ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ	ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ	ΤΜΗΜΑ ΝΟΜΙΚΗΣ
ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ	

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΣΥΓΧΡΟΝΟ ΤΕΧΝΟΛΟΓΙΚΟ ΠΕΡΙΒΑΛΛΟΝ

Διπλωματική Εργασία του Βάιου Ντόκα

Η εργασία αντιμετωπίζει:

Το πρόβλημα

- Η προστασία των προσωπικών δεδομένων λόγω της αυξανόμενης χρήσης νέων τεχνολογιών ανάλυσης και επεξεργασίας δεδομένων
- Δυσκολίες της νομοθεσίας να προσαρμοστεί στις νέες και συνεχώς εξελισσόμενες τεχνολογίες

Αντιμετώπιση μέσω της χρήσης

- Καινοτόμων τεχνολογιών όπως η χρησιμοποίηση των δικτύων του **blockchain**
- Σύγχρονων τεχνικών **ανωνυμοποίησης** και **κρυπτογράφησης**

Η παρούσα εργασία περιλαμβάνει:

Στοιχεία

- Μελέτη του διεθνούς και ελληνικού **νομοθετικού πλαισίου** προστασίας των προσωπικών δεδομένων
- Ανάλυση των **διεθνών κανόνων** ασφαλούς επεξεργασίας και **διαβίβασης** δεδομένων
- Ανάλυση **εννοιών της ασφάλειας πληροφοριών** όσον αφορά πληροφοριακά συστήματα
- Αναζήτηση τρόπων ενίσχυσης του ασφαλούς **σχεδιασμού πληροφοριακών συστημάτων**, πολιτικών χρήσης και ασφαλών εφαρμογών
- Ανάλυση **τεχνικών μέτρων** που προάγουν την ασφάλεια, την διαφάνεια και την ανωνυμία
- Ανάλυση και προοπτικές χρήσης **σύγχρονων τεχνικών κρυπτογράφησης**, της τεχνολογίας **blockchain** και των **έξυπνων συμβολαίων** ως τεχνικών για την διασφάλιση των αρχών της ακεραιότητας και της διαφάνειας.

ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Κύριες διεθνείς πράξεις

- Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα (ΟΔΔΑ)
- Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (ICCPR)
- Κατευθυντήριες Αρχές του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ)

ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Θεμελιώδες Ευρωπαϊκό Δίκαιο

- Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ)
- Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
- Επικαιροποιημένη Σύμβαση 108 του Συμβουλίου της Ευρώπης

ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Ευρωπαϊκό Δίκαιο για την προστασία των προσωπικών δεδομένων

- Γενικός Κανονισμός για την Προστασία Δεδομένων (2016/679)
- Οδηγία 2016/680 (Αστυνομική Οδηγία)
- Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (2002/58/ΕΚ) +

ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Ευρωπαϊκό Δίκαιο για την προστασία των προσωπικών δεδομένων

- Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών στην ΕΕ
- Ειδικές Νομοθετικές πράξεις (ανά τομέα)

ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Προστασία από το Εθνικό δίκαιο (πέραν του Γενικού Κανονισμού Προσωπικών Δεδομένων)

- Συνταγματική Προστασία
- Ο Νόμος 2472/97
- Ο Νόμος 4624/2019

ΚΑΝΟΝΕΣ ΑΣΦΑΛΟΥΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

4.

- Υποχρέωση διασφάλισης ασφαλούς επεξεργασίας
- Τρόποι διασφάλισης ασφάλειας δεδομένων
- Εμπιστευτικότητα - Ακεραιότητα

ΚΑΝΟΝΕΣ ΑΣΦΑΛΟΥΣ ΕΠΕΞΕΡΓΑΣΙΑΣ
Υποχρέωση διασφάλισης ασφαλούς επεξεργασίας

Το άρθρο 32 του ΓΔΚΠ:

Ορίζει τις υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντα την επεξεργασία για ασφαλή επεξεργασία.

Το αναγκαίο επίπεδο ασφαλείας καθορίζεται:

(1) τις τελευταίες εξελίξεις

(2) το κόστος εφαρμογής των διαδικασιών

(3) την φύση και τον σκοπό της επεξεργασίας

(4) τους κινδύνους της επεξεργασίας

Κρίσιμα στοιχεία:

Οι υπεύθυνοι επεξεργασίας έχουν γενική υποχρέωση διαφάνειας και λογοδοσίας, ιδίως όταν εμφανίζονται παραβιάσεις δεδομένων.

Προβλέπεται έλεγχος των δεδομένων από το υποκείμενο και επεξεργασία μόνο στον βαθμό που είναι αναγκαία και ανάλογη για την επίτευξη του σκοπού και διασφάλιση της ασφάλειας του ΥΕ.

Απαγόρευση χρήσης τεχνικών «κατάρτισης προφίλ» με αυστηρούς όρους εξαίρεσης, όπως λχ. όταν υπάρχει ρητή πρόβλεψη απ' το δίκαιο της ΕΕ.

