με μια νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας· (δ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών*

*συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου· (ε) η επεξεργασία είναι απαραίτητη για την εκτέλεση μιας εργασίας που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση επίσημης εξουσίας που ανατίθεται στον υπεύθυνο επεξεργασίας· (στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο μέρος, εκτός εάν αυτά τα συμφέροντα υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων που απαιτούν προστασία των προσωπικών δεδομένων , ιδίως όταν το υποκείμενο των δεδομένων είναι παιδί. Ανατρέξτε στο άρθρο: 13 & 21 και αιτιολογική σκέψη: 113, 47 & 48*

Ειδικές κατηγορίες προσωπικών δεδομένων

Ειδικές κατηγορίες προσωπικών δεδομένων είναι τύποι προσωπικών δεδομένων που θεωρείται ότι ενέχουν σημαντικότερο κίνδυνο για τα δικαιώματα και τις ελευθερίες ενός ατόμου. Σύμφωνα με το άρθρο 9 παράγραφος 1, ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα περιλαμβάνουν:

Φυλετική ή εθνική καταγωγή

Πολιτικές απόψεις

Θρησκευτικές ή φιλοσοφικές πεποιθήσεις

Μέλη συνδικαλιστικών οργανώσεων

Υγεία, σεξουαλική ζωή ή σεξουαλικός προσανατολισμός

Γενετικά δεδομένα

Βιομετρικά δεδομένα

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα μπορούν να υποβληθούν σε επεξεργασία μόνο σε νόμιμη βάση, όπως αναφέρεται στο άρθρο 6 & 9. Η λήψη ρητής συναίνεσης από το άτομο, όπως το άρθρο 9 παράγραφος 2α, είναι η πιο κοινή μέθοδος για την επίτευξη νόμιμης βάσης. Όπου απαιτείται επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων, τα δεδομένα θα πρέπει να προστατεύονται με τα ισχυρότερα μέτρα ασφαλείας, όπως η εφαρμογή κρυπτογράφησης βάσης δεδομένων. Ο παραβιασμός ειδικών κατηγοριών προσωπικών δεδομένων είναι πιθανό να οδηγήσει στα σημαντικότερα μέτρα επιβολής από τις εποπτικές αρχές. Δεδομένων των πρόσθετων γενικών εξόδων ασφαλείας και του αυξημένου κινδύνου με τη χρήση ειδικών κατηγοριών προσωπικών δεδομένων, οι υποψήφιοι προγραμματιστές θα πρέπει πάντα να επαληθεύουν και να αμφισβητούν οποιαδήποτε προτεινόμενη χρήση που προτείνουν οι χορηγοί του έργου, διασφαλίζοντας ότι υπάρχει σαφής, νόμιμος σκοπός για χρήση αυτών των δεδομένων από η εφαρμογή.

Υπεύθυνος προστασίας δεδομένων

Οι περισσότεροι οργανισμοί πρέπει να ορίσουν έναν κατάλληλο επαγγελματία προστασίας δεδομένων ως υπεύθυνο προστασίας δεδομένων (DPO). Το άρθρο 39 ορίζει ότι ο ρόλος του DPO

είναι να ενημερώνει και να συμβουλεύει τον οργανισμό σχετικά με τις υποχρεώσεις του GDPR και να παρακολουθεί τη συμμόρφωση με τον GDPR, συμπεριλαμβανομένων των διαδικασιών ανάπτυξης εφαρμογών και υποστήριξης. Ο ΥΠΔ είναι επίσης το κύριο σημείο επαφής για τα υποκείμενα των δεδομένων και τις εποπτικές αρχές.

Ορισμοί ρόλου ευθύνης προσωπικών δεδομένων

Όπως η πρόδρομη Οδηγία της ΕΕ για την Προστασία Δεδομένων, ο GDPR ορίζει δύο τύπους ρόλων ευθύνης για τα προσωπικά δεδομένα του οργανισμού: έναν υπεύθυνο επεξεργασίας δεδομένων και έναν εκτελούντα την επεξεργασία. Ωστόσο, σε αντίθεση με την οδηγία, ο GDPR επιβάλλει περαιτέρω ευθύνες και υποχρεώσεις στους επεξεργαστές δεδομένων και περιλαμβάνει οργανισμούς επεξεργασίας που φιλοξενούν εφαρμογές που χρησιμοποιούνται από άλλους οργανισμούς. Με κάθε εφαρμογή που αναπτύσσεται και υποστηρίζεται, πρέπει να κατανοείτε ξεκάθαρα εάν ο οργανισμός σας βρίσκεται σε θέση υπευθύνου επεξεργασίας ή επεξεργασίας, καθώς η ευθύνη της διευκόλυνσης των περισσότερων από τα ατομικά δικαιώματα απορρήτου του GDPR ανήκει στους οργανισμούς ελεγκτών.

Ελεγκτής

Ο υπεύθυνος επεξεργασίας είναι ένας οργανισμός υπεύθυνος για τον καθορισμό των σκοπών και των μέσων επεξεργασίας προσωπικών δεδομένων. Όταν ένας οργανισμός αναπτύσσει εφαρμογές μόνο για εσωτερική χρήση, ο οργανισμός συνήθως έχει το ρόλο του ελεγκτή. *Άρθρο 4 παράγραφος 7 του ΓΚΠΔ "υπεύθυνος επεξεργασίας" σημαίνει το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που, μόνος ή από κοινού με άλλους, καθορίζει σκοπούς και μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα,*

Επεξεργαστής

Ο εκτελών την επεξεργασία είναι ένας οργανισμός που επεξεργάζεται προσωπικά δεδομένα σύμφωνα με τις οδηγίες ή για λογαριασμό ενός υπεύθυνου επεξεργασίας. Όταν η ανάπτυξη και η ανάπτυξη εφαρμογών προορίζεται για μεταπώληση και χρήση από άλλους οργανισμούς, συμπεριλαμβανομένης της παροχής φιλοξενίας εφαρμογών, ο οργανισμός παροχής εφαρμογών είναι συνήθως σε ρόλο επεξεργαστή. Όταν παρέχετε εφαρμογές για οργανισμούς επεξεργασίας, θα πρέπει να εξετάσετε το ενδεχόμενο ανάπτυξης και παροχής τέτοιων εφαρμογών με την απαραίτητη λειτουργικότητα για να βοηθήσετε τους οργανισμούς ελεγκτών να διευκολύνουν τα δικαιώματα απορρήτου του GDPR μέσω της εφαρμογής. *Άρθρο 4 παράγραφος 8 του ΓΚΠΔ "υπεύθυνος επεξεργασίας" σημαίνει φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας.*

Λήψη συναίνεσης

Ο GDPR δίνει έμφαση στους οργανισμούς που λαμβάνουν τη συγκατάθεση του υποκειμένου των δεδομένων πριν από την πρόσβαση και τον χειρισμό των προσωπικών τους δεδομένων. Για τις

εφαρμογές, η συναίνεση συνήθως σημαίνει τη λήψη της άδειας κάθε χρήστη πριν από την ολοκλήρωση μιας διαδικασίας εγγραφής λογαριασμού, καθώς αυτή είναι συνήθως η αρχική συλλογή προσωπικών δεδομένων που πραγματοποιείται από την εφαρμογή. Η συγκατάθεση απαιτεί από το υποκείμενο των δεδομένων να ενημερώνεται σαφώς σχετικά με τον τρόπο επεξεργασίας και αποθήκευσης των προσωπικών του δεδομένων από την εφαρμογή, συμπεριλαμβανομένης τυχόν πρόσβασης τρίτων και κοινής χρήσης δεδομένων, και στη συνέχεια να ζητά και να καταγράφει την άδεια του χρήστη. Το άρθρο 4 παράγραφος 11 του ΓΚΠΔ απαιτεί τη λήψη συναίνεσης μέσω θετικής ενέργειας από το υποκείμενο των δεδομένων. Αυτό σημαίνει ότι εάν η εφαρμογή παρέχει μια δήλωση συναίνεσης με πλαίσιο επιλογής άδειας, το πλαίσιο επιλογής πρέπει να οριστεί ως κενό από προεπιλογή, έτσι ώστε να απαιτείται από τον χρήστη να κάνει μια ενέργεια για να ελέγξει το πλαίσιο επιλογής συμφωνίας συναίνεσης. Αυτό θεωρείται απόκτηση συναίνεσης μέσω μιας σαφής θετικής ενέργειας χρήστη. *Άρθρο 4 παράγραφος 11«συναίνεση» του υποκειμένου των δεδομένων σημαίνει κάθε ελεύθερα δεδομένη, συγκεκριμένη, ενημερωμένη και σαφή ένδειξη των επιθυμιών του υποκειμένου των δεδομένων με την οποία αυτό ή αυτή , με δήλωση ή με σαφή καταφατική ενέργεια, υποδηλώνει συμφωνία για την επεξεργασία προσωπικών δεδομένων που τον αφορούν·* Η εφαρμογή πρέπει να παρακολουθεί πότε λήφθηκε η συναίνεση του χρήστη κατά ημερομηνία και, ιδανικά, ώρα. Η συγκατάθεση καταγραφής επιτρέπει στην εφαρμογή να αποδείξει αποδεικτικά στοιχεία της συναίνεσης του χρήστη, η οποία απαιτείται σύμφωνα με το άρθρο 7 παράγραφος 1. *Άρθρο 7 παράγραφος 1Όταν η επεξεργασία βασίζεται στη συγκατάθεση, ο υπεύθυνος επεξεργασίας πρέπει να μπορεί να αποδείξει ότι το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των προσωπικών του δεδομένων .* Η εφαρμογή πρέπει να έχει μια ειδική δήλωση συναίνεσης απορρήτου που πρέπει να είναι χωριστή και να μην αποτελεί μέρος οποιασδήποτε άλλης άδειας χρήσης ή συμφωνίας παροχής υπηρεσιών. Η δήλωση απορρήτου πρέπει να συντάσσεται με σαφή και συνοπτικό τρόπο και να εξηγεί λεπτομερώς τον τρόπο επεξεργασίας των προσωπικών δεδομένων του χρήστη από την εφαρμογή. Αυτό απαιτείται από το άρθρο 7 παράγραφος 2. *Άρθρο 7 παράγραφος 2Εάν η συγκατάθεση του υποκειμένου των δεδομένων δίδεται στο πλαίσιο γραπτής δήλωσης που αφορά επίσης άλλα θέματα, το αίτημα συναίνεσης υποβάλλεται σε τρόπο που διακρίνεται σαφώς από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα. Οποιοδήποτε μέρος μιας τέτοιας δήλωσης που συνιστά παράβαση του παρόντος κανονισμού δεν είναι δεσμευτικό.* Το υποκείμενο των δεδομένων έχει το δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή, όπως ορίζεται στο άρθρο 7 παράγραφος 3. Για να συμμορφωθούν οι εφαρμογές, η εφαρμογή πρέπει να παρέχει στους χρήστες μια απλή λειτουργία ανάκλησης συναίνεσης χρήστη. Εάν ο χρήστης θεσπίσει ανάκληση συναίνεσης, η εφαρμογή θα πρέπει να διεκπεραιώσει την πλήρη διαγραφή όλων των περιπτώσεων του λογαριασμού και των προσωπικών δεδομένων του χρήστη, συμπεριλαμβανομένων των περιπτώσεων όπου τα δεδομένα αυτά διατηρούνται σε εφεδρικά συστήματα. *Άρθρο 7 παράγραφος 3Το υποκείμενο των δεδομένων έχει το δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν επηρεάζει τη νομιμότητα της επεξεργασίας που βασίζεται στη συγκατάθεση πριν από την ανάκλησή της. Πριν δώσει τη συγκατάθεσή του, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση θα είναι τόσο εύκολη όσο και η συναίνεση.* Το άρθρο 7 παράγραφος 4, που υποστηρίζεται από την αιτιολογική

σκέψη 43, απαιτεί να παρέχεται ελεύθερα η συναίνεση του χρήστη, πράγμα που σημαίνει ότι τα υποκείμενα των δεδομένων δεν πρέπει να αναγκάζονται να εγγραφούν και να δώσουν τη συγκατάθεσή τους για χρήση της εφαρμογής ως προϋπόθεση για τη λήψη μιας υπηρεσίας. *ΓΚΠΔ Άρθρο 7 παράγραφος 4Όταν αξιολογείται εάν η συγκατάθεση παρέχεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη εάν, μεταξύ άλλων, η εκτέλεση μιας σύμβασης, συμπεριλαμβανομένων των Η παροχή μιας υπηρεσίας εξαρτάται από τη συγκατάθεση για την επεξεργασία προσωπικών δεδομένων που δεν είναι απαραίτητα για την εκτέλεση αυτής της σύμβασης.*

Συναίνεση παιδιού

Εάν η αίτηση προορίζεται ή έχει τη δυνατότητα να χρησιμοποιηθεί από υποκείμενα των δεδομένων ηλικίας κάτω των 16 ετών (παιδιά), η συγκατάθεση πρέπει να ληφθεί από άτομο που έχει τη γονική μέριμνα για το παιδί. Αυτό αποτελεί απαίτηση του άρθρου 8 (1 & 2). Επομένως, πρέπει να καταβληθούν εύλογες προσπάθειες για να επαληθευτεί ότι το άτομο που παρέχει τη γονική συναίνεση είναι στην πραγματικότητα το γονικό ποσό για τον λογαριασμό του παιδιού. Μια λύση εφαρμογής σε αυτήν την απαίτηση, μαζί με την επαλήθευση ηλικίας, είναι να ζητήσετε συναίνεση μέσω ενός πρόσθετου γονικού λογαριασμού που είναι συνδεδεμένος με τον λογαριασμό του παιδιού. Η εφαρμογή μπορεί να επαληθεύσει ότι η διεύθυνση email του γονικού λογαριασμού είναι ενεργή και διαφορετική από τη διεύθυνση email που σχετίζεται με τον λογαριασμό του παιδιού. Μια τέτοια διαδικασία επαλήθευσης θα μπορούσε να θεωρηθεί ότι καταβάλλει εύλογες προσπάθειες σε αντίθεση με την παροχή ενός επιπλέον πλαισίου επιλογής γονικής συναίνεσης κατά τη διαδικασία δημιουργίας λογαριασμού του παιδιού. *Άρθρο 8 παράγραφος 1 Όταν εφαρμόζεται το στοιχείο α) του άρθρου 6 παράγραφος 1, σε σχέση με την προσφορά υπηρεσιών της κοινωνίας της πληροφορίας απευθείας σε ένα παιδί, Η επεξεργασία των προσωπικών δεδομένων ενός παιδιού είναι νόμιμη όταν το παιδί είναι τουλάχιστον 16 ετών. Όταν το παιδί είναι κάτω των 16 ετών, αυτή η επεξεργασία θα είναι νόμιμη μόνο εάν και στον βαθμό που η συγκατάθεση έχει δοθεί ή εξουσιοδοτηθεί από τον κάτοχο της γονικής μέριμνας του παιδιού. Τα κράτη μέλη μπορούν να προβλέπουν από το νόμο χαμηλότερη ηλικία για τους σκοπούς αυτούς, υπό τον όρο ότι αυτή η κατώτερη ηλικία δεν είναι κάτω των 13 ετών. Άρθρο 8 παράγραφος 2Ο υπεύθυνος επεξεργασίας καταβάλλει εύλογες προσπάθειες για να επαληθεύσει σε τέτοιες περιπτώσεις ότι η συγκατάθεση έχει δοθεί ή εξουσιοδοτηθεί από τον κάτοχο της γονικής μέριμνας για το παιδί, λαμβάνοντας λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία* .

Δικαιώματα απορρήτου GDPR

Οι εφαρμογές που επεξεργάζονται τα προσωπικά δεδομένα πολιτών της ΕΕ εμπίπτουν στο πεδίο εφαρμογής ορισμένων ειδικών δικαιωμάτων απορρήτου GDPR. Οι προγραμματιστές πρέπει να διασφαλίζουν ότι οι εφαρμογές αναπτύσσονται και διατηρούνται με τα κατάλληλα μέτρα και λειτουργικότητα για τη διευκόλυνση των ακόλουθων δικαιωμάτων απορρήτου GDPR στους χρήστες της εφαρμογής:

Δικαίωμα ενημέρωσης

Το δικαίωμα πρόσβασης

Το δικαίωμα διόρθωσης

Δικαίωμα διαγραφής

Το δικαίωμα περιορισμού της επεξεργασίας

Το δικαίωμα στη φορητότητα δεδομένων

Δικαίωμα αντίρρησης

Το δικαίωμα να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της δημιουργίας προφίλ

Το δικαίωμα στην ενημέρωση

Οι εφαρμογές που επεξεργάζονται προσωπικά δεδομένα πρέπει να είναι απολύτως διαφανείς με τους χρήστες ως προς τον τρόπο επεξεργασίας των προσωπικών τους δεδομένων. Αυτό θα πρέπει να διευκολύνεται σε κάθε χρήστη της εφαρμογής μέσω δήλωσης απορρήτου ή ειδοποίησης απορρήτου. Ένα συνηθισμένο λάθος κατά τη σύνταξη μιας δήλωσης απορρήτου είναι η χρήση γλώσσας και όρων ανάπτυξης εφαρμογών. Η δήλωση απορρήτου πρέπει να συντάσσεται με χρήση κοινών γλωσσικών όρων, ώστε να είναι εύκολα κατανοητή από άτομα που δεν είναι τεχνικά και όχι ειδικοί σε θέματα απορρήτου δεδομένων. Για να διευκολυνθεί η κατανόηση, εξετάστε το ενδεχόμενο να χρησιμοποιήσετε γραφικές εικόνες και διαγράμματα ροής στη δήλωση απορρήτου, για να παρέχετε μια οπτική αναπαράσταση του τρόπου με τον οποίο η εφαρμογή επεξεργάζεται τα προσωπικά τους στοιχεία. Εάν η εφαρμογή προορίζεται να χρησιμοποιηθεί από παιδιά, τότε η δήλωση απορρήτου πρέπει να συνταχθεί με διατύπωση που να κατανοούν τα παιδιά. Η δήλωση απορρήτου θα πρέπει να περιγράφει τις προσωπικές πληροφορίες που συλλέγονται και επεξεργάζονται η εφαρμογή. Επιπλέον, η δήλωση θα πρέπει να αιτιολογεί κάθε χρήση προσωπικών δεδομένων από την εφαρμογή παρέχοντας συγκεκριμένους λόγους για όλη τη συλλογή δεδομένων και την επεξεργασία δεδομένων από την εφαρμογή. Η δήλωση απορρήτου θα πρέπει επίσης να περιγράφει με σαφήνεια οποιαδήποτε άλλη εμπλοκή τρίτου μέρους με την επεξεργασία προσωπικών δεδομένων από την εφαρμογή, συμπεριλαμβανομένης οποιασδήποτε φιλοξενίας τρίτων (για παράδειγμα, αποθήκευση δεδομένων, συμπεριλαμβανομένων των αντιγράφων ασφαλείας), οποιαδήποτε προσβασιμότητα (για παράδειγμα, απομακρυσμένη υποστήριξη τρίτων) και οποιαδήποτε μεταφορά ή κοινή χρήση δεδομένων με άλλους τρίτους οργανισμούς. *Άρθρο 12 παράγραφος 1Ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για την παροχή οποιασδήποτε πληροφορίας που αναφέρεται στα άρθρα 13 και 14 και κάθε επικοινωνία σύμφωνα με τα άρθρα 15 έως 22 και 34 σχετικά με στην επεξεργασία προς το υποκείμενο των δεδομένων σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, με χρήση σαφούς και απλής γλώσσας, ιδίως για κάθε πληροφορία που απευθύνεται ειδικά σε ένα παιδί. Δείτε επίσης την αιτιολογική σκέψη 58 και την αιτιολογική σκέψη 59.*

Το δικαίωμα πρόσβασης

Οι χρήστες της αίτησης πολιτών της ΕΕ έχουν το δικαίωμα πρόσβασης σε όλα τα προσωπικά τους δεδομένα όπως τηρούνται και υποβάλλονται σε επεξεργασία από την εφαρμογή. Ο οργανισμός που διαχειρίζεται την εφαρμογή είναι ο υπεύθυνος επεξεργασίας και το μέρος που είναι υπεύθυνο για τη διευκόλυνση αυτού του δικαιώματος στους χρήστες της εφαρμογής. Για να υποβοηθηθεί η συμμόρφωση με τον GDPR ενός οργανισμού, θα πρέπει να αναπτυχθούν εφαρμογές που θα διευκολύνουν το δικαίωμα πρόσβασης ενός χρήστη, συμπεριλαμβάνοντας μια λειτουργία χρήστη που επιστρέφει όλα τα προσωπικά δεδομένα του χρήστη, όπως τα κατέχει η εφαρμογή.