ΚΑΝΟΝΕΣ ΑΣΦΑΛΟΥΣ ΕΠΕΞΕΡΓΑΣΙΑΣ
Τρόποι διασφάλισης ασφάλειας δεδομένων

Βάσει του άρθρου 32§1 του ΓΔΚΠ:

Τα τεχνικά και οργανωτικά μέτρα περιλαμβάνουν μεταξύ άλλων:

- Ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων
- Διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων ελέγχου
- Διαδικασίες εκτίμησης της αποτελεσματικότητας των μέτρων
- Χρήση εγκεκριμένου κώδικα δεοντολογίας κ.α.

Βάσει διεθνών προτύπων:

Μέσω της χρήσης de jure ή de facto προτύπων.

Μέσω αναλύσεων και συμβουλών για τις τρέχουσες απειλές ασφάλειας, που δημοσιεύει ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

ΚΑΝΟΝΕΣ ΑΣΦΑΛΟΥΣ ΕΠΕΞΕΡΓΑΣΙΑΣ
Υποχρεώσεις γνωστοποίησης παραβίασης δεδομένων

Παραβίαση δεδομένων υπάρχει σε κάθε περίπτωση απώλειας εμπιστευτικότητας.

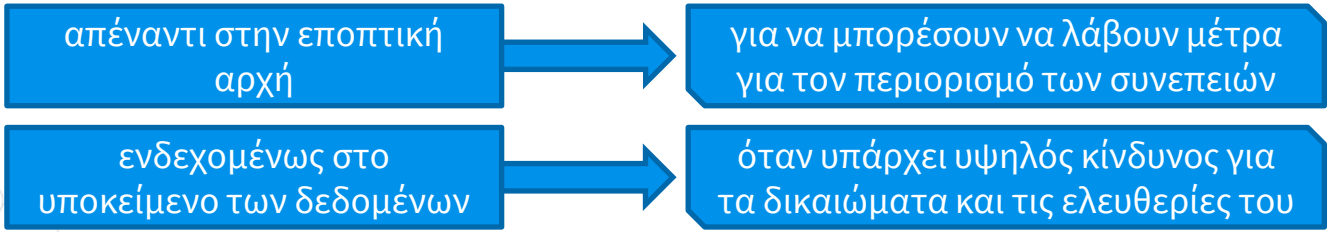
Η ΟΕ του άρθρου 29 είχε κρίνει ότι υπάρχουν τριών ειδών επιπτώσεις στα δεδομένα προσωπικού χαρακτήρα:

η κοινοποίηση, η απώλεια και η μεταβολή.

Η υποχρέωση υπάρχει για τους υπευθύνους επεξεργασίας και τους εκτελούντες.

Παράλληλα με την ανάγκη λήψης μέτρων, υπάρχει η υποχρέωση καταγραφής στην συμμόρφωση κάθε οργανισμού του περιστατικού ασφαλείας.

Η υποχρέωση αναφοράς υπάρχει:



ΚΑΝΟΝΕΣ ΑΣΦΑΛΟΥΣ ΕΠΕΞΕΡΓΑΣΙΑΣ
Υποχρεώσεις γνωστοποίησης παραβίασης δεδομένων

Υψηλός κίνδυνος παραβίασης δεδομένων, θεωρείται ότι υφίσταται, όταν η παραβίαση ενδέχεται να οδηγήσει σε σωματική, υλική ή ηθική βλάβη για τα πρόσωπα, τα δεδομένων των οποίων έχουν παραβιαστεί.

Τα κριτήρια αξιολόγησης, μπορεί να είναι:

Το **είδος της παραβίασης**, η **φύση**, η ευαισθησία και ο **όγκος των δεδομένων** προσωπικού χαρακτήρα, η **ευκολία ταυτοποίησης** των προσώπων, η **σοβαρότητα των συνεπειών** κ.α.

ΚΑΝΟΝΕΣ ΑΣΦΑΛΟΥΣ ΕΠΕΞΕΡΓΑΣΙΑΣ
Υποχρεώσεις γνωστοποίησης παραβίασης δεδομένων

Η ανωνυμοποίηση ως λόγος εξαίρεσης:

Η ανωνυμοποίηση των δεδομένων μπορεί να αποτελέσει λόγο εξαίρεσης από την υποχρέωση γνωστοποίησης στο υποκείμενο.

Στον **Κανονισμό 611/2013**, ορίζεται ότι πρέπει να λαμβάνονται μέτρα που καθιστούν τα δεδομένα «μη κατανοητά», τέτοια μπορεί να είναι όταν τα δεδομένα:

1. έχουν κρυπτογραφηθεί.
2. έχουν αντικατασταθεί από την τιμή κατακερματισμού τους.

Το **Άρθρο 34 ΓΚΠΔ**, ορίζει ότι η ανακοίνωση δεν απαιτείται στο υποκείμενο αν:

(1) ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας και τα δεδομένα είναι ανωνυμοποιημένα ή

(2) έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος ή

(3) προϋποθέτει δυσανάλογες προσπάθειες

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

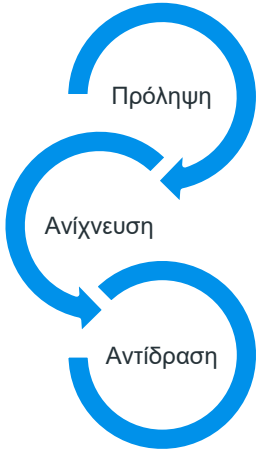
5.

- Ασφάλεια Πληροφοριών
- Διαφάνεια
- Σχεδιασμός ασφαλών πολιτικών
- Ασφαλής σχεδιασμός ΠΣ

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Ασφάλεια πληροφοριών

Η Ασφάλεια πληροφοριών έχει ως σκοπό την προστασία των πληροφοριακών συστημάτων από πιθανές επιπτώσεις στην εμπιστευτικότητα και την ακεραιότητά τους, αλλά και την εξασφάλιση της διαθεσιμότητάς τους προς τους εξουσιοδοτημένους χρήστες.

Η λήψη των κατάλληλων μέτρων προστασίας μπορεί να αφορά μια ή περισσότερες από τις ακόλουθες τρεις φάσεις των περιστατικών ασφαλείας:



Αφορά την προστασία των ακόλουθων τριών θεμελιωδών ιδιοτήτων των δεδομένων:

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Ασφάλεια πληροφοριών

Πλήγμα σε οποιοδήποτε από τα ανωτέρω, από τυχαία ή εσκεμμένη ενέργεια, συνιστά γενικά, περιστατικό ασφάλειας.

Η χρησιμοποίηση νέων τεχνολογιών (SaaS, Blockchain) μπορεί να προσφέρει περισσότερες δυνατότητες αλλά και να αυξήσει τα προβλήματα στην ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριακών αγαθών.

Η ασφάλεια των πληροφοριών συσχετίζεται με την επιτυχημένη εφαρμογή των ακόλουθων μηχανισμών:

Εξουσιοδότησης	*αφορά τη διαδικασία παρουσίασης της ταυτότητας μιας οντότητας στο σύστημα*
Αυθεντικοποίησης	*αφορά τη διαδικασία επιβεβαίωσης της ταυτότητας που έχει παρουσιάσει μια οντότητα στο σύστημα*
Αναγνώρισης	*αφορά τη διαδικασία λήψης απόφασης σχετικά με την αποδοχή ή την απόρριψη ενός αιτήματος πρόσβασης μιας αυθεντικοποιημένης οντότητας στο σύστημα*
Αδυναμία αποποίησης	*αφορά τη διαδικασία αδιαμφισβήτητου καταλογισμού ευθύνης για την επιτέλεση μιας ενέργειας στο σύστημα*

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Διαφάνεια

Η απεικόνιση ως μέσο διαφάνειας

Η απαίτηση για διαφάνεια επεξεργασίας είναι μέρος της γενικής απαίτησης για νομιμότητα και ορθότητα στην επεξεργασία και ενσωματώνεται στα άρθρα 12, 13, 14 και 34 του ΓΚΠΔ.

Αιτιολογική σκέψη 58:

Η αρχή της διαφάνειας απαιτεί «οποιαδήποτε ενημέρωση που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή.

Εκτίμηση αντίκτυπου (άρθρο 35 ΓΚΠΔ)

Η DPIA: είναι το βασικό εργαλείο με σκοπό να αξιολογηθεί εάν οι σχεδιαστικές επιλογές για ένα σύστημα ή μία διαδικασία, αντιστοιχούν στις απαιτήσεις για τη διασφάλιση της ιδιωτικότητας.

Είναι υποχρεωτική όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Σκοπός της είναι να διασφαλιστεί η συμμόρφωση με τις απαιτήσεις του Νόμου, αποτελώντας κομμάτι του συνολικού ασφαλούς σχεδιασμού

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Διαφάνεια

Πιστοποιήσεις ασφαλείας

Στο άρθρο 42 του ΓΚΠΔ υπάρχει παρότρυνση για «τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων».

Τα δύο πρότυπα TRUSTe και EuroPriSe παρέχουν στους υπευθύνους επεξεργασίας κανόνες και περιορισμούς για τη σωστή τήρηση των οποίων μπορούν να λάβουν σχετική πιστοποίηση για τον οργανισμό τους.

Privacy Shield και απόφαση C-311/18 του ΔΕΕ στην υπόθεση «Schrems II»

Αποτελούσε ένα μηχανισμό αυτοπιστοποίησης για εταιρείες που εδρεύουν στις ΗΠΑ.

Με την απόφαση C-311/18 του ΔΕΕ, καταργήθηκε το Privacy Shield.