Αιτήματα πρόσβασης υποκειμένου δεδομένων

Το δικαίωμα πρόσβασης σημαίνει επίσης ότι οι χρήστες της εφαρμογής έχουν το δικαίωμα να υποβάλουν γραπτό αίτημα για να τους παρασχεθούν είτε όλα, είτε συγκεκριμένα μέρη, των προσωπικών τους πληροφοριών, όπως διατηρούνται από την εφαρμογή και τον οργανισμό επεξεργασίας. Αυτή η διαδικασία είναι γνωστή ως αίτημα πρόσβασης υποκειμένου δεδομένων. Ο GDPR απαιτεί τα αιτήματα πρόσβασης στα υποκείμενα των δεδομένων να παρέχονται δωρεάν και εντός ενός μήνα από την υποβολή του αιτήματος. Όταν ένας οργανισμός είναι υπεύθυνος επεξεργασίας, θα πρέπει να παρέχει στοιχεία επικοινωνίας στους χρήστες της εφαρμογής για να υποβάλλουν αιτήματα πρόσβασης στο υποκείμενο των δεδομένων και να έχουν επίσημη διαδικασία για την έγκαιρη διαχείριση τέτοιων αιτημάτων. *Άρθρο 15 παράγραφος 1Το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει επιβεβαίωση από τον υπεύθυνο επεξεργασίας σχετικά με το εάν τα προσωπικά δεδομένα που το αφορούν υποβάλλονται σε επεξεργασία ή όχι, και, όπου συμβαίνει αυτό, πρόσβαση στα προσωπικά δεδομένα.*

Το δικαίωμα στη διόρθωση

Οι χρήστες εφαρμογών έχουν το δικαίωμα διόρθωσης των προσωπικών τους δεδομένων όταν διατηρούνται εσφαλμένα ή είναι ελλιπή, σύμφωνα με το άρθρο 16. Για να διευκολύνεται η συμμόρφωση του υπεύθυνου επεξεργασίας, οι εφαρμογές θα πρέπει να παρέχουν στους χρήστες τη δυνατότητα να επεξεργάζονται τα δικά τους αρχεία προσωπικών δεδομένων. Κάθε πεδίο προσωπικών δεδομένων θα πρέπει να είναι επεξεργάσιμο σε περίπτωση τυχαίας εισαγωγής σφαλμάτων ή εάν τα προσωπικά δεδομένα καταστούν παρωχημένα, για παράδειγμα, όταν ένας χρήστης έχει αλλάξει τη διεύθυνση κατοικίας του ή μετά από αλλαγή στην οικογενειακή του κατάσταση (για παράδειγμα, νέο επώνυμο). Οι εφαρμογές θα πρέπει να υπενθυμίζουν τακτικά στους χρήστες να επαληθεύουν ότι τα προσωπικά τους δεδομένα είναι ακριβή και πλήρη. Η εφαρμογή θα πρέπει να καταγράφει όλες τις αλλαγές στα προσωπικά δεδομένα και να παρέχει επίσημη ειδοποίηση για όλες τις αλλαγές στο υποκείμενο των δεδομένων. Αυτό μπορεί να επιτευχθεί στις περισσότερες περιπτώσεις με μια ειδοποίηση μέσω email. Η κοινοποίηση αλλαγών σε δεδομένα προσωπικού χαρακτήρα απαιτείται για το άρθρο 19 και αποτελεί επίσης καλή πρακτική ασφάλειας, καθώς οι χρήστες ενημερώνονται γρήγορα σε περίπτωση που άλλο μέρος αλλάξει παράνομα τα προσωπικά του δεδομένα εν αγνοία του. Συνήθως, αφού θέσουν σε κίνδυνο έναν

λογαριασμό χρήστη εφαρμογής, οι χάκερ αλλάζουν τον κωδικό πρόσβασης του λογαριασμού, τη διεύθυνση ηλεκτρονικού ταχυδρομείου και την ταχυδρομική διεύθυνση για να βοηθήσουν σε δόλιες και κακόβουλες δραστηριότητες. *Άρθρο 16Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών προσωπικών δεδομένων που το αφορούν. Λαμβάνοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να συμπληρώσει ελλιπή προσωπικά δεδομένα, μεταξύ άλλων μέσω της παροχής συμπληρωματικής δήλωσης. Άρθρο 19Ο υπεύθυνος επεξεργασίας κοινοποιεί οποιαδήποτε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που πραγματοποιείται*

Το δικαίωμα διαγραφής

Το δικαίωμα διαγραφής, κοινώς γνωστό ως “δικαίωμα στη λήθη”, δίνει στους χρήστες εφαρμογών το δικαίωμα να δώσουν εντολή σε έναν υπεύθυνο επεξεργασίας να διαγράψει όλες τις προσωπικές τους πληροφορίες, συμπεριλαμβανομένου του τόπου αποθήκευσης των δεδομένων τους σε αντίγραφα ασφαλείας της βάσης δεδομένων και με επεξεργαστές. Υπάρχουν νομικές περιστάσεις όπου το δικαίωμα του άρθρου 17 δεν ισχύει, επομένως ένας εγκληματίας απλά δεν μπορεί να περιμένει ότι θα διαγραφεί το ποινικό του μητρώο κατόπιν αιτήματος. Ωστόσο, γενικά, για τις περισσότερες εμπορικές εφαρμογές, η εφαρμογή θα πρέπει να περιλαμβάνει μια λειτουργία χρήστη όπου ένας χρήστης μπορεί να δώσει οδηγίες για τη διαγραφή του λογαριασμού του και όλων των προσωπικών δεδομένων που διατηρούνται. Η διαδικασία διαγραφής λογαριασμού θα πρέπει επίσης να περιλαμβάνει τη διαγραφή όλων των λογαριασμών και προσωπικών δεδομένων που διατηρούνται σε εφεδρικά συστήματα. Η εφαρμογή πρέπει επίσης να παρέχει στον χρήστη επιβεβαίωση αφού διαγραφούν όλα τα προσωπικά του δεδομένα, κάτι που απαιτείται σύμφωνα με το άρθρο 19. *Άρθρο 17(1) Το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει από τον υπεύθυνο επεξεργασίας τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας έχουν την υποχρέωση να διαγράφουν προσωπικά δεδομένα χωρίς αδικαιολόγητη καθυστέρηση. Άρθρο 19Ο υπεύθυνος επεξεργασίας κοινοποιεί οποιαδήποτε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που πραγματοποιείται*

Το δικαίωμα περιορισμού της επεξεργασίας

Οι πολίτες της ΕΕ έχουν το δικαίωμα να μπλοκάρουν την επεξεργασία των προσωπικών τους δεδομένων σύμφωνα με το άρθρο 18. Όταν αυτό το δικαίωμα επικαλείται ένα υποκείμενο των δεδομένων με υπεύθυνο επεξεργασίας, σημαίνει ότι η εφαρμογή εξακολουθεί να επιτρέπεται να διατηρεί τα προσωπικά στοιχεία ενός υποκειμένου των δεδομένων, αλλά δεν επιτρέπεται για τα προσωπικά στοιχεία που πρέπει να επεξεργαστεί η εφαρμογή. Μια εφαρμογή μπορεί να διευκολύνει αυτό το δικαίωμα επιτρέποντας τον ορισμό του λογαριασμού του χρήστη ως ανενεργού ή αδρανούς. Ο χρήστης της εφαρμογής πρέπει να ειδοποιείται επίσημα (δηλαδή μέσω email) όταν διευκολύνει αυτό το δικαίωμα καθιστώντας τον λογαριασμό του ανενεργό, αυτό απαιτείται για το άρθρο 19. *Άρθρο 18 παράγραφος 1Το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει από τον*

*υπεύθυνο επεξεργασίας περιορισμό της επεξεργασίας Άρθρο 19Ο υπεύθυνος επεξεργασίας κοινοποιεί κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό__επεξεργασίας που πραγματοποιείται.*

Το δικαίωμα στη φορητότητα δεδομένων

Το δικαίωμα στη φορητότητα δεδομένων δίνει σε έναν χρήστη της εφαρμογής το δικαίωμα να ζητήσει να μετακινήσει ή να αντιγράψει τα προσωπικά του δεδομένα μεταξύ διαφορετικών οργανισμών επεξεργασίας. Η μεταφορά δεδομένων πρέπει να χρησιμοποιεί αποδεκτή μορφή δεδομένων και να εκτελείται με ασφάλεια. Τα αιτήματα φορητότητας δεδομένων θα πρέπει να ολοκληρωθούν εντός ενός μηνός και οι οργανισμοί δεν επιτρέπεται να χρεώνουν χρέωση. Μια συνάρτηση εξαγωγής δεδομένων εφαρμογής μπορεί να επιταχύνει τα αιτήματα φορητότητας δεδομένων, σύμφωνα με το άρθρο 20, εξάγοντας τα αρχεία προσωπικών δεδομένων ενός υποκειμένου των δεδομένων από την εφαρμογή σε αρχείο μορφοποιημένο CSV. Η μορφή CSV θεωρείται μια ανοιχτή και παγκοσμίως αποδεκτή μορφή δεδομένων «αναγνώσιμη από μηχανή», η οποία επιτρέπει σε άλλους οργανισμούς ελεγκτών να αυτοματοποιούν την εισαγωγή των προσωπικών δεδομένων του υποκειμένου των δεδομένων στις εφαρμογές και τα συστήματά τους χωρίς εμπόδια. Η μεταφορά προσωπικών δεδομένων μεταξύ των οργανισμών επεξεργασίας πρέπει να είναι επαρκώς ασφαλής και πρέπει να είναι κρυπτογραφημένη όταν τα προσωπικά δεδομένα μεταφέρονται σε μη αξιόπιστα ή δημόσια μέσα και περιβάλλοντα. *Άρθρο 20 παράγραφος 1Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα προσωπικά δεδομένα που το αφορούν, τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε μια δομημένη, κοινώς χρησιμοποιούμενη και αναγνώσιμη από μηχανή μορφή και έχουν το δικαίωμα να διαβιβάζουν αυτά τα δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς εμπόδια από τον υπεύθυνο επεξεργασίας στον οποίο έχουν παρασχεθεί τα προσωπικά δεδομένα. Βλέπε αιτιολογική σκέψη 68*

Το δικαίωμα αντίρρησης

Οι χρήστες εφαρμογών της ΕΕ έχουν το δικαίωμα να αντιταχθούν στη χρήση των προσωπικών τους στοιχείων για δημιουργία προφίλ, άμεσο μάρκετινγκ και για επιστημονική ή ιστορική έρευνα, δικαίωμα που παρέχεται βάσει του άρθρου 21.

Αντίρρηση για δημιουργία προφίλ

Ο GDPR ορίζει το προφίλ σύμφωνα με το άρθρο 4 παράγραφος 4. Με απλά λόγια, σημαίνει τη χρήση προσωπικών στοιχείων και στατιστικών δεδομένων ενός ατόμου για τη δημιουργία ενός προφίλ σχετικά με τον τύπο του ατόμου, τον τρόπο συμπεριφοράς του, την υγεία του, την οικονομική του θέση ή το πού βρίσκονται. Όταν οι εφαρμογές σκοπεύουν να πραγματοποιήσουν δημιουργία προφίλ χρήστη, η δραστηριότητα θα πρέπει να καθίσταται σαφής στη δήλωση απορρήτου, όπου λαμβάνεται η συναίνεση του χρήστη. Θα πρέπει να δοθεί στον χρήστη η επιλογή να αντιταχθεί στη δημιουργία προφίλ και να απενεργοποιήσει τις διαδικασίες δημιουργίας προφίλ της εφαρμογής, ιδανικά εντός των στοιχείων ελέγχου λογαριασμού του χρήστη. *Άρθρο 4 παράγραφος 4Προφίλ σημαίνει κάθε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που*

*συνίσταται στη χρήση προσωπικών δεδομένων για την αξιολόγηση ορισμένων προσωπικών πτυχών που σχετίζονται με ένα φυσικό πρόσωπο, ειδικότερα για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση αυτού του φυσικού προσώπου στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, την τοποθεσία ή τις μετακινήσεις του.*

Αντίρρηση στο άμεσο μάρκετινγκ

Οι εφαρμογές που μπορούν να στείλουν μηνύματα μάρκετινγκ στους χρήστες, μεταξύ άλλων μέσω email, μηνύματος κειμένου, ανάρτησης μέσων κοινωνικής δικτύωσης και ταχυδρομικής αλληλογραφίας, πρέπει αρχικά να λάβουν τη συναίνεση του χρήστη για να το πράξουν. Η συναίνεση μάρκετινγκ θα πρέπει να παρέχεται μέσω ειδικής δήλωσης συμμετοχής, με σαφή δήλωση σχετικά με τον τύπο των μηνυμάτων μάρκετινγκ που αναμένεται να σταλούν από την εφαρμογή, τα κανάλια επικοινωνίας που χρησιμοποιούνται και ένα πλαίσιο επιλογής συγκατάθεσης. Το πλαίσιο ελέγχου συναίνεσης πρέπει να είναι προεπιλεγμένο ως μη επιλεγμένο όταν παρουσιάστηκε αρχικά στον χρήστη. Οι εφαρμογές θα πρέπει επίσης να παρέχουν στους χρήστες τη δυνατότητα να εξαιρεθούν από μηνύματα άμεσου μάρκετινγκ ανά πάσα στιγμή. *Άρθρο 21 παράγραφος 2Όταν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς άμεσου μάρκετινγκ, το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν αυτόν ή αυτήν για τέτοιο μάρκετινγκ, το οποίο περιλαμβάνει τη δημιουργία προφίλ στο βαθμό που σχετίζεται με τέτοιο άμεσο μάρκετινγκ.*

Αντίρρηση στην επιστημονική ή ιστορική έρευνα

Εάν τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται η εφαρμογή προορίζονται να χρησιμοποιηθούν για ερευνητικούς σκοπούς, οι χρήστες θα πρέπει να έχουν τη δυνατότητα να αντιταχθούν σε τέτοια χρήση σύμφωνα με το άρθρο 21 παράγραφος 6, εκτός εάν η έρευνα είναι προς το δημόσιο συμφέρον. *Άρθρο 21 παράγραφος 6Όταν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, το υποκείμενο των δεδομένων, για λόγους που σχετίζεται με την ιδιαίτερη κατάστασή του, έχει το δικαίωμα να αντιταχθεί στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που τον αφορούν, εκτός εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση μιας εργασίας που εκτελείται για λόγους δημοσίου συμφέροντος.* Ανατρέξτε στα άρθρα 12 και 89 και στις αιτιολογικές σκέψεις 156, 157, 158, 159, 160, 161, 162 και 163.

Το δικαίωμα να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της δημιουργίας προφίλ

Το άρθρο 22 απαιτεί από τους χρήστες να ενημερώνονται με σαφήνεια και να τους δίνεται η δυνατότητα να αντιταχθούν, εάν η εφαρμογή αναλύει ή διαμορφώσει τα προσωπικά τους στοιχεία, με σκοπό να αποκτήσουν μια εικόνα για τις συμπεριφορές και τα χαρακτηριστικά τους. Αυτό περιλαμβάνει όπου μια εφαρμογή λαμβάνει αυτοματοποιημένες αποφάσεις με βάση την ανάλυση προσωπικών δεδομένων, συμπεριλαμβανομένων τυχόν επιπτώσεων που μπορεί να έχει για τον

χρήστη και τα προσωπικά του δεδομένα. Μια τέτοια δραστηριότητα πρέπει να εκτελείται μόνο εάν υπάρχει νόμιμη απαίτηση. *Άρθρο 22 παράγραφος 1Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα σχετικά με αυτόν ή αυτήν ή με παρόμοιο τρόπο τον επηρεάζει σημαντικά*

Συμπέρασμα

Για να αναπτύξετε εφαρμογές που να συμμορφώνονται με τον GDPR, χρειάζεστε μια καλή κατανόηση των βασικών όρων και ορισμών περί απορρήτου δεδομένων. Αυτό σας βοηθά να συνομιλείτε καλύτερα με ειδικούς σε θέματα απορρήτου δεδομένων για να εξηγήσετε ζητήματα και να κατανοήσετε συμβουλές κατά την ανάπτυξη λύσεων μετριασμού του κινδύνου απορρήτου, ως μέρος της ανάπτυξης και υποστήριξης μιας εφαρμογής. Πρέπει επίσης να είστε εξοικειωμένοι με όλα τα ατομικά δικαιώματα απορρήτου που παρέχονται στους χρήστες εφαρμογών από τον GDPR. Αυτό βοηθά να διασφαλιστεί ότι όλες οι διαδικασίες εφαρμογών και οι λειτουργίες χρήστη έχουν σχεδιαστεί και κωδικοποιηθεί για να διευκολύνουν τα ισχύοντα δικαιώματα απορρήτου GDPR για τους χρήστες εφαρμογών.

## 2.5.4 IoT και edge computing

Το Edge computing αφορά την τοποθέτηση φόρτου εργασίας του υπολογιστή (τόσο υλικού όσο και λογισμικού) όσο το δυνατόν πιο κοντά στην άκρη—στο σημείο όπου δημιουργούνται τα δεδομένα και όπου πραγματοποιούνται ενέργειες. Τα περιβάλλοντα υπολογιστών αιχμής προσφέρουν στους πελάτες ταχύτερους χρόνους απόκρισης, μεγαλύτερο απόρρητο δεδομένων και μειωμένο κόστος μεταφοράς δεδομένων.

Καθώς οι μικροί, φθηνοί και δικτυακοί υπολογιστές γίνονται πιο ισχυροί, οι υπολογιστές αιχμής θα γίνονται πιο διαδεδομένοι σε όλους τους τομείς της οικονομίας.

Για τους παρόχους τηλεπικοινωνιών, τα περιβάλλοντα υπολογιστών αιχμής επιτρέπουν στους πελάτες να εκτελούν φόρτους εργασίας στις εγκαταστάσεις υπολογιστών αιχμής πολλαπλής πρόσβασης (MEC) που είναι ενσωματωμένες σε τοπικές κοινότητες.

Για τους αγρότες, ο υπολογισμός αιχμής σημαίνει παρακολούθηση των συνθηκών καλλιέργειας σε πολύ πιο λεπτή κλίμακα για ακριβέστερη δράση και αύξηση των αποδόσεων.

Για τους λιανοπωλητές, το edge computing σημαίνει ότι μπορούν να διαχειρίζονται τους κύκλους ζωής του μεγάλου εύρους φόρτου εργασίας τους σε συσκευές πολλών τύπων και αρχιτεκτονικών σε πολλές τοποθεσίες καταστημάτων.