Το ΕΣΠΔ διατήρησε σε ισχύ τις Τυποποιημένες Συμβατικές Ρήτρες (ΤΣΡ) και έκρινε ότι είναι επαρκείς, εφόσον τηρούνται συμπληρωματικά ορισμένα συμβατικά μέτρα, οργανωτικά και τεχνικά μέτρα.

Τον Ιανουάριο του 2021, εκδόθηκαν νέες ΤΣΡ από το ΕΣΠΔ (λαμβάνουν υπόψη την απόφαση).

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Σχεδιασμός πληροφοριακών συστημάτων

Το άρθρο 25 του ΓΚΠΔ

- Ορίζει ότι πρέπει να λαμβάνονται υπόψη οι τελευταίες εξελίξεις, όσον αφορά την λήψη τεχνικών και οργανωτικών μέτρων.
- Ενσωματώνει ουσιαστικά την απαίτηση για διενέργεια εκτίμησης αντικτύπου.

Ασφαλής Σχεδιασμός Πληροφοριακών Συστημάτων (Data protection by design)

Στα πλαίσια του άρθρου 25 παρ. 1 ΓΚΠΔ, ο υπεύθυνος επεξεργασίας πρέπει να ενσωματώνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα.

Κατάλληλα μέσα σημαίνει ότι τα μέτρα είναι και αποτελεσματικά για την επίτευξη του επιδιωκόμενου σκοπού.

Προστασία δεδομένων εξ ορισμού (Data protection by default)

Στόχος: Ο υπεύθυνος επεξεργασίας, θα πρέπει να σχεδιάσει το σκοπούμενο σύστημα με τρόπο ώστε να διενεργείται η κάθε επεξεργασία, μόνο όταν είναι απαραίτητη για την επίτευξη του επιδιωκόμενου σκοπού.

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Απαιτήσεις του ΓΚΠΔ για ασφαλή σχεδιασμό

Ο ΓΚΠΔ θέτει τα πλαίσια και απαιτεί την εφαρμογή των αρχών προστασίας των προσωπικών δεδομένων, καθ' όλο τον κύκλο ζωής των δεδομένων.

Απαιτείται:

Ασφάλεια κατά την συλλογή των δεδομένων

- Περιλαμβάνει τις υποχρεώσεις του ΥΕ για διαφάνεια όρων επεξεργασίας, ενημέρωση και λήψη συναίνεσης.

Ασφαλής διατήρηση και ορθότητα δεδομένων

- Τήρηση αρχής περιορισμού αποθήκευσης, ακρίβειας δεδομένων και ικανοποίησης των δικαιωμάτων της διαγραφής και της εναντίωσης.

Τήρηση αρχών κατά την επεξεργασία

- Κάθε επεξεργασία θα πρέπει να είναι αναγκαία και να στηρίζεται στην ορθή νομική βάση και να συνδέεται με σαφήνεια με τον επιδιωκόμενο σκοπό επεξεργασίας.
- Σημαντικό είναι να τηρούνται οι αρχές της αντικειμενικότητας και της ελαχιστοποίησης.

Ασφάλεια κατά την διαγραφή

- Περιλαμβάνει την εξασφάλιση της δυνατότητας άσκησης των δικαιωμάτων στη λήθη και στην φορητότητα.

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Απαιτήσεις του ΓΚΠΔ για ασφαλή σχεδιασμό

Ανασταλτικοί παράγοντας στην ενσωμάτωση του ασφαλούς σχεδιασμού

- Υψηλό κόστος ενσωμάτωσης νέων τεχνολογιών.
- Εξασφάλιση κερδοφορίας από διαφημίσεις τηρώντας την σχετική νομοθεσία.
- Δυσκολίες χρήσης των κρυπτογραφημένων δεδομένων και μειωμένη διαλειτουργικότητα.
- Παρατηρούμενη αύξηση δυνατότητας επαναταυτοποίησης ανωνυμοποιημένων δεδομένων.

Υπάρχει συνεπώς ανάγκη για:

- ενσωμάτωσης νομοθετικών εργαλείων που θα λαμβάνουν υπόψη τις τεχνικές προκλήσεις
- και εκπαίδευση των σχεδιαστών των εφαρμογών προστασίας στις νομικές απαιτήσεις.

ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΕΝΙΣΧΥΣΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

6.

- Τρόποι ενίσχυσης της ασφάλειας
- Κρυπτογραφία
- Μέτρα ενίσχυσης της ακεραιότητας, της αυθεντικότητας
- Η απόκρυψη της ταυτότητας

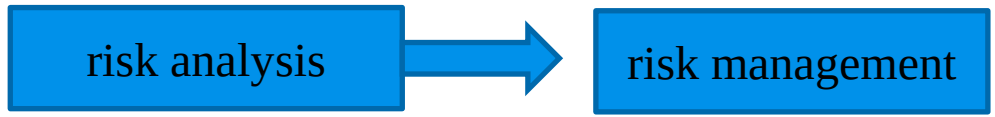
ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΕΝΙΣΧΥΣΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ
Ενίσχυση της ασφάλειας

Σκοπός της ενίσχυσης της ασφάλειας των πληροφοριακών συστημάτων, είναι η αποφυγή αδυναμιών, ο εντοπισμός απειλών, η πρόληψη ατυχημάτων και η μείωση του κινδύνου.