Για τους κατασκευαστές, τα περιβάλλοντα υπολογιστών αιχμής τους επιτρέπουν να χρησιμοποιούν ένα σύγχρονο στυλ ανάπτυξης και ανάπτυξης που είναι εγγενές στο cloud, ενώ παραμένουν “αέρας” (εντελώς αποσυνδεδεμένοι) από το διαδίκτυο.

Επεξεργασία δεδομένων στην άκρη

Μια σημαντική διαφορά με τον υπολογισμό ακμών είναι αυτό που συμβαίνει με τα δεδομένα στην άκρη του δικτύου. Από πού προέρχονται όλα αυτά τα δεδομένα; Είναι σύνηθες να σκεφτόμαστε τα μεγάλα δεδομένα ως κεντρικά στο cloud, όπου πιθανώς η περισσότερη επεξεργασία δεδομένων λαμβάνει χώρα σήμερα. Αλλά το σύννεφο δεν είναι από όπου προέρχονται τα δεδομένα. Τα δεδομένα προέρχονται από ανθρώπους, το περιβάλλον μας και τα μηχανήματα μας (αυτοκίνητα, εργοστασιακές μηχανές, κινητές συσκευές και άλλα). Όταν εμείς ή οι μηχανές μας εκτελούμε ενέργειες στον πραγματικό κόσμο, παράγουμε δεδομένα. Ο ίδιος ο κόσμος μας είναι επίσης μια τεράστια πηγή δεδομένων.

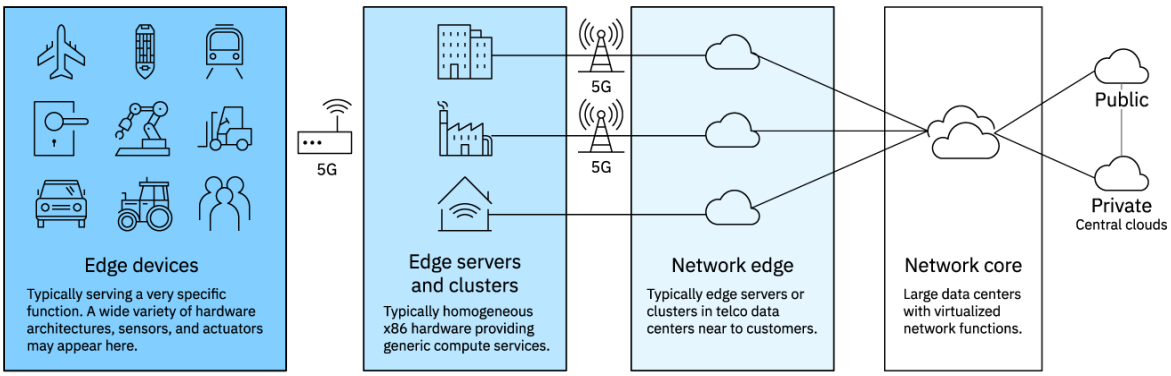
Στην εποχή του Διαδικτύου των Πραγμάτων (IoT), οι υπολογιστές στην άκρη ήταν συνήθως απλώς άσκοπες αντλίες δεδομένων. Η δουλειά τους ήταν να δοκιμάζουν περιοδικά το περιβάλλον τους σε μια συγκεκριμένη ανάλυση. Στη συνέχεια, θα έστελναν αντίστοιχες εγγραφές δεδομένων ή θα περίμεναν παθητικά εντολές από έναν κεντρικό διακομιστή σε ένα κέντρο δεδομένων κάπου. Αυτοί οι κεντρικοί διακομιστές θα μπορούσαν να βρίσκονται σε δημόσιο σύννεφο, ιδιωτικό σύννεφο ή οποιοδήποτε κέντρο δεδομένων. Πραγματικά δεν είχε σημασία. Η σημαντική διαφορά είναι ότι αυτές οι συσκευές IoT δεν ήταν σε θέση να λάβουν τοπικές αποφάσεις. Ήταν ουσιαστικά χαζά περιφερειακά για αυτούς τους κεντρικούς διακομιστές. Οι αποφάσεις παίρνονταν κεντρικά. Αυτή η αρχιτεκτονική δεν έχει καλή κλίμακα.

Οι μικροί και φθηνοί υπολογιστές εξελίσσονται ραγδαία. Είναι πολύ πιο ισχυρά τώρα και ικανά για σημαντική τοπική επεξεργασία, συμπεριλαμβανομένων εξελιγμένων αναλύσεων, ακόμη και εφαρμογών τεχνητής νοημοσύνης (AI). Ο αριθμός τους έχει αυξηθεί εκθετικά σε σημείο όπου η απλή άντληση όλων των δεδομένων τους στο cloud είναι απαγορευτικά δαπανηρή ή ακόμα και αδύνατη. Αυτοί οι παράγοντες βοήθησαν στο να επιτραπεί η άνοδος των υπολογιστών αιχμής.

Ενώ οι συσκευές IoT στέλνουν αφιλτράριστα δεδομένα στο cloud, οι συσκευές edge επιτρέπουν την τοπική επεξεργασία των δεδομένων. Με τους υπολογιστές edge, μπορείτε να κάνετε δειγματοληψία των δεδομένων σας σε υψηλότερες αναλύσεις και σε μεγαλύτερες συχνότητες δειγματοληψίας. Μετά από τοπική ανάλυση, μπορούν ακόμα να στείλουν τα δεδομένα τους στο cloud, αλλά μπορεί να είναι πολύ μικρότερος όγκος δεδομένων πολύ μεγαλύτερης αξίας. Οι κεντρικοί σας διακομιστές μπορούν στη συνέχεια να επικεντρωθούν στη συγκέντρωση δεδομένων σε μεγάλους αριθμούς υπολογιστών αιχμής, καλύπτοντας μεγαλύτερες περιοχές και για μεγαλύτερες περιόδους, πράγμα που σημαίνει ότι μπορείτε να παρατηρήσετε πιο εύκολα σημαντικές τάσεις.

Η εκτέλεση αναλύσεων τοπικά στην άκρη παράγει επίσης εξαιρετικά χαμηλούς χρόνους απόκρισης ερεθίσματος. Όταν τόσο ένας αισθητήρας όσο και ένας ενεργοποιητής είναι συνδεδεμένοι στην ίδια συσκευή άκρων ή σε διακομιστές ακμών που βρίσκονται κοντά ο ένας στον άλλο στο δίκτυο, οι χρόνοι απόκρισης μπορεί να είναι μόλις λίγα χιλιοστά του δευτερολέπτου ή ακόμη και λιγότεροι από ένα χιλιοστό του δευτερολέπτου σε ορισμένες περιπτώσεις. Αυτός είναι πολύ πιο γρήγορος από έναν τυπικό χρόνο μετ' επιστροφής για επικοινωνία με οποιονδήποτε απομακρυσμένο διακομιστή

cloud. Αυτές οι εξαιρετικά χαμηλές καθυστερήσεις προκαλούν επίσης πολύ πιο γρήγορες αντιδράσεις στις απαραίτητες αποφάσεις και δραστηριότητες.




Για τους παρόχους τηλεπικοινωνιών, ο υπολογισμός αιχμής αφορά το άκρο των δικτύων παρόχων τους, το οποίο ονομάζεται *άκρη δικτύου*. Καθώς αυτοί οι πάροχοι αναπτύσσουν τις υποδομές 5G τους, είναι σε θέση να προσφέρουν στους πελάτες τους υπολογιστική ικανότητα πολύ χαμηλής καθυστέρησης. Φιλοξενώντας συμπλέγματα Kubernetes στις εγκαταστάσεις MEC τους στα άκρα του δικτύου τους, δίνουν τη δυνατότητα στις επιχειρήσεις να αναπτύξουν εγγενείς εφαρμογές στο cloud μέσα σε λίγα χιλιοστά του δευτερολέπτου από τους πελάτες τους. Με τη σειρά του, αυτό το νέο περιβάλλον υπολογιστών αιχμής επιτρέπει εντελώς νέες επιχειρηματικές εφαρμογές.

Τα εξαιρετικά ασφαλή δίκτυα 5G επιτρέπουν επίσης την άμεση σύνδεση σε πολλές νέες τοποθεσίες. Πλέον, μεμονωμένα μηχανήματα σε αποθήκη λιανικής διανομής, κατάστημα, τράπεζα ή ξενοδοχείο ή στον όροφο ενός εργοστασίου, μπορούν να επικοινωνούν με ασφάλεια με απομακρυσμένες υπηρεσίες. Με το 5G, οι υπολογιστές μπορούν να αναπτυχθούν με ασφάλεια σε αυτές τις νέες τοποθεσίες, γεγονός που δημιουργεί νέες λύσεις και επιχειρηματικές ευκαιρίες.

Οι υπολογιστές που είναι εγκατεστημένοι στην άκρη μπορεί να διαφέρουν πολύ. Μπορούν να είναι μηχανήματα κατηγορίας κέντρου δεδομένων, τα οποία ονομάζονται *διακομιστές αιχμής*. Μπορεί να βρείτε διακομιστές αιχμής σε εργοστάσιο, νοσοκομείο, αποθήκη διανομής, λιμάνι αποστολής ή στάδιο. Αυτά τα μηχανήματα είναι συνήθως υλικό x86 και είναι ως επί το πλείστον ανταλλάξιμα περιουσιακά στοιχεία. Δηλαδή, ένας φόρτος εργασίας που προορίζεται για οποιονδήποτε από αυτούς τους διακομιστές αιχμής μπορεί να τοποθετηθεί σε οποιονδήποτε από αυτούς, καθώς παρέχουν μια γενική υπηρεσία υπολογιστών. Οι διακομιστές Edge αναπτύσσονται συχνά σε συμπλέγματα που εκτελούν το Kubernetes, επιτρέποντας έτσι λειτουργίες εγγενείς στο cloud, όπως η αυτόνομη παρακολούθηση φόρτου εργασίας, η αυτόματη κλιμάκωση προς τα πάνω και προς τα κάτω για τη διαχείριση του φόρτου και την αυτόματη μετεγκατάσταση φόρτου εργασίας σε περίπτωση αστοχίας.

Ο άλλος τύπος μηχανής άκρων ονομάζεται *συσκευή άκρων*. Μια συσκευή ακμών συνήθως κατασκευάζεται για έναν συγκεκριμένο σκοπό ή εγκαθίσταται σε ένα συγκεκριμένο πλαίσιο έτσι ώστε να εξυπηρετεί κάποιο συγκεκριμένο σκοπό. Ένα παράδειγμα είναι μια έξυπνη κάμερα που

είναι εγκατεστημένη σε ένα παντοπωλείο και είναι στραμμένη προς μια σειρά από ράφια καταστημάτων όπου προσφέρονται προς πώληση διάφορες μάρκες ζυμαρικών. Ένα άλλο παράδειγμα είναι ένα μηχάνημα που παρακολουθεί την υγρασία σε μια περιοχή και ενεργοποιεί έναν υγραντήρα ή έναν αφυγραντήρα όπως απαιτείται για να διατηρήσει ένα κατάλληλο περιβάλλον.

Ως εκ τούτου, οι υπολογιστικοί φόρτοι εργασίας σε συσκευές άκρων δεν είναι τόσο εναλλάξιμοι όσο στους διακομιστές αιχμής. Για παράδειγμα, δεν θα είχε νόημα να εκτελείτε λογισμικό έξυπνης κάμερας για παρακολούθηση ραφιών στο μηχάνημα διαχείρισης υγρασίας που δεν έχει κάμερα και δεν βρίσκεται πουθενά κοντά σε αυτά τα ράφια. Σε αντίθεση με τους διακομιστές edge, οι συσκευές edge μπορεί να είναι εξαιρετικά διαφορετικές ως προς την αρχιτεκτονική υλικού, την κατανάλωση ενέργειας, την υπολογιστική χωρητικότητα, τη μνήμη, την αποθήκευση, την ικανότητα δικτύωσης, τα συνδεδεμένα περιφερειακά και πολλά άλλα. Συχνά αναπτύσσονται επίσης σε περιβάλλοντα που είναι εντελώς διαφορετικά από τα κέντρα δεδομένων. Βασικές υπηρεσίες όπως συνδέσεις δικτύου ή ακόμα και τροφοδοτικά ενδέχεται να είναι διακοπτόμενες ή με άλλο τρόπο αναξιόπιστες.

Συχνά, οι αρχιτεκτονικές υπολογιστών ακμών αποτελούνται από συσκευές ακμών που συγκεντρώνονται σε διακομιστές ακμών, οι οποίοι μπορεί να αναπτυχθούν στην άκρη του δικτύου. Με τη σειρά τους, αυτοί οι διακομιστές αιχμής συχνά συγκεντρώνονται σε πιο κεντρικά υβριδικά περιβάλλοντα cloud. Αυτές οι αρχιτεκτονικές επιτρέπουν την έξυπνη ανάλυση σε πολύ χαμηλή καθυστέρηση ακριβώς εκεί που δημιουργούνται τα δεδομένα, αλλά επιτρέπουν επίσης την κεντρική συγκέντρωση, τον έλεγχο και τη διαχείριση.

Ο τεράστιος αριθμός των υπολογιστικών συσκευών αιχμής στον κόσμο είναι εκπληκτικός. Η IBM υπολογίζει ότι 15 δισεκατομμύρια συσκευές edge βρίσκονται στο πεδίο σήμερα. Η Cisco Systems εκτιμά ότι ο αριθμός αυτός θα εκτιναχθεί στα 29,3 δισεκατομμύρια μέχρι το επόμενο έτος. Η Juniper Research υπολογίζει ότι ο αριθμός αυτός θα αυξηθεί στα 83 δισεκατομμύρια έως το 2024. Αυτός ο πολλαπλασιασμός των συσκευών άκρων μπορεί να προκαλέσει σημαντικές αλλαγές στον τρόπο με τον οποίο οι άνθρωποι εργάζονται, παίζουν, μαθαίνουν και ζουν. Εάν αυτές οι προβλέψεις είναι σωστές, τότε μια μεμονωμένη μεγάλη επιχείρηση μπορεί να έχει δεκάδες χιλιάδες, εκατοντάδες χιλιάδες, ή ίσως ακόμη και εκατομμύρια μηχανές αιχμής για διαχείριση!

Πώς θα διαχειριστούν οι άνθρωποι όλες αυτές τις μηχανές αιχμής; Πώς θα διασφαλίσουμε ότι οι κατάλληλοι φόρτοι εργασίας λογισμικού αναπτύσσονται σε όλα τα σωστά μέρη εγκαίρως; Πώς θα διασφαλίσουμε ότι οι επείγουσες ενημερώσεις κώδικα ασφαλείας παραδίδονται σε όλους εκείνους τους φόρτους εργασίας που τις απαιτούν; Πώς θα αποτρέψουμε τους κακόβουλους ηθοποιούς από το να οδηγήσουν αυτές τις συσκευές σε ένα botnet και να προκαλέσουν τον όλεθρο μαζί τους;

Από cloud-native σε edge-native

Για να διαχειριστείτε διακομιστές και συσκευές αιχμής, μπορείτε να χρησιμοποιήσετε διδάγματα στο υβριδικό περιβάλλον cloud. Πριν από δεκαετίες, οι εικονικές μηχανές (VM) αντικατέστησαν το αποκλειστικό υλικό σε αυτά τα περιβάλλοντα. Πιο πρόσφατα, τα κοντέινερ έφεραν επανάσταση στα

κέντρα δεδομένων. Τα κοντέινερ είναι τάξεις μεγέθους πιο αποτελεσματικά από τα VM και μπορούν να εκτελεστούν στα περισσότερα μέρη όπου υπάρχει πυρήνας Linux. Ως αποτέλεσμα, ο πιο συνηθισμένος τρόπος ανάπτυξης λογισμικού στο cloud σήμερα είναι η χρήση κοντέινερ. Ο *εγγενής στο cloud* υπολογισμός αναφέρεται κυρίως στη χρήση κοντέινερ για την ανάπτυξη κλιμακούμενων μικροϋπηρεσιών. Οι αρχιτεκτονικές *Edge-native* μεταφέρουν αυτές τις μικροϋπηρεσίες με κοντέινερ προς τα έξω.

Με τα περισσότερα σύννεφα, μπορείτε να διαχειριστείτε φόρτους εργασίας σε κοντέινερ σε κλίμακα χρησιμοποιώντας συμπλέγματα Kubernetes. Τα κέντρα δεδομένων Edge, όπως τα MEC 5G, παρέχουν επίσης συχνά Kubernetes για ανάπτυξη λογισμικού με κοντέινερ. Το Kubernetes μπορεί να σας βοηθήσει να αναπτύξετε αυτόματα νέες παρουσίες όταν αυξάνεται το φορτίο και να διαγράψετε περιπτώσεις όταν μειώνεται το φόρτο. Μπορεί επίσης να σας βοηθήσει να διατηρήσετε ισχυρές τις εφαρμογές σας με τη μετεγκατάσταση παρουσιών σε νέα μηχανήματα στο σύμπλεγμα όταν συμβαίνουν αστοχίες του μηχανήματος. Το Kubernetes είναι μια εξαιρετική επιλογή όταν οι διακομιστές edge είναι όσο το δυνατόν πιο ομοιόμορφοι και ανταλλάξιμοι.

Οι συσκευές Edge τείνουν να είναι πιο διαφορετικές ως προς την αρχιτεκτονική και τις δυνατότητες. Έχουν λιγότερο αξιόπιστες συνδέσεις δικτύου, ακόμη και αναξιόπιστη ισχύ. δεν είναι εναλλάξιμα ως προς τον σκοπό. Είναι επίσης λιγότερο ασφαλή από φυσική άποψη, καθώς συχνά αναπτύσσονται σε εξωτερικούς χώρους ή σε άλλες τοποθεσίες χωρίς επίβλεψη. Τα περιβάλλοντα συσκευών Edge διαφέρουν πολύ από τα περιβάλλοντα κέντρων δεδομένων. Το Kubernetes, το οποίο σχεδιάστηκε για τη διαχείριση κοντέινερ σε κέντρα δεδομένων cloud, δεν είναι επομένως πάντα η καλύτερη επιλογή για τη διαχείριση συσκευών αιχμής.

Η ποικιλία των υπολογιστών αιχμής, από την άκρη του δικτύου έως τους διακομιστές και τις συσκευές αιχμής, λειτουργεί καλύτερα με ένα ανοιχτό οικοσύστημα. Τα ανοιχτά οικοσυστήματα ενεργοποιούνται από λογισμικό ανοιχτού κώδικα και μια σειρά από προμηθευτές. Ο οργανισμός Linux Foundation Edge παρέχει το έργο Open Horizon ακριβώς για αυτόν τον σκοπό. Το Open Horizon επιτρέπει σε συσκευές edge, διακομιστές edge (με μόνο Linux και Docker) και ολόκληρα συμπλέγματα Kubernetes την ταυτόχρονη και ασφαλή διαχείριση σε κλίμακα από τα ίδια εργαλεία. Το προϊόν IBM Edge Application Manager είναι η εμπορική διανομή Open Horizon της IBM. Πάνω από το Open Horizon, το IBM Edge Application Manager προσθέτει μια γραφική διεπαφή ιστού για να απλοποιήσει τη διαχείριση των κοντέινερ σας σε ολόκληρο τον στόλο συσκευών και διακομιστών αιχμής.

Σύνοψη

Ο σκοπός του edge computing είναι να φέρει τις εφαρμογές σας πιο κοντά στο σημείο όπου δημιουργούνται τα δεδομένα και πρέπει να πραγματοποιηθούν ενέργειες. Όταν το κάνετε αυτό, μπορείτε να επιτύχετε πολύ πιο γρήγορους χρόνους απόκρισης (πολύ χαμηλή καθυστέρηση από τη στιγμή που συμβαίνει ένα συμβάν έως την εμφάνιση μιας απόκρισης). Απολαμβάνετε επίσης το πλεονέκτημα της μεταφοράς λιγότερων δεδομένων μέσω του Διαδικτύου, γεγονός που μειώνει το

κόστος backhaul και διατηρεί τα δεδομένα πιο τοπικά, ασφαλή και ιδιωτικά. Με το edge computing, μπορείτε επίσης να αναλύσετε περισσότερα δεδομένα σε υψηλότερες αναλύσεις και συχνότητες.

Μερικοί από τους κύριους παράγοντες διευκόλυνσης των υπολογιστών αιχμής περιλαμβάνουν τα δίκτυα 5G και την επικράτηση μικρότερων, λιγότερο ακριβών, ισχυρότερων και δικτυωμένων υπολογιστών που υποστηρίζουν κοντέινερ σε πολλές διαφορετικές αρχιτεκτονικές υλικού.

Στο ένα άκρο του φάσματος, ο υπολογισμός αιχμής αφορά την παροχή υπηρεσιών στην άκρη του παρόχου τηλεπικοινωνιών, επιτρέποντας στις εφαρμογές κινητών και κινητών τηλεφώνων να έχουν εξαιρετικά γρήγορους χρόνους απόκρισης. Στο άλλο άκρο του φάσματος, ο υπολογισμός αιχμής αφορά τη χρήση της μεγαλύτερης υπολογιστικής ικανότητας των σημερινών μικρών συσκευών που κυκλοφορούν στο πεδίο. Υπάρχουν επίσης πολλές άλλες εφαρμογές αιχμής μεταξύ αυτών των άκρων και ο υπολογισμός ακμών προβλέπεται να αναπτυχθεί εκθετικά κατά την υπόλοιπη τουλάχιστον δεκαετία αυτής της δεκαετίας.

Η επανάσταση του edge computing είναι συγκρίσιμη με την προηγούμενη επανάσταση φορητών υπολογιστών. Είναι έτοιμο να έχει παρόμοιο, ή ακόμη μεγαλύτερο, αντίκτυπο στις ζωές και τις επιχειρήσεις μας. Το Edge computing παρουσιάζει ταυτόχρονα μια τεράστια πρόκληση για την ασφαλή διαχείριση όλων αυτών των δεδομένων και μια τεράστια ευκαιρία για τη δημιουργία νέας αξίας για τους πελάτες.

Το IBM Edge Application Manager, το οποίο βασίζεται στο Open Horizon, έχει σχεδιαστεί για να σας βοηθήσει να πλοηγηθείτε σε αυτήν την τεράστια αλλαγή παραδείγματος. Με την υποστήριξη της IBM, μπορείτε να είστε έτοιμοι να διαχειριστείτε τις προκλήσεις των υπολογιστών αιχμής και να ανεβάσετε την επιχείρησή σας στο επόμενο επίπεδο. Ένας εντελώς νέος κόσμος έρχεται. Ας το δημιουργήσουμε μαζί.

## 2.5.5 Απόρρητο εφαρμογής και IoT

Εισαγωγή

Ο κίνδυνος απορρήτου μιας εφαρμογής λαμβάνει υπόψη την πιθανή αγωνία και τη βλάβη που προκαλείται στους χρήστες της εφαρμογής, εάν οι χρήστες χάσουν τον έλεγχο των προσωπικών τους πληροφοριών που διαχειρίζονται οι εφαρμογές. Οι οργανισμοί που παρέχουν απευθείας εφαρμογές σε χρήστες υπόκεινται στον δικό τους κίνδυνο απορρήτου, ο οποίος λαμβάνει υπόψη τις πιθανές ζημιές στη φήμη και τις οικονομικές επιπτώσεις του οργανισμού επεξεργασίας, σε περίπτωση που η εφαρμογή δεν παρέχει στους πολίτες της ΕΕ τα δικαιώματα απορρήτου που προβλέπονται από τον Γενικό Κανονισμό για την Προστασία Δεδομένων. GDPR). Ως εκ τούτου, η ενσωμάτωση ενός απορρήτου εφαρμογής από το σχεδιασμό, που αναφέρεται επίσης ως προστασία δεδομένων από το σχεδιασμό από τον GDPR, στον κύκλο ζωής ανάπτυξης λογισμικού είναι μια ουσιαστική πρακτική για να διασφαλιστεί ότι ο κίνδυνος απορρήτου μιας εφαρμογής είναι πλήρως κατανοητός και αξιολογημένος και όπου κρίνεται σκόπιμο, μετριάζεται σε αποδεκτό επίπεδο κινδύνου. Αυτό το

άρθρο είναι το Μέρος 2 μιας σειράς άρθρων που παρέχει καθοδήγηση για την ανάπτυξη εφαρμογών που συμμορφώνονται με τον Γενικό Κανονισμό Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης. Το Μέρος 1 συνοψίζει τον GDPR και Μέρος 3 διερευνά πρακτικές τεχνικές ανάπτυξης εφαρμογών που μπορούν να μετριάσουν τον κίνδυνο απορρήτου μιας εφαρμογής.

Προστασία δεδομένων GDPR βάσει της απαίτησης σχεδιασμού

Το άρθρο 25 του ΓΚΠΔ ορίζει ότι η προστασία δεδομένων βάσει σχεδιασμού ισχύει για οργανισμούς που έχουν ρόλο ελεγκτή, αυτό ισχύει άμεσα για εφαρμογές που έχουν αναπτυχθεί εσωτερικά για χρήση από τον οργανισμό του προγραμματιστή. Όταν οι εφαρμογές αναπτύσσονται για χρήση από εξωτερικούς οργανισμούς, αυτοί οι οργανισμοί ως ελεγκτές, θα προσπαθήσουν να κατανοήσουν και να επαληθεύσουν τον κίνδυνο απορρήτου της εφαρμογής με τους προγραμματιστές της εφαρμογής. Ως εκ τούτου, μια προσέγγιση ανάπτυξης προστασίας δεδομένων μέσω σχεδιασμού θα πρέπει να υιοθετηθεί ανεξάρτητα από το εάν μια εφαρμογή προορίζεται για εσωτερική χρήση ή για χρήση από άλλους οργανισμούς που έχουν ρόλο ελεγκτή. Το άρθρο 25 παράγραφος 2 του GDPR απαιτεί από προεπιλογή την προστασία των δεδομένων. Αυτό σημαίνει ότι όλες οι ρυθμίσεις απορρήτου της εφαρμογής πρέπει να ρυθμιστούν για την προστασία του απορρήτου ενός χρήστη όταν η εφαρμογή παρέχεται στους χρήστες. *Άρθρο 25 Προστασία δεδομένων από το σχεδιασμό και από προεπιλογή* 1. Λαμβάνοντας υπόψη την εξέλιξη της τεχνολογίας, το κόστος υλοποίησης και τη φύση, το εύρος, το πλαίσιο και τους σκοπούς της επεξεργασίας ως καθώς και τους κινδύνους ποικίλης πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που θέτει η επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλες τεχνικές και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, που έχουν σχεδιαστεί για την εφαρμογή αρχών προστασίας δεδομένων, όπως η ελαχιστοποίηση δεδομένων, με αποτελεσματικό τρόπο και για την ενσωμάτωση των απαραίτητων διασφαλίσεων στην επεξεργασία προκειμένου να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των δεδομένων μαθήματα. 2. Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας. Η υποχρέωση αυτή ισχύει για τον όγκο των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, την έκταση της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα μέτρα αυτά διασφαλίζουν ότι, εξ ορισμού, τα προσωπικά δεδομένα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του ατόμου σε αόριστο αριθμό φυσικών προσώπων.Ένας εγκεκριμένος μηχανισμός πιστοποίησης σύμφωνα με το άρθρο 42 μπορεί να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με την απαιτήσεις που ορίζονται στις παραγράφους 1 και 2 του παρόντος άρθρου. Υποστηρίζεται από την αιτιολογική σκέψη 78 Ένα ουσιαστικό εργαλείο για την ανάπτυξη εφαρμογών με προστασία δεδομένων βάσει σχεδιασμού είναι η αξιολόγηση επιπτώσεων της περιστροφής δεδομένων.

Αξιολόγηση επιπτώσεων στην προστασία δεδομένων εφαρμογής

Η αξιολόγηση επιπτώσεων της προστασίας δεδομένων εφαρμογής (DPIA) βοηθά τους προγραμματιστές να εντοπίσουν, να αναλύσουν και να εξηγήσουν πώς μια εφαρμογή επηρεάζει τα δικαιώματα και τις ελευθερίες απορρήτου των χρηστών της. Ένα DPIA θα πρέπει να εκτελείται έναντι εφαρμογών που σκοπεύουν να συλλέξουν, να διατηρήσουν ή/και να μοιραστούν προσωπικές πληροφορίες. Με την ενσωμάτωση ενός DPIA νωρίς στον κύκλο ζωής ανάπτυξης λογισμικού, οι προγραμματιστές είναι σε θέση να μετριάσουν τους απαράδεκτους κινδύνους απορρήτου και να επιλύσουν ζητήματα συμμόρφωσης με τα δικαιώματα απορρήτου των χρηστών του GDPR πριν από την ολοκλήρωση του σχεδιασμού της εφαρμογής. Αυτό διασφαλίζει ότι η εφαρμογή αναπτύσσεται αποτελεσματικά για την ελαχιστοποίηση του κινδύνου απορρήτου, που ωφελεί τους χρήστες, και του κινδύνου για τους οργανισμούς επεξεργασίας δεδομένων που παρέχουν την εφαρμογή. Οι DPIA θα πρέπει επίσης να εκτελούνται αναδρομικά έναντι εφαρμογών που έχουν εκδοθεί προηγουμένως και βρίσκονται σε παραγωγή για να διασφαλιστεί ότι ο κίνδυνος απορρήτου τους είναι αποδεκτός και για να επαληθευτεί η συμμόρφωσή τους με τον GDPR.

Ρόλοι και αρμοδιότητες DPIA εφαρμογής

Οι αναμενόμενοι ρόλοι και ευθύνες που σχετίζονται με μια εφαρμογή DPIA περιλαμβάνουν:

Ο επικεφαλής προγραμματιστής είναι υπεύθυνος για τη διαχείριση της διαδικασίας DPIA της εφαρμογής. Όπου δεν υπάρχει επικεφαλής προγραμματιστής, η ευθύνη του DPIA θα πρέπει να βαρύνει τον υπεύθυνο έργου ανάπτυξης εφαρμογών.

Ένας υπεύθυνος προστασίας δεδομένων (DPO) ή ένας ειδικός σε θέματα απορρήτου δεδομένων απαιτείται να συμβουλευτεί και να υποστηρίξει τη διαδικασία DPIA, η οποία αναφέρεται ως απαίτηση DPIA στο άρθρο 35 παράγραφος 2 του GDPR. *Άρθρο 35 (2) Ο υπεύθυνος επεξεργασίας ζητά τη συμβουλή του υπευθύνου προστασίας δεδομένων, όπου ορίζεται, κατά τη διεξαγωγή εκτίμησης επιπτώσεων στην προστασία δεδομένων.*

Ένας DPO μπορεί να προέρχεται από εξωτερική πηγή εάν ο οργανισμός προγραμματιστή δεν έχει ρόλο DPO ή ένα άτομο με επαρκή τεχνογνωσία σε θέματα απορρήτου δεδομένων. Απαιτείται επίσης ένας DPO για την υπογραφή του ολοκληρωμένου DPIA.

Ένας επαγγελματίας ασφάλειας πληροφοριών ή ένας ειδικός σε θέματα ασφάλειας εφαρμογών απαιτείται να συμβουλευτεί και να επαληθεύσει ότι οι βέλτιστες πρακτικές ασφάλειας εφαρμογών υιοθετούνται καθ' όλη τη διάρκεια της ανάπτυξης της εφαρμογής.

Συνιστάται ένας διαχειριστής κινδύνου να συμβουλεύεται και να συμβουλεύει σχετικά με τις πρακτικές διαχείρισης κινδύνου απορρήτου.

Ο υπεύθυνος του έργου ανάπτυξης θα πρέπει να ενημερώνεται για τα αποτελέσματα και τις ενέργειες DPIA.

Οι χορηγοί έργων και οι διευθυντές επιχειρήσεων είναι υπεύθυνοι για τον κίνδυνο απορρήτου. Ως εκ τούτου, πρέπει να ενημερωθούν και να τους παρασχεθεί αντίγραφο του συμπληρωμένου DPIA και του μητρώου κινδύνου απορρήτου της εφαρμογής.

Όταν αναπτύσσονται εφαρμογές για εξωτερικούς οργανισμούς επεξεργασίας, αναμένετε από αυτούς τους οργανισμούς να ζητήσουν αντίγραφο της καθοδήγησης απορρήτου της εφαρμογής DPIA και εφαρμογής εφαρμογής ως μέρος της δικής τους διαδικασίας DPIA, της επαλήθευσης των υποχρεώσεων GDPR και της διαχείρισης κινδύνου απορρήτου.

Εκτέλεση DPIA εντός του SDLC

Οι υποχρεώσεις για τα δικαιώματα απορρήτου της εφαρμογής GDPR θα πρέπει να τεκμηριώνονται ως απαιτήσεις στη φάση ανάλυσης απαιτήσεων του Κύκλου Ζωής Ανάπτυξης Λογισμικού (SDLC). Η DPIA θα πρέπει να εκτελείται εντός της φάσης σχεδιασμού του SDLC. Στη συνέχεια, θα πρέπει να διεξαχθεί περαιτέρω επαλήθευση του κινδύνου απορρήτου σε όλες τις τελευταίες φάσεις του SDLC, για να διασφαλιστεί ότι όλες οι απαιτήσεις απορρήτου της εφαρμογής έχουν εκπληρωθεί και ότι ο σχεδιασμός της εφαρμογής μετριάζει ή εξαλείφει τους κινδύνους απορρήτου όπως προβλέπεται. Οι φάσεις εφαρμογής SDLC (Μοντέλο Καταρράκτη) περιλαμβάνουν:

Ανάλυση απαιτήσεων (υποχρεώσεις δικαιωμάτων απορρήτου GDPR)

Σχεδίαση (DPIA)

Ανάπτυξη (Παράδοση ενεργειών αποτελεσμάτων DPIA και λειτουργικότητα δικαιωμάτων GDPR)

Δοκιμές (αποτελέσματα DPIA, λειτουργικότητα δικαιωμάτων GDPR και δοκιμή ασφάλειας εφαρμογών)

Εφαρμογή (οδηγίες εφαρμογής απορρήτου)

Συντήρηση (Επανεξέταση και ενημερώσεις DPIA)

Οι υποχρεώσεις του GDPR για τα δικαιώματα απορρήτου επεξηγούνται στο πρώτο μέρος αυτής της σειράς καθοδήγησης. Οι εντοπισμένοι κίνδυνοι απορρήτου θα πρέπει να αξιολογούνται με σκοπό τον σχεδιασμό τεχνικών λύσεων εφαρμογών που ελαχιστοποιούν τον κίνδυνο απορρήτου, όπως η χρήση κρυπτογράφησης βάσεων δεδομένων και ψευδωνυμοποίησης. Αυτές οι τεχνικές λύσεις συζητούνται στο τρίτο μέρος αυτής της σειράς καθοδήγησης.

Διαδικασία DPIA εφαρμογής

Υπάρχουν έξι φάσεις σε μια εφαρμογή DPIA:

Προσδιορίστε την ανάγκη για DPIA

Περιγράψτε τη ροή προσωπικών δεδομένων

Εντοπισμός κινδύνων απορρήτου

Προσδιορίστε και αξιολογήστε λύσεις απορρήτου

Τεκμηριώστε τα αποτελέσματα DPIA και υπογράψτε τον DPO

Εφαρμόστε λύσεις απορρήτου DPIA εντός του σχεδίου ανάπτυξης

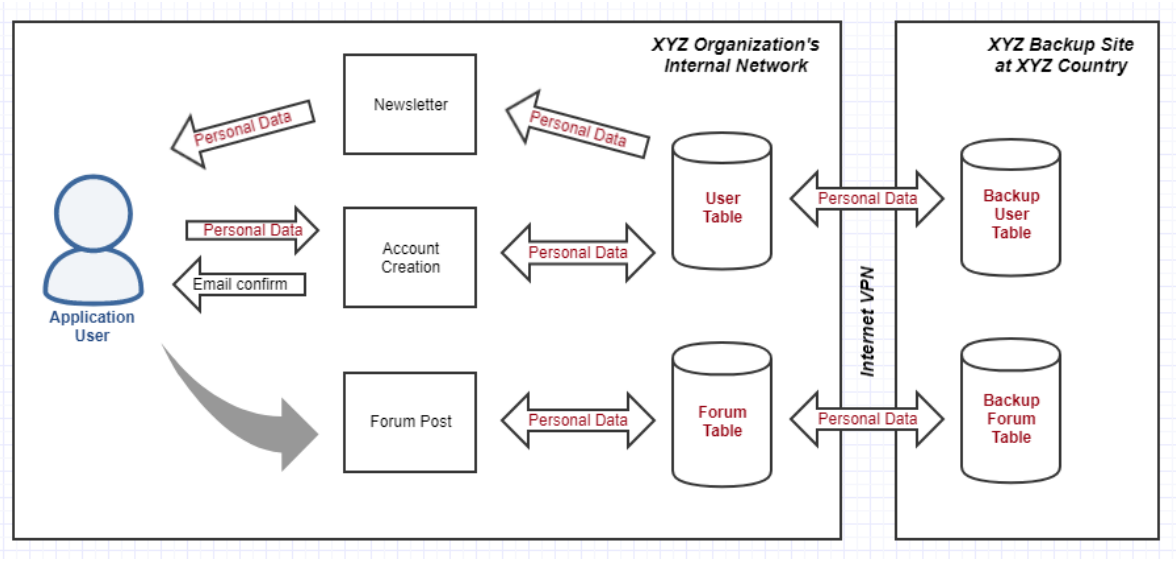
Προσδιορίστε την ανάγκη για DPIA

Το άρθρο 35 παράγραφος 1 του ΓΚΠΔ απαιτεί τη διενέργεια εκτίμησης επιπτώσεων στην προστασία δεδομένων όπου *"νέες τεχνολογίες"* είναι *"πιθανόν να οδηγήσουν σε υψηλό κίνδυνο"* για άτομα. Η αιτιολογική σκέψη 75 που υποστηρίζει περιγράφει τους κινδύνους απορρήτου που είναι τυπικοί των εφαρμογών που επεξεργάζονται προσωπικά δεδομένα, δηλώνοντας *"όπου η επεξεργασία μπορεί να προκαλέσει διακρίσεις, κλοπή ταυτότητας ή απάτη, οικονομική απώλεια, βλάβη στη φήμη, απώλεια του απορρήτου των προσωπικών δεδομένων που προστατεύονται από επαγγελματικό απόρρητο, μη εξουσιοδοτημένη ανατροπή της ψευδωνυμοποίησης ή οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα»*. Η ανάπτυξη νέας εφαρμογής μπορεί να θεωρηθεί ως "νέα τεχνολογία" σύμφωνα με το άρθρο 35 παράγραφος 1. Αν και ο GDPR δεν ορίζει συγκεκριμένα τον "υψηλού κινδύνου", όπου οι εφαρμογές επεξεργάζονται προσωπικά δεδομένα μαζικά, είναι πιθανό οι περισσότερες εποπτικές αρχές να θεωρούν ότι αυτές οι εφαρμογές ενέχουν εγγενή υψηλό κίνδυνο για το απόρρητο των χρηστών, ειδικά όταν η εφαρμογή αντιμετωπίζει το Διαδίκτυο. Επομένως, εκτός εάν η εφαρμογή δεν έχει δυνατότητα επεξεργασίας προσωπικών στοιχείων πολιτών της ΕΕ, συνιστάται η διενέργεια ΕΑΠ σε όλες τις αναπτυγμένες εφαρμογές για συμμόρφωση με το άρθρο 35 παράγραφος 1 του GDPR. *Άρθρο 35 παράγραφος 1 Όταν ένας τύπος επεξεργασίας που χρησιμοποιεί ιδίως νέες τεχνολογίες και λαμβάνει υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, είναι που ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, αξιολόγηση του αντίκτυπου των προβλεπόμενων εργασιών επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα. Μια ενιαία αξιολόγηση μπορεί να αφορά ένα σύνολο παρόμοιων εργασιών επεξεργασίας που παρουσιάζουν παρόμοιους υψηλούς κινδύνους.* Άρθρο 35 παράγραφος 7**Αξιολόγηση επιπτώσεων στην προστασία δεδομένων«Η αξιολόγηση περιλαμβάνει τουλάχιστον: (α) συστηματική περιγραφή των προβλεπόμενων εργασιών επεξεργασίας και των σκοπών της επεξεργασίας, συμπεριλαμβανομένων, κατά περίπτωση, των έννομο συμφέρον που επιδιώκει ο υπεύθυνος επεξεργασίας· β) αξιολόγηση της αναγκαιότητας και της αναλογικότητας των εργασιών επεξεργασίας σε σχέση με τους σκοπούς· γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1· και (δ) τα μέτρα που προβλέπονται για την αντιμετώπιση των κινδύνων, συμπεριλαμβανομένων διασφαλίσεων, μέτρων ασφαλείας και μηχανισμών για τη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα και την απόδειξη της συμμόρφωσης με τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερομένων προσώπων.__