Η αναγνώριση των απειλών γίνεται με την ανάλυση επικινδυνότητας και η μελέτη για τη λήψη των μέτρων προστασίας με την διαχείριση επικινδυνότητας.

Για την πιστοποίηση της καταλληλότητας των μέτρων χρησιμοποιείται η σειρά προτύπων ISO/IEC 27000.

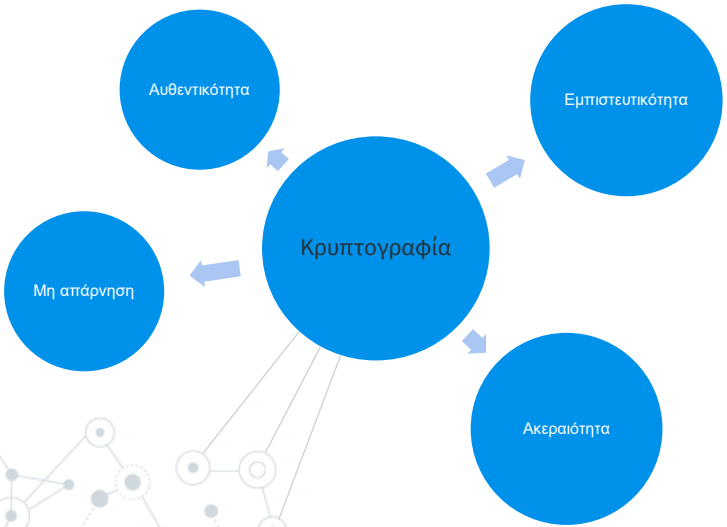
Η τήρηση των αρχών της εμπιστευτικότητας και της ακεραιότητας επιτυγχάνεται με τις «Privacy Enhancing Technologies» (PETs), που αποτελούν την βάση της ασφαλούς σχεδίασης.



ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΕΝΙΣΧΥΣΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ
Κρυπτογραφία

Σημαντικό εργαλείο ενίσχυσης της ασφάλειας είναι η κρυπτογραφία.

Η κρυπτογραφία έχει τέσσερις βασικούς αντικειμενικούς σκοπούς:



Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.

Ακεραιότητα: Η πληροφορία δεν μπορεί να αλλοιώνεται χωρίς να ακολουθεί ανίχνευση της αλλοίωσης.

Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να απαρνηθεί την αποστολή ή την παραλαβή της.

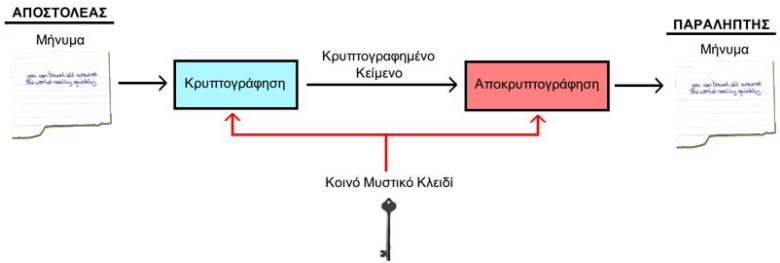
Αυθεντικότητα: Ο παραλήπτης μπορεί να εξακριβώνει την ταυτότητα του αποστολέα.

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Κρυπτογραφία

Συμμετρική κρυπτογραφία

Είναι η κλασσική μέθοδος κρυπτογραφίας.

Χρησιμοποιείται το ίδιο κλειδί στην κρυπτογράφηση και στην αποκρυπτογράφηση.



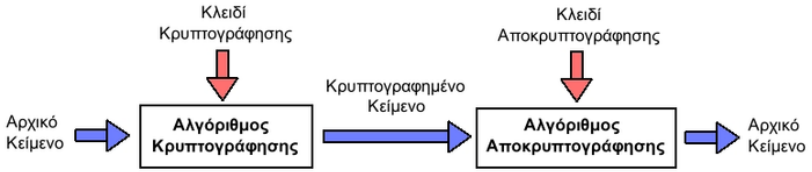
Κίνδυνος σε περίπτωση απώλειας του κλειδιού.

Σήμερα χρησιμοποιείται το Advanced Encryption Standard (AES).

Ασύμμετρη κρυπτογραφία

Χρησιμοποιείται διαφορετικό κλειδί για την κρυπτογράφηση και για την αποκρυπτογράφηση όμως του ίδιου ζεύγους.

Το δημόσιο (public) κλειδί που μπορεί να το δει οποιοσδήποτε και το ιδιωτικό (private) κλειδί το οποίο είναι απόρρητο.



Το μήνυμα στέλνεται κρυπτογραφημένο και το πραγματικό κλειδί που θα κάνει την αποκρυπτογράφηση δεν το γνωρίζει ούτε καν ο αποστολέας.