Περιγράψτε τη ροή προσωπικών δεδομένων

Το DPIA της εφαρμογής πρέπει να τεκμηριώνεται, το οποίο θα πρέπει να ξεκινά με μια περιγραφή του γενικού σκοπού της εφαρμογής και μια απλή επισκόπηση των λειτουργιών της εφαρμογής. Καταγράψτε επίσης εάν ο οργανισμός ανάπτυξης εφαρμογών θα έχει ρόλο GDPR ως υπεύθυνου επεξεργασίας (δηλαδή παροχής της εφαρμογής), επεξεργαστή (δηλαδή απλώς φιλοξενώντας την εφαρμογή) ή κανένα από τα δύο. Το επόμενο βήμα είναι να προσδιοριστεί και να περιγραφεί ο τρόπος λήψης, επεξεργασίας, αποθήκευσης και μετακίνησης προσωπικών πληροφοριών από την εφαρμογή. Με τη βοήθεια του αρχιτέκτονα εφαρμογών, ελέγξτε και χαρτογραφήστε τις ροές και τις διαδικασίες δεδομένων της εφαρμογής. Η τεκμηρίωση με ένα διάγραμμα ροής δεδομένων, επιτρέπει στις διαδικασίες της εφαρμογής και τις ροές προσωπικών δεδομένων να περιγράφονται με σαφήνεια και να κατανοούνται, ένα παράδειγμα φαίνεται στο Σχήμα 1.

**Εικόνα 21. Παράδειγμα ροής δεδομένων εφαρμογής**




Εκτός από το διάγραμμα ροής δεδομένων, θα πρέπει να καταγράφονται περαιτέρω πιο ολοκληρωμένες λεπτομέρειες σχετικά με τη χρήση προσωπικών δεδομένων της εφαρμογής. Ελέγξτε τη σχεδίαση της εφαρμογής και εξερευνήστε τις ακόλουθες πτυχές με τους τεχνικούς πελάτες.

Συλλογή προσωπικών δεδομένων Εισαγωγή προσωπικών δεδομένων: Η διαδικασία δημιουργίας λογαριασμού χρήστη Δυνατότητες εισαγωγής δεδομένων χρήστη και επεξεργασίας δεδομένων Μεταφορές δεδομένων σε π.χ. δεδομένα που συλλέγονται από πηγές τρίτων Πεδία προσωπικών δεδομένων: Τεκμηριώστε τα συγκεκριμένα ονόματα πεδίων και πίνακες που περιέχουν προσωπικά δεδομένα Επισήμανση προσωπικών δεδομένων πεδία που θεωρούνται άμεσα ή έμμεσα προσωπικά αναγνωριστικά, π.χ. όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμός λογαριασμού, δεδομένα τοποθεσίας Επισημάνετε τα πεδία προσωπικών δεδομένων που ορίζονται ως «Ειδικές Κατηγορίες» προσωπικών δεδομένων σύμφωνα με τον GDPR, π.χ. βιομετρικά, υγεία, φυλή, πολιτικές απόψεις, θρησκεία, γενετικά δεδομένα Επισημάνετε πεδία προσωπικών δεδομένων που

μπορούν να χρησιμοποιηθούν για τον εντοπισμό ή την παρακολούθηση ενός ατόμου, π.χ. cookies, διεύθυνση IP, γεωμετρικά δεδομένα Επισημάνετε τυχόν μη καθορισμένα πεδία προσωπικών δεδομένων που ενδέχεται να περιέχουν προσωπικά δεδομένα, όπως πεδία πλαισίου κειμένου, π.χ. χρήστη που πληκτρολογεί ελεύθερα προσωπικά δεδομένα σε πλαίσιο κειμένου περιγραφής Τεκμηρίωση του σκοπού κάθε πεδίου προσωπικών δεδομένων: τεκμηριώστε τον λόγο λήψης της αίτησης και επεξεργασία κάθε αναγνωρισμένου πεδίου προσωπικών δεδομένων Έγγραφο εάν τα παιδιά θα μπορούν να χρησιμοποιήσουν την εφαρμογή

Επεξεργασία προσωπικών δεδομένων Τεκμηριώστε πώς θα χρησιμοποιηθούν τα προσωπικά δεδομένα από την εφαρμογή Αναλυτικά τυχόν αυτόματες αλλαγές ή δημιουργία προσωπικών δεδομένων από την εφαρμογή: όπως η αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων από την εφαρμογή, οι διαδικασίες δημιουργίας προφίλ και οποιαδήποτε τήρηση αρχείων δραστηριότητα χρήστη Έγγραφο στο οποίο η εφαρμογή χρησιμοποιεί τεχνολογία ή διαδικασίες που θα μπορούσαν να θεωρηθούν ως παρεμβατικές στο απόρρητο: π.χ. χρήση βιομετρικών στοιχείων, παρακολούθηση τοποθεσίας χρήστη και ανάλυση γενετικών δεδομένων

Πρόσβαση και αλληλεπίδραση χρήστη Τεκμηριώστε τις δυνατότητες αλληλεπίδρασης του χρήστη της εφαρμογής με τα προσωπικά του δεδομένα: Δυνατότητα χρήστη να βλέπει όλα τα πεδία προσωπικών δεδομένων του Δυνατότητα χρήστη να επεξεργάζεται και να διαγράφει τα προσωπικά του δεδομένα Τεκμηρίωση τυχόν παρεχόμενων ρόλων λογαριασμού χρήστη με προνομιακά επίπεδα πρόσβασης σε προσωπικά δεδομένα δεδομένα όπως λογαριασμοί διαχειριστή, επόπτη, υποστήριξης και αναφοράς που μπορούν να έχουν πρόσβαση σε αρχεία προσωπικών δεδομένων πολλαπλών χρηστών. Αναλυτικά οι δυνατότητες του ρόλου του λογαριασμού στην πρόσβαση, την αλλαγή και την εξαγωγή προσωπικών δεδομένων.

Αποθήκευση προσωπικών δεδομένων Καταγράψτε λεπτομέρειες όλων των βάσεων δεδομένων\πίνακες που χρησιμοποιούνται από την εφαρμογή για την ανάκτηση και αποθήκευση προσωπικών πληροφοριών Περιγράψτε πού φιλοξενείται κάθε βάση δεδομένων\πίνακες (π.χ. διακομιστής/σύστημα) και πού βρίσκεται φυσικά: εξετάστε το ενδεχόμενο τοπικής φιλοξενίας, φιλοξενίας τρίτων\cloud και συστήματα δημιουργίας αντιγράφων ασφαλείας Αναλυτικά οποιαδήποτε αποθήκευση ή χρήση προσωπικών δεδομένων στα συστήματα παρακολούθησης και καταγραφής. δηλαδή αρχεία καταγραφής διακομιστή τοπικών εφαρμογών, εξαγωγές εφαρμογών σε διακομιστές καταγραφής συστήματος

Εξαγωγή προσωπικών δεδομένων Τεκμηρίωση όλων των σημείων εξόδου προσωπικών δεδομένων: εξετάστε αναφορές, μηνύματα ηλεκτρονικού ταχυδρομείου, SMS, ταχυδρομική αλληλογραφία (εκτύπωση), μαζικές μεταφορές δεδομένων προς τα έξω και διαδικασίες εξαγωγής δεδομένων Τεκμηρίωση τυχόν κοινής χρήσης προσωπικών δεδομένων και προσβασιμότητας Κοινή χρήση ή πρόσβαση που παρέχεται σε τρίτους οργανισμούς , άλλοι χρήστες εντός της εφαρμογής, συνδεσιμότητα με άλλες εφαρμογές ή δημόσια, π.χ. συνδεσιμότητα μέσων κοινωνικής δικτύωσης Υποστήριξη τρίτων, π.χ. απομακρυσμένη τεχνική υποστήριξη, αναβαθμίσεις συστήματος

Ένα υπολογιστικό φύλλο ή ένας πίνακας είναι μια χρήσιμη μέθοδος για την τεκμηρίωση της χρήσης τεχνικών προσωπικών δεδομένων της εφαρμογής. Το σχήμα 2 απεικονίζει ένα παράδειγμα.

### Εικόνα 22. Χρήση τεχνικών προσωπικών δεδομένων εφαρμογής

| Field | Table | Database location | Data Ingress | Purpose | Data Subject Identifier? | Special Cat. Data? | Can Track Data Subject? | User Interaction | Accessible to other App Users? | Public Accessible? | Privacy Risk Notes |
|---|---|---|---|---|---|---|---|---|---|---|---|
| <full_name> | Users | Internal Data Centre, Backup in Cloud | Data subject requested input as part of the account creation process | Required personal identifier for the application user's profile | Yes | No | No | Edit, View | No | No | None |
| <app_user_id> | Users | Internal Data Centre, Backup in Cloud | Data subject requested input as part of the account creation process | Unique ID required to authenticate user account with application | Yes | No | No | View Only | No | No | Users will be able delete their account and all data, however, forum post may not be removed |
| <password> | Users | Internal Data Centre, Backup in Cloud | Data subject requested input as part of the account creation process | Required to authenticate the user's account with the application | No | No | No | Edit only | No | No | Password will be stored using a salted hash in the table |
| <email address> | Users | Internal Data Centre, Backup in Cloud | Data subject requested input as part of the account creation process | Required to notify the user of forum posts and comments, and to provide a monthly copy of the newsletter (if opted in), used for account recreation and for password resets | Yes | No | No | Edit, View | No | No | Notifications will be sent to the users, which will require a specific opt-in by the data subject, with opt-out enabled by default. |
| <forum handle> | Users | Internal Data Centre, Backup in Cloud | Data subject requested input as part of the account creation process | Required identify the data subject (user) on the forum | Yes | No | No | Edit, View | Yes | No | Forum handle can identify a data subject (directly or indirectly) |
| <religion> | Forum | Internal Data Centre, Backup in Cloud | Data subject requested input as part of the account creation process | The forum is religious, and the project sponsors seta a requirement for users to be optionally identify with their religion of choice on their forum account profile | No | Yes | No | Edit, View, Delete | Yes | No | Religion is not a mandatory field, users are asked to provide as part of account creation |
| <ip_address> | Forum, AppsLog | Internal Data Centre | Created and used by application security and logging processes | Application captures the users' device IP address for security purposes i.e. Tracking should the user's account be compromised by a third party | Yes | No | Yes | Field Not accessible | No | No | Confirmed this field will not used with any automated or profiling processed by the application |

Προσδιορισμός κινδύνων απορρήτου

Το επόμενο βήμα της DPIA είναι ο εντοπισμός των κινδύνων για την προστασία της ιδιωτικής ζωής με την εξέταση της τεκμηρίωσης της ροής δεδομένων προσωπικού χαρακτήρα. Αυτή η αναθεώρηση θα πρέπει να υποστηρίζεται από τον υπεύθυνο προστασίας δεδομένων ή από ειδικό σε θέματα απορρήτου δεδομένων. Συμμετάσχετε επίσης έναν διαχειριστή κινδύνου ή έναν επαγγελματία κινδύνου, για να καθοδηγήσει και να τεκμηριώσει επίσημα την αξιολόγηση του κινδύνου προστασίας της ιδιωτικής ζωής. Υπάρχουν τρεις γενικές ομάδες κινδύνου απορρήτου που πρέπει να λάβετε υπόψη και να τεκμηριώσετε με μια εφαρμογή DPIA:

Κίνδυνοι απορρήτου χρήστη της εφαρμογής (υπόκειται στα δεδομένα)

Κίνδυνος απορρήτου εφαρμογής στη διευκόλυνση των δικαιωμάτων απορρήτου του GDPR στους χρήστες

Κινδυνεύει το απόρρητο του οργανισμού ως υπεύθυνος επεξεργασίας ή επεξεργασίας

Κίνδυνοι απορρήτου χρήστη της εφαρμογής

Κατά την αξιολόγηση του κινδύνου απορρήτου των χρηστών της εφαρμογής, εξετάστε τα πιθανά σενάρια παραβίασης της εφαρμογής στα δικαιώματα και τις ελευθερίες απορρήτου ενός χρήστη, με την πιθανότητα κάθε παραβίασης του απορρήτου και τον πιθανό αντίκτυπο στον χρήστη, όπως προσωπική αγωνία και οικονομική απώλεια. Οι ακόλουθοι τύποι εισβολών απορρήτου εφαρμογών μπορούν να επηρεάσουν αρνητικά τους χρήστες και θα πρέπει να διερευνηθούν:

Εμπιστευτικότητα: σενάρια που αφορούν ακούσιο ή κακόβουλο παραβιασμό προσωπικών δεδομένων

Ακεραιότητα: σενάρια που οδηγούν σε ανακριβή δεδομένα προσωπικού χαρακτήρα

Διαθεσιμότητα: σενάρια που καθιστούν την εφαρμογή ή τα προσωπικά δεδομένα απρόσιτα στους χρήστες

Περιγράψτε κάθε σενάριο κινδύνου απορρήτου που προσδιορίζεται σε ένα μητρώο κινδύνου. Κάθε κίνδυνος στο μητρώο θα πρέπει να περιλαμβάνει μια αξιολογημένη αξιολόγηση κινδύνου από τη συνεκτίμηση της πιθανότητας παραβίασης του απορρήτου με τον αντίκτυπο στο απόρρητο του χρήστη. Ένα παράδειγμα μητρώου κινδύνου εφαρμογής απεικονίζεται στο Σχήμα 3.

**Εικόνα 23. Μητρώο κινδύνου**

| Risk ID | Risk Description | Likelihood | Impact | Risk Rating | Risk Owner |
|---|---|---|---|---|---|
| R01 | The application's password reset process could be used to lock a user out of their account should their user account be compromised by a malicious third party | Low | Medium | Medium | Developer Lead |
| R02 | The application process which permits the manual edit of user details by administrators could result in the inaccurate personal data, given the process uses an account lookup by a user's their full name instead of unique record identifier such as user ID or email. This means an administrator could update the wrong record details | Medium | Medium | Medium | Developer Lead |
| R03 | A person under age of 16 (child) could put in a fake date of birth to create an account on the system | Low | Low | Low | Developer Lead |

Κίνδυνοι απορρήτου της εφαρμογής στη διευκόλυνση των δικαιωμάτων απορρήτου του GDPR στους χρήστες

Υπάρχει ένας αριθμός δικαιωμάτων απορρήτου των χρηστών του GDPR που επηρεάζουν τις εφαρμογές, αυτά τα δικαιώματα εξηγούνται στο πρώτο μέρος αυτής της σειράς καθοδήγησης. Με την υποστήριξη του αρχιτέκτονα εφαρμογών, ελέγξτε την τεκμηρίωση σχεδιασμού της εφαρμογής και αξιολογήστε πώς η εφαρμογή διευκολύνει ή όχι καθένα από τα ισχύοντα δικαιώματα απορρήτου των χρηστών του GDPR, τα οποία περιλαμβάνουν:

Δικαίωμα ενημέρωσης (άρθρο 12)

Δικαίωμα πρόσβασης (άρθρο 15)

Δικαίωμα διαγραφής (άρθρο 17)

Το δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18)

Το δικαίωμα στη φορητότητα δεδομένων (άρθρο 20)

Δικαίωμα αντίρρησης (άρθρο 21)

Το δικαίωμα να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της δημιουργίας προφίλ (άρθρο 22)

Τεκμηριώστε τις διαδικασίες αίτησης που διευκολύνουν επαρκώς καθένα από τα δικαιώματα απορρήτου του GDPR εντός της τεκμηρίωσης DPIA. Όπου οποιοδήποτε από τα ισχύοντα δικαιώματα απορρήτου GDPR δεν διευκολύνεται επαρκώς από την εφαρμογή, τεκμηριώστε τα ως κινδύνους απορρήτου στο μητρώο κινδύνων.

Κίνδυνοι απορρήτου οργανισμού

Οργανισμοί που έχουν το ρόλο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία που δεν συμμορφώνονται με τον GDPR, κινδυνεύουν με σημαντικές κυρώσεις που περιλαμβάνουν μεγάλα πρόστιμα από τις εποπτικές αρχές, νομικές αξιώσεις για ζημίες από χρήστες, απαγορεύσεις επεξεργασίας προσωπικών δεδομένων και ζημιές στη φήμη. Οι κίνδυνοι απορρήτου του οργανισμού θα πρέπει να αξιολογούνται με την υποστήριξη του ΥΠΔ και επίσης να καταγράφονται στο μητρώο κινδύνων. Όταν ο οργανισμός ανάπτυξης λογισμικού σκοπεύει να αναλάβει το ρόλο του ελεγκτή, δηλαδή να παρέχει την εφαρμογή απευθείας στους χρήστες, θα πρέπει να λαμβάνονται υπόψη οι ακόλουθοι κίνδυνοι και οι πιθανές επιπτώσεις τους στον αναπτυσσόμενο οργανισμό:

Λήψη συναίνεσης χρήστη και ακρίβεια της δήλωσης απορρήτου

Αποφυγή συλλογής υπερβολικών προσωπικών δεδομένων

Παραβιάσεις προσωπικών δεδομένων, ακούσια ή κακόβουλη παραβίαση δεδομένων, συμπεριλαμβανομένων μαζικών παραβιάσεων προσωπικών δεδομένων

Διασφάλιση ότι τα προσωπικά δεδομένα παραμένουν ενημερωμένα και ακριβή

Αποτυχία παροχής δικαιωμάτων GDPR στους χρήστες της εφαρμογής, είτε εντός της εφαρμογής είτε απευθείας από τον οργανισμό ως υπεύθυνος επεξεργασίας

Η μη διαθεσιμότητα της εφαρμογής ή των προσωπικών δεδομένων, π.χ. διακοπές λειτουργίας συστήματος, ανάκτηση αντιγράφων ασφαλείας, κακόβουλες επιθέσεις άρνησης υπηρεσίας

Προσδιορισμός και αξιολόγηση λύσεων απορρήτου

Το επόμενο στάδιο είναι η αξιολόγηση κάθε κινδύνου απορρήτου που καταγράφεται στο μητρώο κινδύνων με σκοπό την αποδοχή, τη μείωση ή την εξάλειψη κάθε κινδύνου. Ο μετριασμός του κινδύνου απορρήτου μπορεί να επιτευχθεί με την επινόηση λύσεων και την πραγματοποίηση αλλαγών στο σχεδιασμό της εφαρμογής, την εφαρμογή βελτιώσεων στις διαδικασίες SDLC ή την εισαγωγή διαδικασιών και ελέγχων στον οργανισμό ελεγκτή. Ο αρχιτέκτονας εφαρμογών, ο τεχνικός επικεφαλής, ο Υπεύθυνος Ασφάλειας Πληροφοριών και ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων θα πρέπει όλοι να συμμετέχουν στον καθορισμό και την αξιολόγηση λύσεων μετριασμού του κινδύνου προστασίας της ιδιωτικής ζωής. Το τρίτο μέρος αυτής της σειράς καθοδήγησης επεξηγεί πολλές κοινές λύσεις μετριασμού του κινδύνου απορρήτου εφαρμογών, όπως κρυπτογράφηση βάσεων δεδομένων και ψευδωνυμοποίηση.

Τεκμηριώστε τα αποτελέσματα DPIA και υπογράψτε από τον ΥΠΔ

Οι κίνδυνοι απορρήτου στο μητρώο κινδύνων θα πρέπει να ενημερωθούν για να αντικατοπτρίζουν τυχόν αλλαγές μετριασμού του κινδύνου που έγιναν στο σχεδιασμό της εφαρμογής και να περιλαμβάνουν μια αξιολόγηση υπολειπόμενου κινδύνου, η οποία είναι η αξιολόγηση κινδύνου μετά την αλλαγή. Βεβαιωθείτε ότι όλες οι αλλαγές και οι λύσεις μετριασμού του κινδύνου απορρήτου έχουν ενσωματωθεί στον σχεδιασμό και το σχέδιο έργου της εφαρμογής. Ο διαχειριστής του έργου ανάπτυξης θα πρέπει να ενημερώνεται για τα αποτελέσματα της DPIA, ώστε να διασφαλίζεται ότι οι ενέργειες μετριασμού του κινδύνου περιλαμβάνονται επίσημα στο σχέδιο ανάπτυξης. Η συμπληρωμένη τεκμηρίωση DPIA θα πρέπει να περιλαμβάνει:

Μια επισκόπηση της εφαρμογής, συμπεριλαμβανομένων του σκοπού και των λειτουργιών της

Η ευθύνη GDPR του οργανισμού ανάπτυξης εφαρμογών π.χ. υπεύθυνος επεξεργασίας, επεξεργαστής ή κανένας από τους δύο

Διάγραμμα ροής δεδομένων προσωπικών δεδομένων

Στοιχεία τεχνικών προσωπικών δεδομένων π.χ. υπολογιστικό φύλλο

Περιγραφή των διαδικασιών για τα δικαιώματα απορρήτου των χρηστών GDPR της εφαρμογής

Αντίγραφο της δήλωσης απορρήτου της εφαρμογής

Ολοκληρωμένο μητρώο κινδύνων που περιλαμβάνει κινδύνους απορρήτου χρήστη και οργανισμού της εφαρμογής

Σελίδα δήλωσης αποσύνδεσης DPO

Ο ΥΠΔ πρέπει να επανεξετάσει την ολοκληρωμένη τεκμηρίωση DPIA, εάν το DPIA θεωρείται ακριβής αναπαράσταση και ο κίνδυνος απορρήτου θεωρείται αποδεκτός, και η εφαρμογή και ο οργανισμός, κατά περίπτωση, ως υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία, συμμορφώνονται πλήρως με τον GDPR , ο ΥΠΔ θα πρέπει να υπογράψει το DPIA. Διαφορετικά, ο ΥΠΔ θα πρέπει να αναφέρει τυχόν ζητήματα και να ζητήσει περαιτέρω αξιολόγηση. Στους χορηγούς του αναπτυξιακού έργου θα πρέπει να παρέχεται αντίγραφο του ολοκληρωμένου DPIA. Καθώς οι χορηγοί έργων είναι συνήθως υπεύθυνοι για τον συνολικό κίνδυνο απορρήτου της αναπτυγμένης εφαρμογής, συνιστάται επίσης να υπογράψουν το DPIA.

Εφαρμογή λύσεων απορρήτου DPIA εντός του σχεδίου ανάπτυξης

Στους χορηγούς του αναπτυξιακού έργου θα πρέπει να παρέχεται αντίγραφο του ολοκληρωμένου DPIA. Καθώς οι χορηγοί έργων είναι συνήθως υπεύθυνοι για τον συνολικό κίνδυνο απορρήτου της αναπτυγμένης εφαρμογής, συνιστάται επίσης να υπογράψουν το DPIA.

Οδηγίες εφαρμογής εφαρμογής

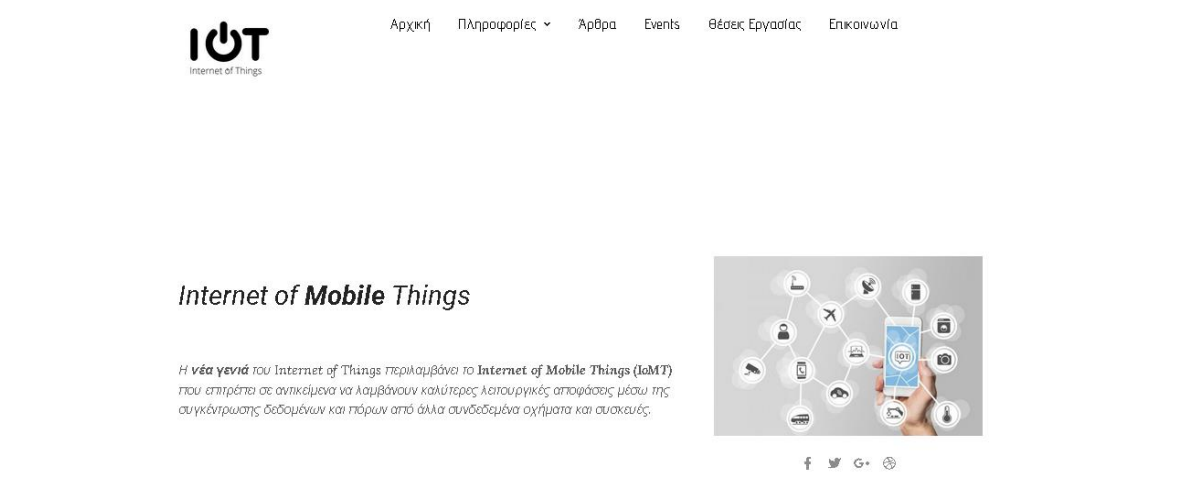
Όπου οι εφαρμογές προορίζονται να μεταπωληθούν, να φιλοξενηθούν ή να χρησιμοποιηθούν από εξωτερικούς οργανισμούς ελεγκτών, οι προγραμματιστές θα πρέπει να γράφουν και να παρέχουν οδηγίες υλοποίησης εφαρμογών, για να βοηθήσουν τους οργανισμούς ελεγκτών να παρέχουν την εφαρμογή για την προστασία του απορρήτου των χρηστών όπως έχει σχεδιαστεί και από προεπιλογή. Η καθοδήγηση υλοποίησης θα πρέπει να περιλαμβάνει συνοπτικές οδηγίες βήμα προς βήμα σχετικά με την εγκατάσταση και τη διαμόρφωση των ρυθμίσεων απορρήτου της εφαρμογής. Η καθοδήγηση θα πρέπει επίσης να προτείνει τη διαμόρφωση ασφαλείας των υποστηρικτικών στοιχείων της εφαρμογής, όπως οι διακομιστές ιστού, οι βάσεις δεδομένων και το περιβάλλον δικτύου. Για την παροχή πρόσθετης διαφάνειας και υποστήριξης GDPR στους οργανισμούς ελεγκτών, η καθοδήγηση εφαρμογής θα πρέπει να περιλαμβάνει πλήρη επεξήγηση όλων των λειτουργιών και διαδικασιών εφαρμογής που σχετίζονται με το απόρρητο. Η καθοδήγηση θα πρέπει επίσης να αναφέρει πού αναμένεται να είναι υπεύθυνος ο οργανισμός επεξεργασίας για την παροχή τυχόν δικαιωμάτων απορρήτου χρήστη GDPR που δεν διευκολύνονται από την εφαρμογή, καθώς και για τις ευθύνες του οργανισμού ελεγκτή για τον μετριασμό του κινδύνου απορρήτου της εφαρμογής. Αυτές οι πληροφορίες θα έχουν ήδη ληφθεί και περιλαμβάνονται στην τεκμηρίωση της DPIA.

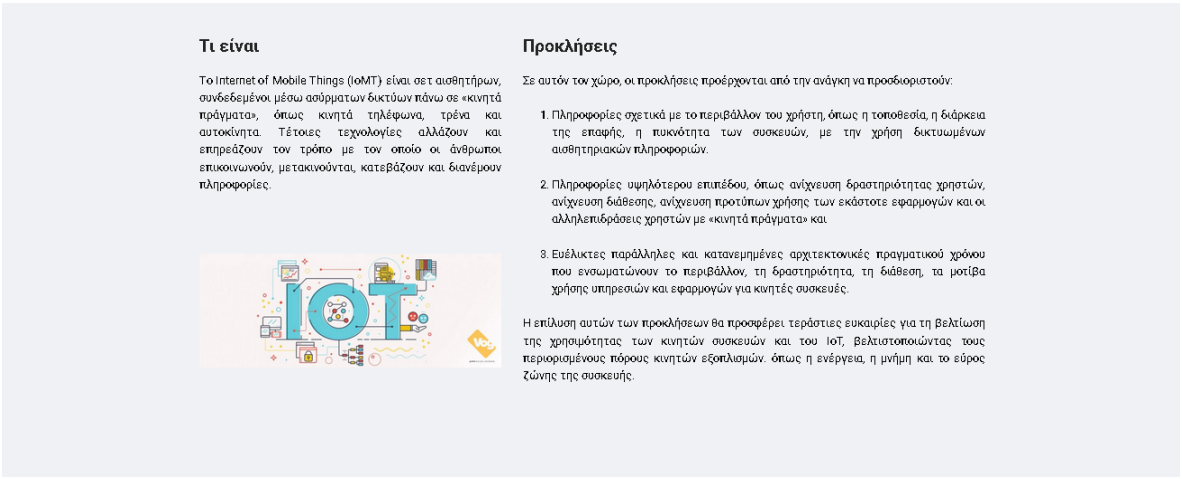
Συμπέρασμα

Το άρθρο 35 του ΓΚΠΔ απαιτεί τη διενέργεια αξιολόγησης επιπτώσεων στην προστασία δεδομένων (DPIA) όπου οι «νέες τεχνολογίες» είναι πιθανό να οδηγήσουν σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες της ιδιωτικής ζωής των ατόμων. Αυτή η απαίτηση μπορεί να ερμηνευθεί ότι ισχύει για την ανάπτυξη οποιασδήποτε εφαρμογής που σκοπεύει να επεξεργαστεί προσωπικά δεδομένα πολιτών της ΕΕ. Η ολοκλήρωση μιας επίσημης DPIA νωρίς στον κύκλο ζωής ανάπτυξης λογισμικού είναι μια ουσιαστική πρακτική για την αποτελεσματική ανάπτυξη εφαρμογών που προστατεύουν τα δικαιώματα απορρήτου των χρηστών από την αρχή. Οι προγραμματιστές θα πρέπει να αναζητούν υποστήριξη από ειδικούς σε θέματα απορρήτου δεδομένων, επαγγέλματα ασφάλειας πληροφοριών και διαχείρισης κινδύνου

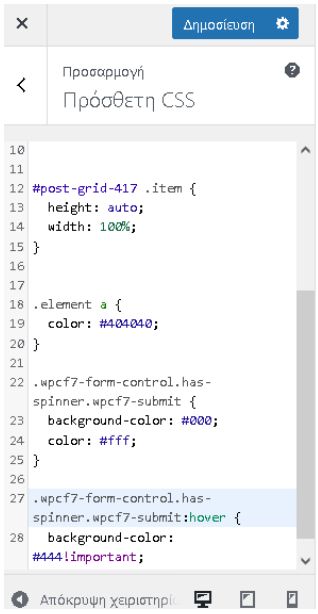
Στις σελίδες που είναι παιδιά του «Πληροφορίες» δημιουργήθηκε διάταξη με δύο στήλες και προστέθηκαν τα κείμενα, υπερσύνδεσμοι και το απαραίτητο πολυμεσικό υλικό (φωτογραφίες, βίντεο, slideshow, gallery κ.ά.).

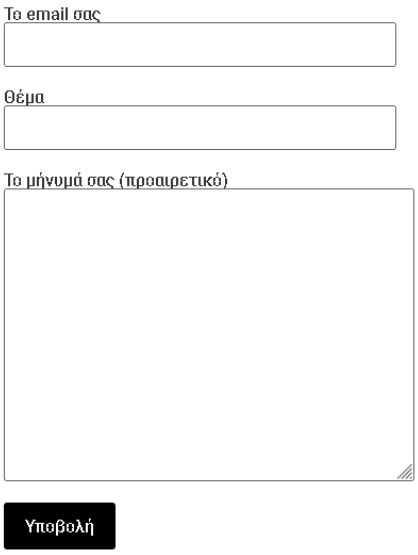
**Εικόνα 24. Πρωιμη μορφή**



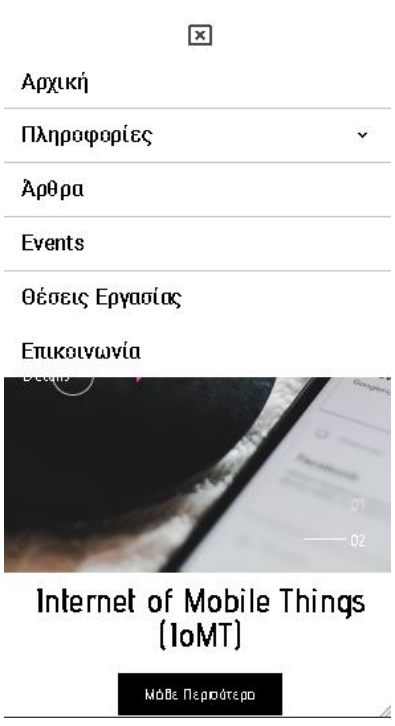

Η επιλογή «Πρόσθετη CSS» από το μενού “Προσαρμογή” του Wordpress φάνηκε εξαιρετικά χρήσιμη για περιπτώσεις που δεν υπήρχε δυνατότητα απευθείας επεξεργασίας των στοιχείων μέσω του Elementor.

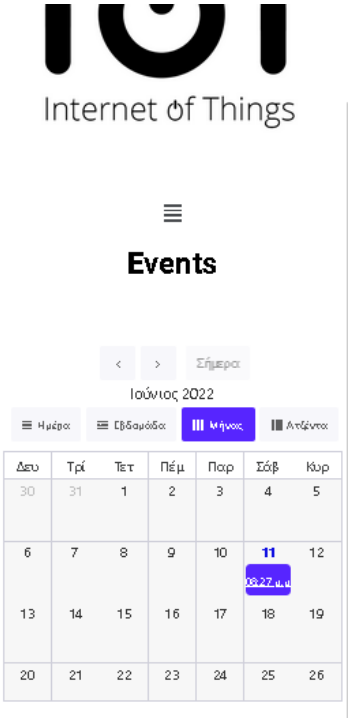


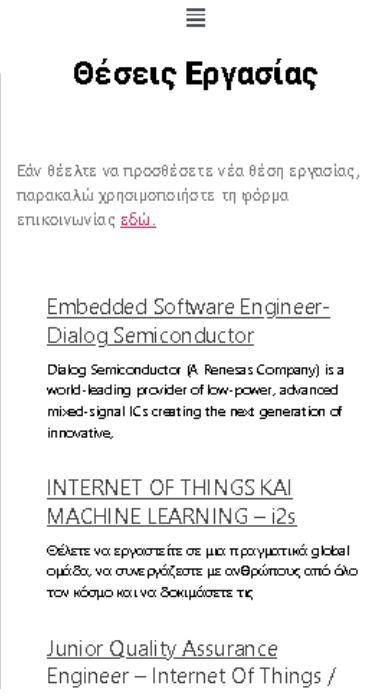




Έπιπρόσθετα σίγουρα θα εμφανιστέι η ανάγκη για είσοδο μέσω κινητής συσκευής.

Παρακάτω μπορούμε να δούμε μερικές εικόνες προβολής σε έξθπνο τηλεφωνο.



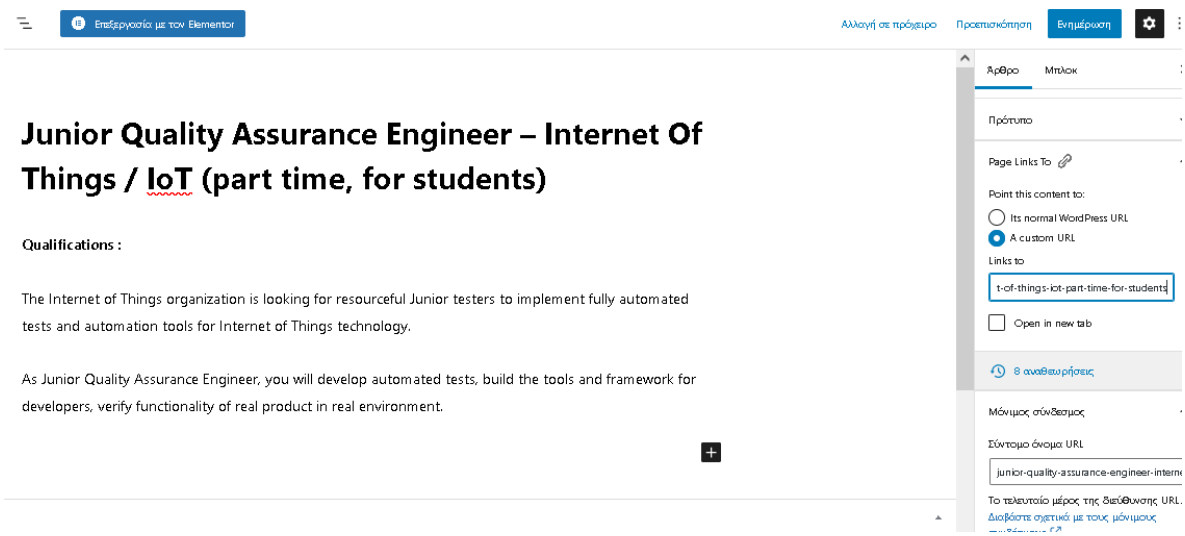



## 2.6 Πρόσθετες δυνατότητες.

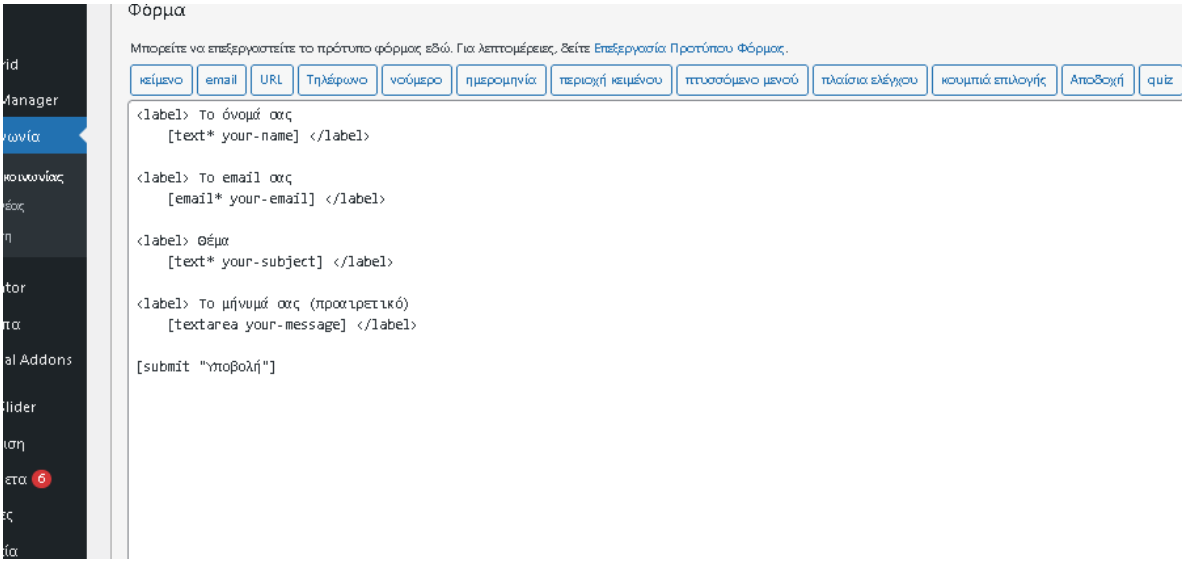
Όπως αναφέρθηκε παραπάνω, κατά τη σχεδίαση, για τη δημιουργία slide εγκαταστάθηκε το πρόσθετο «Prime Slider». Επίσης, για τα άρθρα εγκαταστάθηκε το πρόσθετο «Page Links To» ώστε να μπορούμε εκτός από δικά μας άρθρα να βάζουμε κα άρθρα από εξωτερικές πηγές που ο υπερσύνδεσμος θα οδηγεί σε διαφορετικούς ιστοτόπους. Αυτό χρησιμοποιήθηκε κυρίως στην περίπτωση των άρθρων της κατηγορίας «Θέσεις εργασίας».Εδώ ο χρήστης πλέον μπορεί να δεί τον τίτλο σχετικά με την εργασία που προσφέρεται και αν ενδιαφέρεται και θέλει να μαθει περισσοτερα μπορει να πατήσει πανω στον Τίτλο και να μεταφερθεί στην σελίδα όπου έχει αναρτηθεί η αγγελία.