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Η απόκρυψη της ταυτότητας των υποκειμένων

Ψευδωνυμοποίηση

Σημαντικές αναφορές στον ΓΚΠΔ στα άρθρα 4 παρ.5, 32, 40, 89.

Με την ψευδωνυμοποίηση αντικαθίσταται η ταυτότητα δηλαδή του υποκειμένου των δικαιωμάτων, με τρόπο που να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώρισή του.

Ανωνυμοποίηση

Οριστική διαγραφή των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων.

Βάσει της αιτ. σκέψης (26), ο ΓΚΠΔ δεν εφαρμόζεται σε τέτοιου είδους ανωνυμοποιημένες πληροφορίες, αφού δεν μπορούν να συσχετιστούν με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα.

Δεν υπάρχει κάποιο ορισμένο στάνταρ από την Ευρωπαϊκή Νομοθεσία για το ποιο είναι το επιθυμητό επίπεδο, ώστε να εξασφαλίζεται ότι υπάρχει ανωνυμοποίηση.

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Τεχνικές ανωνυμοποίησης

Η Τυχαιοποίηση (Randomization)

Η τυχαιοποίηση είναι ένα σύνολο τεχνικών που χρησιμοποιούνται, για να αλλάξουν την εγκυρότητα των στοιχείων με σκοπό να μειώσουν την σύνδεση μεταξύ δεδομένων και υποκειμένου.

Λειτουργεί μέσω της προσθήκης θορύβου ή της τυχαίας μετάθεσης των δεδομένων σε σύνολα δεδομένων (datasets).

Η διαφοροποιημένη ιδιωτικότητα (Differential Privacy), είναι η πιο σύγχρονη μορφή της. Με αυτή, η πρόσβαση περιορίζεται στα απαραίτητα δεδομένα, ώστε να απαντηθεί συγκεκριμένο ερώτημα.

Η Γενίκευση γνωρισμάτων (Generalization)

Με αυτή μεταβάλλονται κατάλληλα οι τιμές των πεδίων που είναι ψευδοαναγνωριστικά, μέσω γενίκευσής τους (ομαδοποιούνται).

ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Τεχνικές ψευδωνυμοποίησης και προβλήματα χρήσης

Η Κρυπτογράφηση ως τεχνική ψευδωνυμοποίησης

Όταν τα δεδομένα είναι κρυπτογραφημένα, εφαρμόζεται ο ΓΚΠΔ, ενδεχομένως όμως δεν απαιτείται ενημέρωση του υποκειμένου.

Ολόκληρα τα δεδομένα καθίστανται «μη αναγνώσιμα». Μπορούν να χρησιμοποιηθούν όμως μέσω τεχνικών όπως της ομομορφικής κρυπτογράφησης (Homomorphic encryption).

Με αυτή, μπορούν εξουσιοδοτημένοι χρήστες να εκτελούν υπολογισμούς σε σύνολα δεδομένων, ενώ είναι ακόμα κρυπτογραφημένα, χωρίς δηλαδή να υπάρχει πρόσβαση στα προσωπικά δεδομένα που επεξεργάζονται.

Προβλήματα στην χρήση τεχνικών ανωνυμοποίησης

Είναι πάρα πολύ δύσκολο να εκμηδενιστεί η δυνατότητα ανακάλυψης της ταυτότητας των υποκειμένων.

Έρευνες δείχνουν ότι ακόμα και σε σύνολα δεδομένων, όπου έχουν εφαρμοστεί «βαριές» τεχνικές ανωνυμοποίησης, είναι σχεδόν αδύνατο να πληρούνται οι απαιτήσεις που έχει θέσει ο ΓΚΠΔ.

Κίνδυνοι δημιουργούνται επίσης από περιπτώσεις «κατάρτισης προφίλ» μετά από δημοσιοποίηση ανωνυμοποιημένων δεδομένων.

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN

7.

- Τεχνολογίες Blockchain
- Νομικές πτυχές της τεχνολογίας του Blockchain
- Νομοθετική αντιμετώπιση από Ευρώπη και Ελλάδα

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN
Τεχνολογίες Blockchain

Είναι ένας κατανεμημένος λογιστικός κατάλογος (distributed ledger), στον οποίο συναλλαγές ή δεδομένα συνδέονται μεταξύ τους σε μπλοκ δεδομένων, καθιστώντας τα πρακτικά αμετάβλητα.

Δημιουργεί την δυνατότητα κατανεμημένης μορφής εμπιστοσύνης, αντικαθιστώντας τις έμπιστες οντότητες.

Μπορεί να έχει ευρεία χρήση σε πολλούς κλάδους (ψηφιακά νομίσματα, IoT, πνευματικά δικαιώματα, έξυπνα συμβόλαια, logistics).