Εικόνα 25. Θέσεις εργασίας



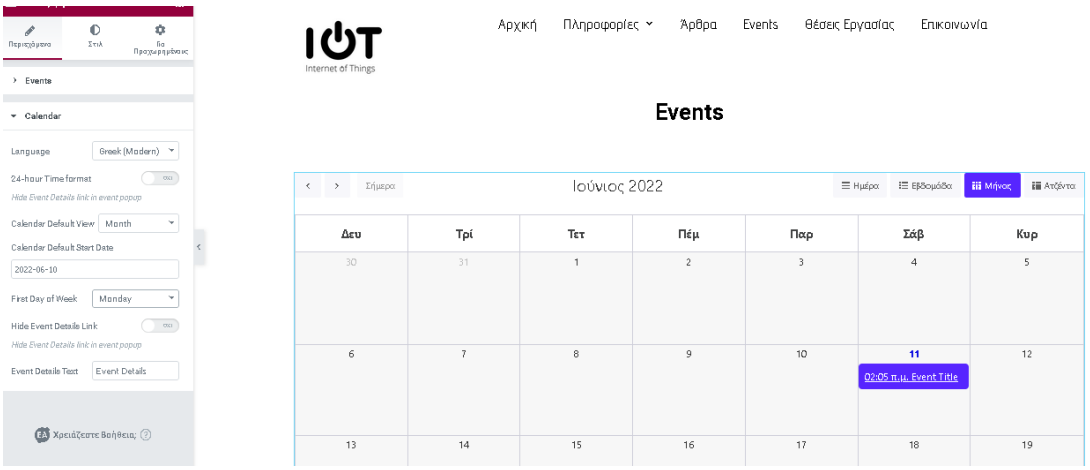

Για την προσθήκη φόρμας γρήγορης επικοινωνίας εγκαταστάθηκε το πρόσθετο Contact Form 7 το οποίο μας δίνει έτοιμα templates για την δημιουργία και διαχείρηση μυνημάτων απο τους χρήστες που θέλουν να επικοινωνήσουν με το διαχειριστικό.

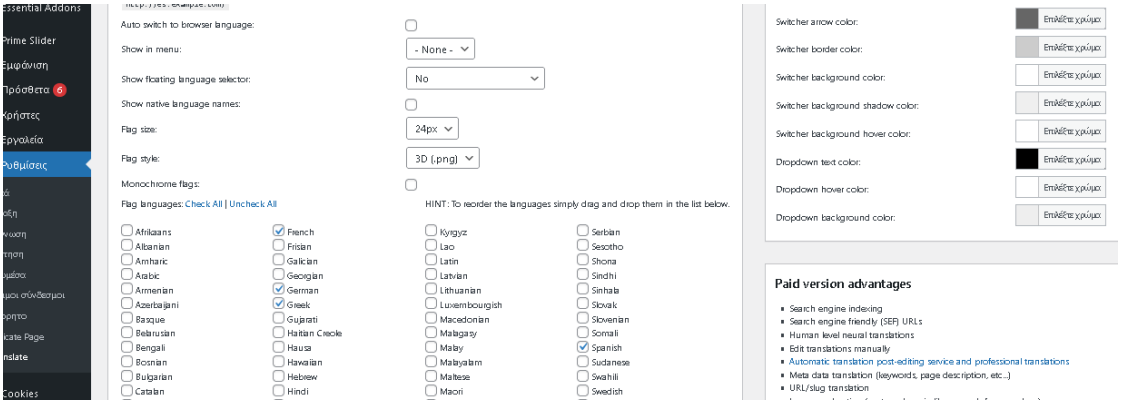
Εικόνα 26 Φόρμα επικοινωνίας




Για τη δημιουργία και διαχείριση του προγράμματος με τα events, εγκαταστάθηκε το πρόσθετο “WP Event Manager», προστέθηκαν κάποια events και χρησιμοποιήθηκε το shortcode [events per_page="18"].Απο το παρακάτω διαχειριστικό έχουμε την δυνατότητα να προσθέσουμε και να διαχειριστούμε επερχόμενα events όπως και να ανακατευθήνουμε τον χρήστη στην σελίδα που φιλοξενεί το event.

Εικόνα 27. Events

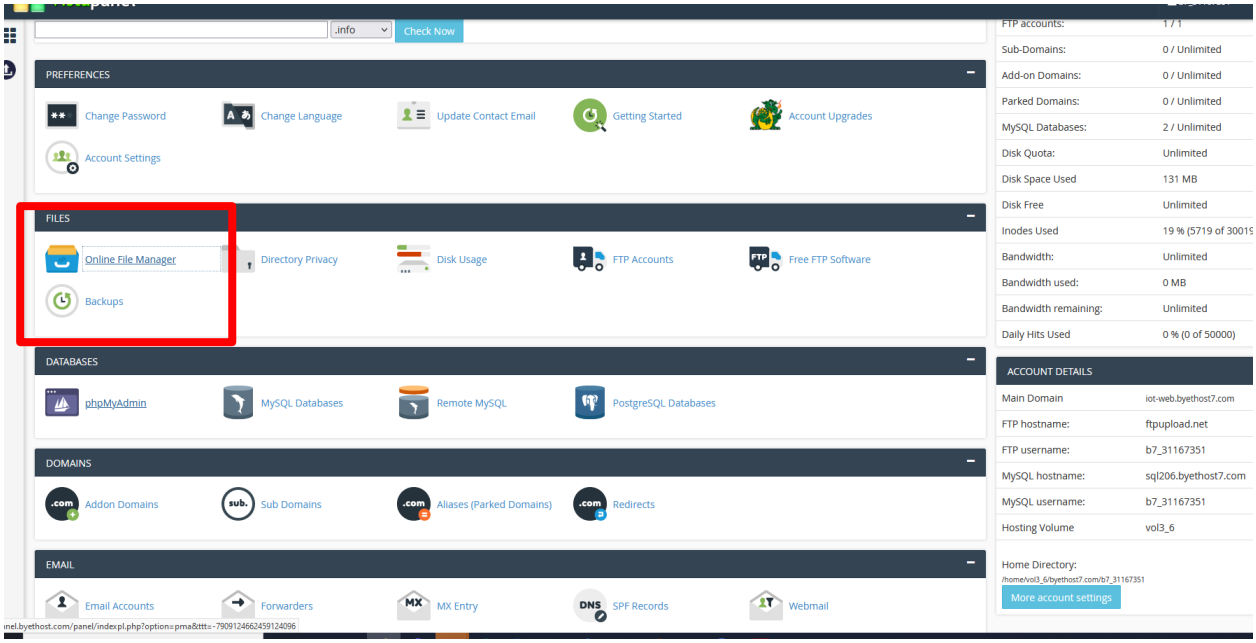



Essential Addons
Prime Slider
Εμφάνιση
Πρόσθετα 6
Χρήστες
Εργαλεία
Ρυθμίσεις
Cookies
Auto switch to browser language:
Show in menu:
- None -
Show floating language selector:
No
Show native language names:
Flag size:
24px
Flag style:
3D (.png)
Monochrome flags:
Flag languages: Check All | Uncheck All
HINT: To reorder the languages simply drag and drop them in the list below.
Afrikaans
Albanian
Amharic
Arabic
Armenian
Azerbaijani
Basque
Belarusian
Bengali
Bosnian
Bulgarian
Catalan
French
Frisian
Galician
Georgian
German
Greek
Gujarati
Haitian Creole
Hausa
Hawaiian
Hebrew
Hindi
Kyrgyz
Lao
Latin
Latvian
Lithuanian
Luxembourgish
Macedonian
Malagasy
Malay
Malayalam
Maltese
Maori
Serbian
Sesotho
Shona
Sindhi
Sinhala
Slovak
Slovenian
Somali
Spanish
Sudanese
Swahili
Swedish
Switcher arrow color:
Switcher border color:
Switcher background color:
Switcher background shadow color:
Switcher background hover color:
Dropdown text color:
Dropdown hover color:
Dropdown background color:
Επιλέξτε χρώμα
Paid version advantages
Search engine indexing
Search engine friendly (SEF) URLs
Human level neural translations
Edit translations manually
Automatic translation post-editing service and professional translations
Meta data translation (keywords, page description, etc...)
URL/slug translation

## 2.7 Βάση δεδομένων.

Μέσα από το διαχειριστικό του host (Α. ΣΥΝΔΕΣΗ ΣΤΟ CONTROL PANEL ΤΟΥ HOST) μπορούμε να χρησιμοποιήσουμε το πρόγραμμα phpMyAdmin για να συνδεθούμε απευθείας στη βάση και να έχουμε γραφικό περιβάλλον χρήστη το οποίο μπορει να μας βοηθήσει να έχουμε μια πιο ολοκληρωμένη και κατανοητή εικόνα της βάσης.

**Εικόνα 28. Σύνδεση στην online βάση**

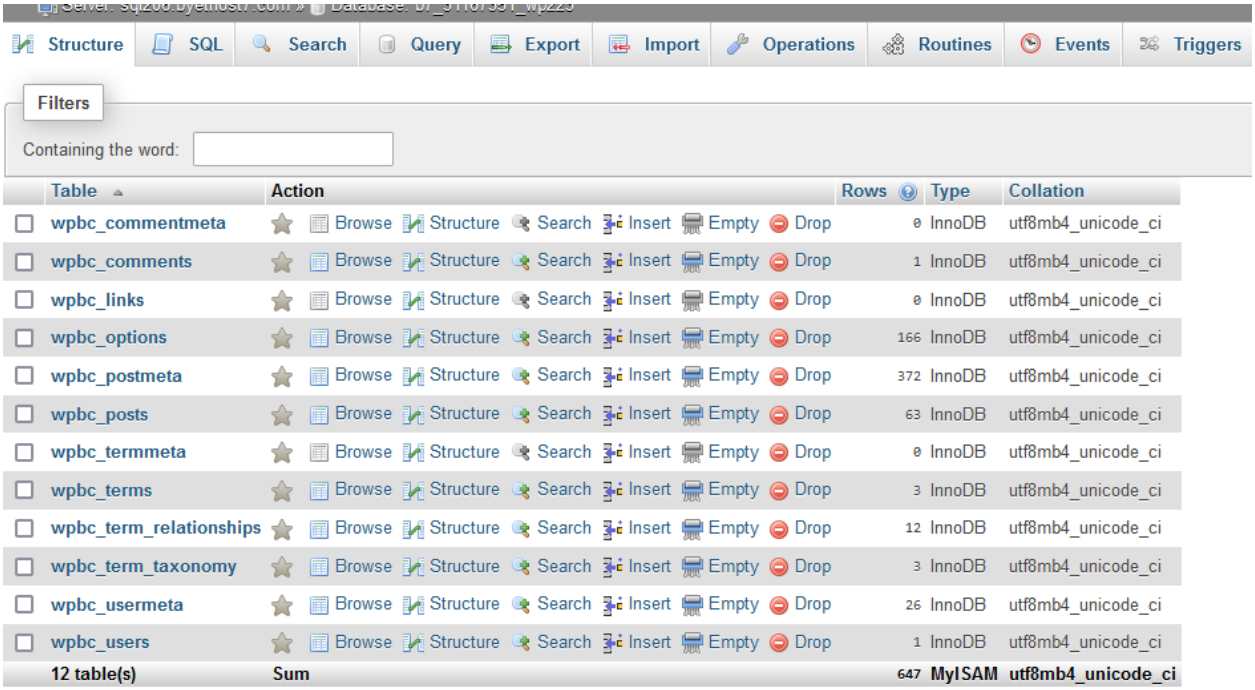



Υπάρχουν δύο βάσεις στον πίνακα ελέγχου, αλλά η μία (iotwp) είναι άδεια και όπως φαίνεται και στο wp-config, το wordpress συνδέεται με την wp223 οποου και αποθηκεύονται
Πατάμε connect now για να ανοιξει το phpMyAdmin.

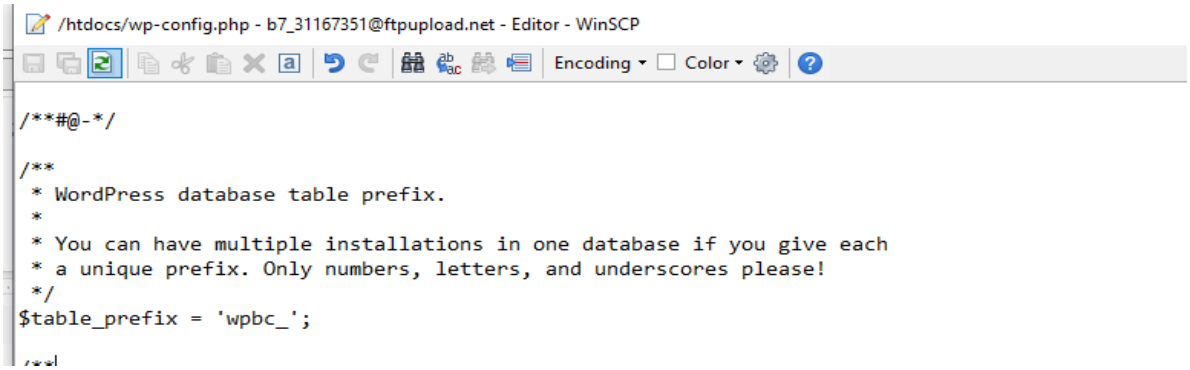



Παρακάτω φαίνονται τα tables που έχει δημιουργήσει το wordpress κατά την εγκατάσταση

Εικόνα 29. Πίνακες Wp



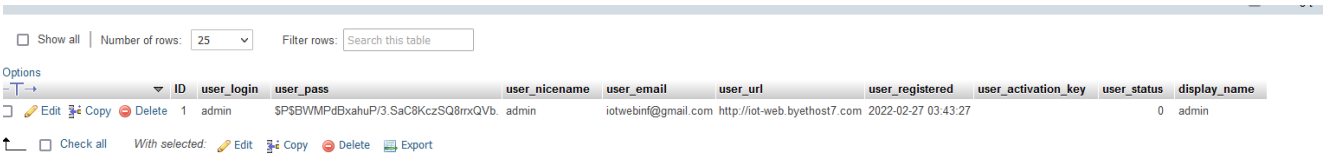

Το πρόθεμα wpbc_ πριν από κάθε table καθορίστηκε κατά την εγκατάσταση και αποθηκεύεται στο wp_config.php:




Μπορούμε να έχουμε πολλές διαφορετικές εγκαταστάσεις του wordpress στην ίδια βάση, με διαφορετικό πρόθεμα. Το ποια εγκατάσταση/δεδομένα θα βλέπει κάθε φορά το Wordpress καθορίζεται από το wp_config.php.

Στο **wpbc_options** κρατάει τις βασικές πληροφορίες για τον ιστότοπο, όπως ο τίτλος, η διεύθυνση κ.ά.

Στο **wpbc_users** αποθηκεύονται οι χρήστες και οι κωδικοί τους όπως φαίνεται παρακάτω και στο **wpbc_usermeta** τα δικαιώματα κάθε χρήστη με βάση το id του




Όπως φαίνεται παραπάνω, ο κωδικός του admin στο **wpbc_users** δεν εμφανίζεται ως απλό κείμενο αλλά είναι κρυπτογραφημένος (το wordpress χρησιμοποιεί δικό του salted hash algorithm, συνδυασμό MD5 και PHPass, για να αποθηκεύει τους κωδικούς). Τα salts καθορίζονται κατά την εγκατάσταση στο αρχείο wp-config.php και μπορούν να αλλαχθούν.