Κύρια χαρακτηριστικά:

- Διαφάνεια
- Καταμερισμός
- Αδυναμία μεταβολής

Κατηγοριοποιήσεις:

- Δημόσια δίκτυα blockchain (ελεύθερη πρόσβαση)
- Δίκτυα που απαιτούν άδεια από πρόσωπα που συμμετέχουν στην διαδικασία επικύρωσης, με πλήρη ή περιορισμένη πρόσβαση
- Ιδιωτικά δίκτυα, τα οποία βρίσκονται υπό τον έλεγχο ενός χρήστη ο οποίος αποκλειστικά διασφαλίζει τον έλεγχο της συμμετοχής και της επικύρωσης.

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN
Εφαρμογές της τεχνολογίας του blockchain

Κρυπτονομίσματα και bitcoin

Το bitcoin ήταν η πρώτη διαδεδομένη εφαρμογή της τεχνολογίας blockchain.

Η ασφάλειά του εξασφαλίζεται λόγω της συνέχειας των μπλοκ που το αποτελούν, καθώς η τροποποίηση έστω κι ενός ελάχιστου δεδομένου μίας συναλλαγής παράγει έναν τελείως διαφορετικό hash, γεγονός που θα δημιουργούσε ανακολουθία στην αλυσίδα των μπλοκ.

Έξυπνα συμβόλαια

Τα έξυπνα συμβόλαια μπορούν να περιγραφούν ως ένα σύνολο κωδικοποιημένων λειτουργιών που δεν προϋποθέτουν την ύπαρξη κάποιας αρχής, νομοθετικού πλαισίου ή τρόπους επιβολής των συμφωνηθέντων.

Μέσω της χρήσης της τεχνολογίας blockchain όχι μόνο καταργείται η ανάγκη για την ύπαρξη τρίτων μερών, αλλά εξασφαλίζεται ότι όλοι οι συμμετέχοντες γνωρίζουν τις λεπτομέρειες των συναλλαγών και ότι οι συμβατικοί όροι θα εκπληρώνονται αυτόματα όταν πληρωθούν ορισμένες προϋποθέσεις.

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN
Νομικές πτυχές της τεχνολογίας του Blockchain

Τα νομικά ζητήματα που μπορούν να προκύψουν από την χρήση της τεχνολογίας του blockchain αφορούν τα θέματα:

Της απαίτησης της χρήσης του ΓΚΠΔ όσον αφορά τεχνολογικές εφαρμογές βασισμένες σε blockchain, η οποία πρέπει να κρίνεται ανά περίπτωση.

Από άποψη εδαφικότητας, η επεξεργασία δεδομένων υποκειμένων κατοίκων της Ευρωπαϊκής Ένωσης είναι το κριτήριο για την εφαρμογή της Ευρωπαϊκής νομοθεσίας.

Θέμα μπορεί να προκύψει και στην αναζήτηση της αρμόδιας Αρχής Προστασίας Προσωπικών Δεδομένων της Ευρωπαϊκής Ένωσης.

Άλλα ζητήματα που μπορεί να προκύψουν είναι:

Η αναζήτηση του υπευθύνου επεξεργασίας και του εκτελούντα την επεξεργασία.

Προβλήματα σε θέματα άσκησης δικαιωμάτων των υποκειμένων, ιδίως της διαγραφής ή της ενημέρωσης.

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN
Προσωπικά δεδομένα στο blockchain

Πολλοί απ' τους τομείς που μπορεί να εφαρμοστεί η τεχνολογία του Blockchain, αφορούν την επεξεργασία προσωπικών δεδομένων, τόσο στο επίπεδο περιεχομένου όσο και στο επίπεδο των πληροφοριών που σχετίζονται με τους συμμετέχοντες.

Ένα Blockchain μπορεί να περιέχει δύο κατηγορίες δεδομένων προσωπικού χαρακτήρα:

- Στοιχεία για την ταυτοποίηση των συμμετεχόντων.
- Συμπληρωματικά δεδομένα, τα οποία εγγράφονται «μέσα» σε μία συναλλαγή.

Βάσει αυτής της κατηγοριοποίησης, εφαρμόζεται ο ΓΚΠΔ ενδεικτικά για την:

- Ταυτοποίηση του υπεύθυνου της επεξεργασίας.
- Τον σεβασμό δικαιωμάτων των υποκειμένων.
- Την εφαρμογή κατάλληλων εγγυήσεων.
- Τήρηση των υποχρεώσεων ασφάλειας.

CNIL:

Ο συμμετέχων σε κάθε δίκτυο Blockchain θα μπορούσε να θεωρηθεί ως ένας υπεύθυνος επεξεργασίας στο βαθμό που αποφασίζει για το σκοπό και τα μέσα της επεξεργασίας των δεδομένων, αλλά ορθό είναι να κρίνεται ανά περίπτωση.

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN
Ενίσχυση της αρχής της λογοδοσίας (accountability)

Η χρήση της τεχνολογίας του blockchain μπορεί να προσφέρει πρακτικές λύσεις σε θέματα επεξεργασίας προσωπικών δεδομένων.