/htdocs/wp-config.php - b7_31167351@ftpupload.net - Editor - WinSCP

Encoding Color

```
/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication unique keys and salts.
 *
 * Change these to different unique phrases! You can generate these using
 * the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}.
 *
 * You can change these at any point in time to invalidate all existing cookies.
 * This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY',         'xnnon20cthydqustik6fey66bjlogssm1renp9vy15olqd1pcg8fmihe5ppjjk1f' );
define( 'SECURE_AUTH_KEY',  'r9vo0qed9saokb5a1elj6uv8qhjyw3261vumg7lxnewons63eynarculqgcnav1t' );
define( 'LOGGED_IN_KEY',    'u0ngakkheebd4laww1iyeb2bpkdwht5vcicox5iezviqduoxlufk9wdgzkyrizwc' );
define( 'NONCE_KEY',        's4pwtbf1ibfneqrhzzj47alr0jv3swewh8r4j7qlygxsazhb9cbm8prglpusdwpe' );
define( 'AUTH_SALT',        '1euyi3m6jkpfgr5zvwajezrhfzhq05muepkw5u667zj5wnep1lvzmicojogiqd1t' );
define( 'SECURE_AUTH_SALT', 'lbz3kjlhmynkkrbdtdfsashoqecb64xh3ezthdm5jaebnzdbytvtwyhypkmyyztb' );
define( 'LOGGED_IN_SALT',   'z8hmrbdi1wgupl7gkq6rfya4s4pnbigsr4aovj61olipqcuri4xkm61ng1pbuc32' );
define( 'NONCE_SALT',       'dk0mm4xw5vatbd4614jip7b6glbvtniax0pzizzxqacs7rkdhwdjww8da7gmteb8' );

/**#@-*/

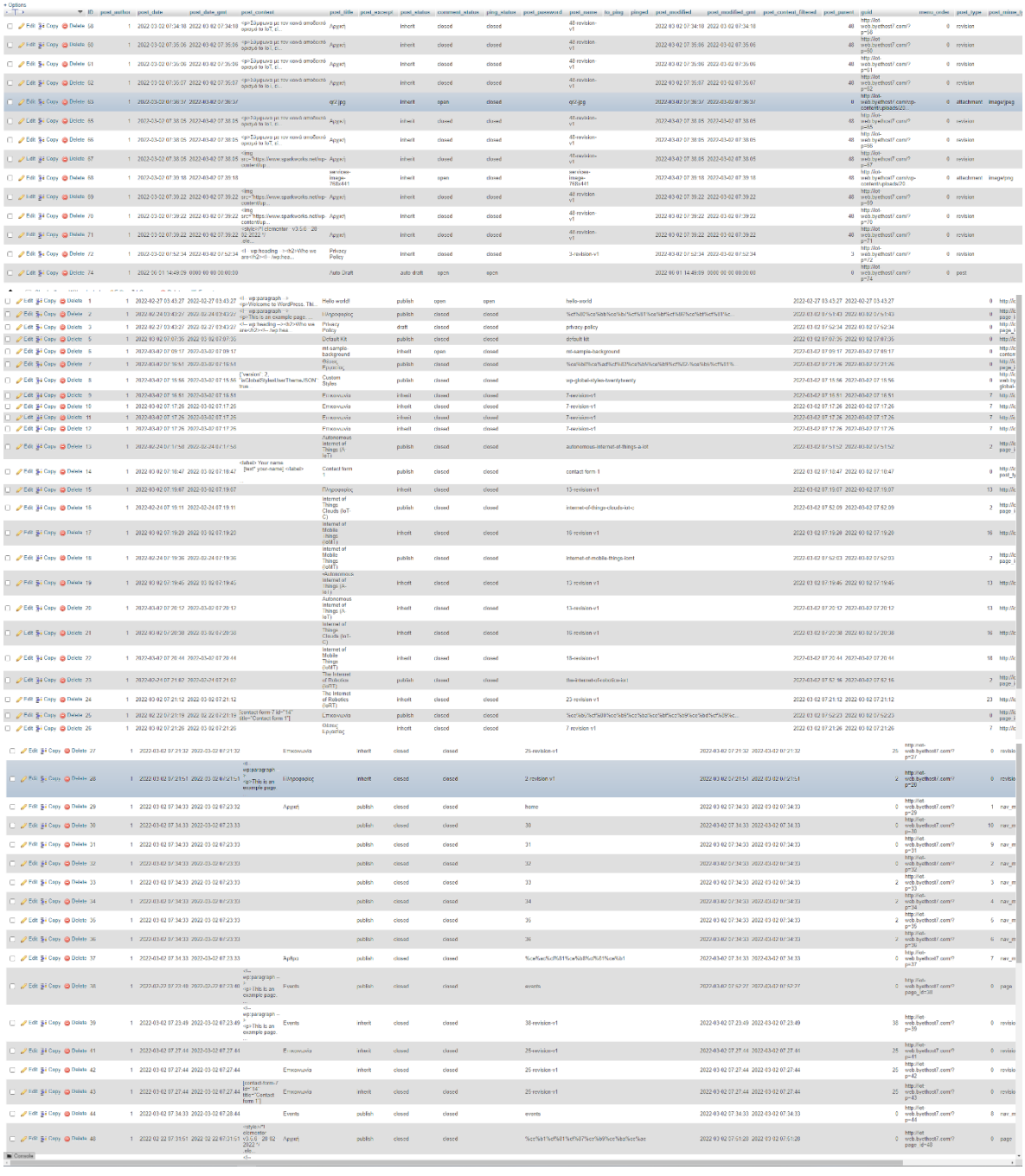
/**
 * WordPress database table prefix.
 *
```

**Σημείωση:** salt είναι ένας τυχαίος αριθμός ή συμβολοσειρά με την οποία «μπλέκουμε» τον κωδικό κατά την κρυπτογράφηση έτσι ώστε να είναι πιο δύσκολο να αναστραφεί/αποκρυπτογραφηθεί)

Όσον αφόρα την βάση δεδομένων ,την περισσότερη δουλεία την έχει κάνει ήδη το WP γύρω απο

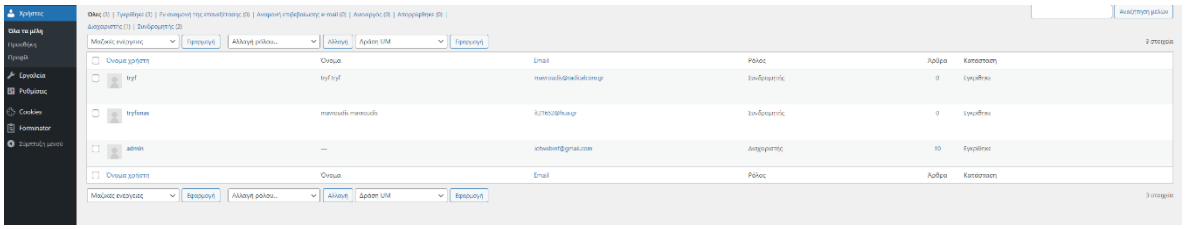
την δημιουργία tables. Μας δίνει φυσικά την δυνατότητα να είμαστε ευελικτοι και να δημιουργησοθμε ή να τροποποιήσουμε οποία tables θεωρουμε αναγκαία μεσώ του phpMyAdmin.

Αυτό που έχει περισσότερτη σημασία να δούμε είναι τα **wpbc_posts** όπου και αποθηκευονται τα posts με ολα τους τα στοιχεία και την κατάσταση τους (published , comment section open-closed κ.α)



Αξίζει να σημειωθει οτι οι χρήστες του WP με τους χρηστες του site δεν μοιράζονται την ίδια βάση.

Αν θέλουμε να δούμε στοιχεία απο το site μπορούμε πολυ ευκολα να μπούμε απο το διαχειριστικό και στην επιλογή Χρήστες να δούμε ολα τα στοιχεία που χρειαζόμαστε αλλα και να τα επεξεργαστούμε.



# 3 Αξιολόγηση.

Στο σημείο αυτό κρίθηκε κατάλληλο να εκθέσουμε το παραπάνω site στον απλο μεν αλλα εξοικειωμένο χρήστη με τις υπηρεσίες που πρέπει να διέπουν ενα Portal.

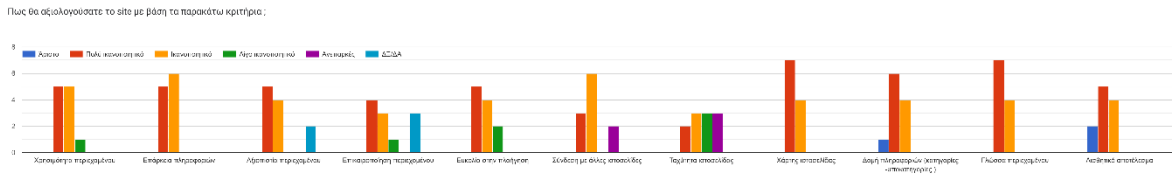
Το link μοιράστηκε σε μέλη μιας διαφημιστικής Εταιρείας (Radical Communications A.E) και σε μέλη ενος απο τους μεγαλύτερους εισαγωγείς ποτών στην Ελλάδα(Τμήμα Marketing Καρούλιας Ε.Ε).Το κοινό που μοιράστηκε αποτελείται απο 35% άντρες και 65% γυναίκες.Οι συμμετέχοντες κατα μέσο όρο έχουν τα 42 έτη ηλικίας ενώ ο μικρότερος είναι 27ετών, ο μεγαλύτερος είναι 64.Το 100% έχει πτυχίο τουλάχιστον τριτοβάθμιας εκπαίδευσης και επίσης έχουν ενα αρκετά υψηλό επίπεδο γνώσεων όσον αφορά το IoT και τις υπηρεσίες που προσφέρει.

Αφου δόθηκε αρκετός χρόνος να περιεργαστούν και να εξοικειωθούν με το site δημιουργήθηκε και μοιράστηκε το παρακάτω ερωτηματολόγιο.

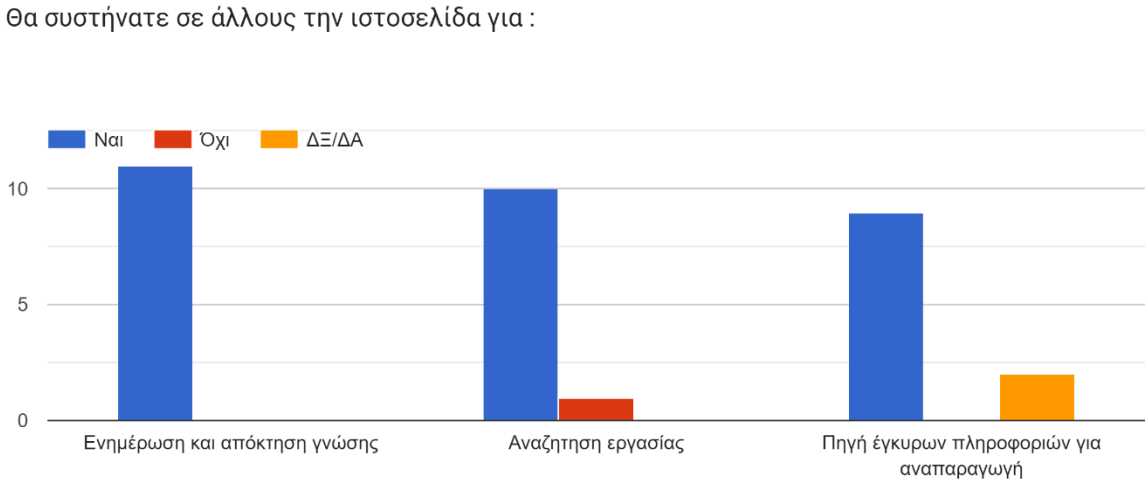
1. Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Χρησιμότητα περιεχομένου ]
2. Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Επάρκεια πληροφοριών ]
3. Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Αξιοπιστία περιεχομένου ]
4. *Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Επικαιροποίηση περιεχομένου ]*
5. *Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Ευκολία στην πλοήγηση ]*
6. *Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Σύνδεση με άλλες ιστοσελίδες ]*
7. *Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Ταχύτητα ιστοσελίδας ]*
8. *Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Χάρτης ιστοσελίδας ]*
9. *Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Δομή πληροφοριών (κατηγορίες - υποκατηγορίες )]*
10. *Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Γλώσσα περιεχομένου ]*
11. *Πως θα αξιολογούσατε το site με βάση τα παρακάτω κριτήρια ; [Αισθητικό αποτέλεσμα ]*

12. *Τι επιπλέον υλικό θα θέλατε να διαθέτει η ιστοσελίδα ;*
13. *Ποιες αλλαγές θα προτείνατε για την βελτίωση της ιστοσελίδας ;*
14. *Θα συστήνατε σε άλλους την ιστοσελίδα για : [Ενημέρωση και απόκτηση γνώσης ]*
15. *Θα συστήνατε σε άλλους την ιστοσελίδα για : [Αναζητηση εργασίας ]*
16. *Θα συστήνατε σε άλλους την ιστοσελίδα για : [Πηγή έγκυρων πληροφοριών για αναπαραγωγή ]*

Αφου συλλέξαμε τα δεδομένα είχαμε τα παρακάτω αποτελέσματα:




**Εικόνα 30. Πρώτο μέρος αποτελεσμάτων ερωτηματολογίου**




**Εικόνα 31. Δεύτερο μέρος ερωτηματολογίου**

Η πλειοψηφία των αποτελεσμάτων ηταν θετική περα απο μερικά αναμενόμενα σχόλια για την ταχύτητα του site.Αυτο το περιμέναμε καθώς το site το κάνουμε Host σε δωρεάν πάροχο και δεσμεθόμαστε απο την επεξεργαστική σύναμη που μας παρέχουν.

Σε άλλα σχόλια είχαμε παρατηρήσεις σχετικά με την πολυπλοκότητα του site.

Επίσης σημειώθηκε οτι θα ηταν πολύ χρήσιμο ο κάθε χρήστης να μπορεί να αλληλεπιδρά ξεχωριστά με το site και να μην έρχεται σε επαφή μόνο με τους διαχειριστές μεσα απο την σελίδα της επικοινωνίας αλλά με άλλους χρήστες οπουθ και θα μπορούν να αλλαζουν απόψεις και να μοιράζονται απορίες.

Τέλος υπήρξαν προτάσεις για την βελτίωση της εικόνας του site όπως προσθήκη επεξειγητικών video και περισότερων οπτικών μέσων.

## 3.1 Βελτίωση.

Έχοντας κατα νου τις παρατηρήσεις των χρηστών αποφασίστηκε να γίνουν οι παρακάτω αλλαγές στο site.

Ξεκινώντας έπειτα απο ερευνα του καταλληλου plug in αποφασίσαμε να προχωρήσουμε με το Ultimate Member για την διαχείριση των χρηστών και στην συνέχεια με το WpForo για την δημιουργία και την διαχείρηση ενος Forum.

Έχει λοιπόν προστεθεί  δυνατότητα εγγραφής και σύνδεσης χρήστη.Οι εγγεγραμένοι χρήστες  έχουν παραπάνω προνόμοια στο Portal.Όπως θα δούμε παρακάτω οι χρήστες έχουν πρόσβαση πλέον σε ένα Forum στο οποίο μπορούν να δημιουργήσουν νεές ενότητες και να συζητήσουν για θέματα γύρω απο το IoT που τους ενδιαφέρουν.Επιπρόσθετα έχουν την δυνατότητα να επεξεργαστούν πλήρως το profile του μέσα απο την ενότητα Λογαριασμός όπως φαίνεται στο παρακάτω διάγραμμα.’Εκει μπορούν να βρούν ολη την δραστηριότητα τους όπως σχόλια και δημοσιεύσεις που έχουν κάνει αλλα και να ειδοποιηθούν για τυχόν νέα threads ή απαντήσεις.

Όσον αφορά τις παρατηρήσεις για την ταχύτητα θα μπορούσε να λυθεί απλα με μια premium συνδρομή στην ίδια πλατφόρμα.

Τέλος δεν κρίθηκε απαραίτητο να γίνει κάποια αλλαγή γύρω  απο την δομή του site καθως η πολυπλοκότητα του είναι σε αρκετά χαμηλο επίπεδο οπως φαίνεται στο παραπάνω διάγραμμα.

## 4.Συμπερασματα Περιορισμοί και Επόμενα βήματα

Στην πορεία δημιουργιας του παραπάνω Portal συναντήσαμε διάφορες δυσκολίες και περιορισμούς, μερικα προσπεράστηκαν, αλλα τα παρακάμψαμε και μερικά λόγω χρόνου παρέμειναν ως έχουν.Το πρώτο πρόβλημα ηταν η ευελιξία που θα θελαμε να έχουμε κατα την δίαρκεια του project και το να δουλεύουμε σε local host ήταν πολυ σεσμευτικό για το προγραμμα μας.Η λύση δόθηκε με την μεταφορά του site στον online πάροχο Byethost ο οποίος μας δίνει την δυνατότητα να δουλεψουμε απο διαφορετικά stations.Ένα αλλο πρόβλημα ήταν ο περιορισμένος χρόνος που είχαμε να δουλέψουμε πανω σε ένα τέτοιο site.Καθώς ειναι ενα ερευνιτικό θέμα , οι πληροφορίες που θα προστεθουν θα πρεπει να ειναι οσο το δυνατον περισσοτερο επαληθευμενες απο εγκυρες πηγες ώστε να έχουμε ενα ολοκληρομένο αποτέλεσμα.Επίσης ενα θέμα το οποίο σημειώθηκε και απο τους χρήστες στους οπόιους μοιράσαμε το ερωτηματολόγιο είναι η ελλειψη περισσοτερον διαδραστηκών μέσων όπως βίντεο να δυνοδέυουν τα κείμενα και να συμπληρώνουν πληροφορίες για το θέμα στο οποίο αναφέρονται.Ενα εμπόδιο το οποιο δεν ξεπεράστηκε ειναι η ταχύτητα φορτωσης του site.Αυτό ειναι ενα πρόβλημα το οποίο εμφανίστηκε μετρα την μεταφορά του site σε online πάροχο.Βέβαι ειναι κατανοήτο καθως έχουμε διαθέσιμες μονο της δωρεαν παροχές που προσφέρει το παραπάνω site και η λυση είναι με μια συνδρομή να το αναβαθμίσουμε σε premium ετσι ωστε να εποφεληθουμε απο μεγαλύτερες ταχύτητες και περισσοτερες λειτουργίες οσον αφορά την αποθήκευση και άλλες δυνατότητες που προσφέρει μια τέτοια συνδρομή.

Το site έχει δημιουργηθεί με τετοιον τρόπο έτσι ωστε να μπορεί να προσαρμοστεί και να εξελιχθεί αναλόγως τον διαχειριστή που το έχει υπο ελεγχο.Παραπάνω μπορούμε να βρουμε όλες τις πληροφορίες που θα χρειαστεί καποιος για να διαχειρηστει το παραπάνω portal απο την συνδεση , την τροποποιηση ακομη και την ολική αλλαγή του περιεχομένου και διαχειρησης του site.Αν υπηρχε παραπάνω χρονος μερικα απο τα βηματα που θα περναμε για την περεταίρο βελτίωση του site θα ηταν τα παρακάτω.

Αναβάθμιση της συνδρομής του Host σε Premium.Οπως αναφέρθηκε και παραπάνω με αυτην την κίνηση θα λύναμε το πρόβλημα της ταχύτητας το οποίο προς το παρόν ειναι το μεγαλύτερο μειωνεκτημα του site αλλα επισης θα μας έδινε προσβαση με μεγαλύτερο αποθηκευτικό χώρο οσο αναφορά την διαχείρηση χρηστών και την προσθήκη περιεχομένου.Το οποίο μας παει στο επόμενο βημα.

Προσθηκη οπτικοακουστικών μεσων σε συνοδεία τον κειμένων.Οι πιθανότητες κάποιος χρήστης να παρακολουθήσει ενα βίντεο ή να διαβασει ενα κειμενο που αναφερονται στο ιδιο θεμα τείνουν προς την μερία του βίντεο.Οπότε μια πολυ καλη προσθηκη για το site θα ηταν η προσθήκη βίντεο αναφορικα με το θεμα που αναφερετε στο κείμενο ωστε να δωσει μια πιο ολοκληρωμενη εικονα στον χρηστη για το τι διαβάζει.

Επίσης μια πολυ καλή προσθήκη θα ηταν ενα FQAs (Frequently Asked Questions) στην αρχίκη οπου και θα προσθέταμε τι πιο συχνα εμφανιζόμενες ερωτήσεις και τι απαντήσεις τους μαζι με εναν υπερσύνδεσμο ετσι ωστε να του καθηδηγούμε σε μια σελίδα αφιερωμένη σε αυτό.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


| **Έγγραφο στο Διαδίκτυο** | 2014-2022 . Ανακτήθηκε από: |
|---|---|
| | • **https://www.dataversity.net/internet-things-iot/**<br>• **https://www.darpa.mil/about-us/timeline/arpanet**<br>• **https://www.dataversity.net/data-management-internet-things/**<br>• **https://www.dataversity.net/big-data-use-cases-developing-smarter-world/**<br>• **https://developer.ibm.com/articles/s-gdpr2/**<br>• **https://eur-lex.europa.eu/eli/reg/2016/679/oj**<br>• **https://eur-lex.europa.eu/eli/reg/2016/679/oj**<br>• **https://developer.ibm.com/articles/iot-vs-edge-computing/**<br>• **https://www.cisco.com/c/en/us/solutions/%20collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html**<br>• **https://gdpr.eu/**<br>• **https://developer.ibm.com/articles/%20%ce%a4%ce%bf%20s-gdpr3/** |