Η αδυναμία μεταγενέστερης τροποποίησης του δημόσιου καταλόγου (ledger) δίνει την δυνατότητα δημιουργίας συστημάτων, τα οποία θα μπορούν να παρέχουν λύσεις στις υποχρεώσεις για την παροχή συγκατάθεσης με δυνατότητα ιχνηλασιμότητας.

Ένα σύστημα βασισμένο στο blockchain (όπως τα έξυπνα συμβόλαια), θα μπορούσε να προσφέρει τις δυνατότητες:

- Παρακολούθησης της πρόσβασης στα προσωπικά δεδομένα από τους υπευθύνους επεξεργασίας και τους εκτελούντες ώστε να επαληθεύεται ότι δεν παραβιάζεται η συναίνεση.
- Ελεύθερης και αποτελεσματικής ανάκλησης της συναίνεσης.
- Ενίσχυσης της λογοδοσίας μέσω της δυνατότητας ιχνηλασιμότητας των δεδομένων, χωρίς τον κίνδυνο περαιτέρω έκθεσης.
- Εύκολης απόδειξης της λήψης συναίνεσης από τους υπευθύνους επεξεργασίας.

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN
Νομικές πτυχές των έξυπνων συμβολαίων

Πλεονεκτήματα με την χρήση των έξυπνων συμβολαίων:

- Υπάρχει βεβαιότητα σχετικά με την ερμηνεία των όρων του συμβολαίου.
- Προστατεύει από μεταγενέστερη αλλαγή των όρων του συμβολαίου, αφού αποθηκεύονται μόνιμα στο blockchain.
- Προσφέρει την δυνατότητα διασύνδεσης με βάσεις δεδομένων για αυτόματη ενημέρωση του ισχύοντος νομοθετικού πλαισίου.

Μειονεκτήματα:

- Είναι δύσκολο να εντοπιστεί σε περίπτωση αμφιβολίας ο τόπος κατοικίας των μερών, ο τόπος κατάρτισης μίας σύμβασης και ο τόπος εκπλήρωσης άρα και το εφαρμοστέο δίκαιο.
- Οι αυστηροί όροι αυτόματης εκπλήρωσης των συνεπειών σε βάρος του μη συμμορφούμενου μέρους δεν συνάδουν με το δημόσιο χαρακτήρα των πράξεων εκτέλεσης.
- Στην πτώχευση, μπορεί να τεθούν θέματα νομιμότητας της εκτέλεσης, ιδίως αν προκύψει έπειτα λόγος αναστολής των πράξεων εκτέλεσης.

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN
Νομικές πτυχές κρυπτονομισμάτων

Δεν είναι νόμισμα με την κλασσική έννοια του όρου.

Πρόκειται για ένα νέο όρο που αναφέρεται σε μια μονάδα αξίας που εκδίδεται από μια ιδιωτική οντότητα.

Νομικά προσιδιάζει περισσότερο με ψηφιακά περιουσιακά στοιχεία, η αξία των οποίων είναι συνδεδεμένη και υπάρχει μόνο μέσα στο οικοσύστημα λειτουργίας ενός συγκεκριμένου πρωτοκόλλου blockchain (παρά σε νόμισμα).

Η αξία του καθορίζεται τελικά από τα τεχνικά χαρακτηριστικά του πρωτοκόλλου, την απήχησή και τη διάδοσή του.

ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN
Η Νομοθετική αντιμετώπιση από Ευρώπη και Ελλάδα

Κυριότερη νομοθετική αντιμετώπιση στην Ευρώπη:

Το Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 3ης Οκτωβρίου 2018 σχετικά με τις τεχνολογίες κατανεμημένου καθολικού (DLT) και το σύστημα blockchain.

- Περιλαμβάνει διάφορες συστάσεις για ομαλή ενσωμάτωση της τεχνολογίας.
- Αναγνωρίζει την ανάγκη συμμόρφωσης της τεχνολογίας blockchain με το ΓΚΠΔ.
- Υπογραμμίζει ότι σε ένα δημόσιο καθολικό (public ledger) τα δεδομένα είναι ψευδωνυμοποιημένα και όχι ανώνυμα.

Το Ευρωπαϊκό Παρατηρητήριο και Φόρουμ για το Blockchain.

Ο σκοπός του είναι να παρακολουθεί τις πρωτοβουλίες όσον αφορά το blockchain στην Ευρώπη και να κάνει προτάσεις για την χρήση του.

Στην Ελληνική Νομοθεσία, ο Νόμος 4734/2020

- Περιορίζει την ανωνυμία, που διέπει τα ψηφιακά νομίσματα.
- Δίνει ορισμούς για το ηλεκτρονικό χρήμα, τα εικονικά νομίσματα και τους παρόχους υπηρεσιών θεματοφυλακής ψηφιακών πορτοφολιών.
- η Επιτροπή Κεφαλαιαγοράς αναλαμβάνει εποπτικά καθήκοντα για τους παρόχους.

ΣΑΣ ΕΥΧΑΡΙΣΤΩ