ΟΜΑΔΑ ΑΝΑΠΤΥΞΗΣ ΛΟΓΙΣΜΙΚΟΥ
Δ/ΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΑΙ ΑΝΑΠΤΥΞΗΣ ΕΦΑΡΜΟΓΩΝ ΥΠΠΕΘ

Ενημερωτικό για τις απαιτήσεις εφαρμογής του νέου κανονισμού προστασίας δεδομένων (GDPR) στα Πληροφοριακά Συστήματα ευθύνης ΥΠΠΕΘ

Επιτελική Σύνοψη (Executive Summary)

Αθήνα, Μαρούσι 2018

Εισαγωγή

Οι απαιτήσεις εφαρμογής του γενικού κανονισμού προστασίας δεδομένων (GDPR) συνοψίζονται σε τέσσερις (4) βασικούς άξονες :

- Ελαχιστοποίηση χρήσης ευαίσθητων δεδομένων, ώστε να απαιτούνται μόνο τα άκρως απαραίτητα από το εκάστοτε πληροφοριακό σύστημα Ηλεκτρονικής Διακυβέρνησης, έπειτα από διαδικασία επαρκούς ανάλυσης και σχεδιασμού του ώστε είτε να αναπτυχθεί GDPR συμβατό από τη σχεδίαση του (GDPR by design) είτε να τροποποιηθεί μετέπειτα ώστε να καταστεί GDPR compliant (συμβατό ως προς τον κανονισμό GDPR).

- Εκτενής Χρήση φορμών συναίνεσης (consent forms) στο σύνολο των πληροφοριακών συστημάτων που διαχειρίζονται ευαίσθητα προσωπικά δεδομένα ώστε το φυσικό πρόσωπο να δύναται όχι μόνο να αποδεχθεί/διαφωνήσει στις πράξεις εκτέλεσης επεξεργασίας στα ευαίσθητα δεδομένα του αλλά και να εξασκήσει και το δικαίωμα του στη λήθη (Right to be Forgotten) με αδιάσειστα διαπιστευτήρια ότι τα ευαίσθητα δεδομένα του διαγράφηκαν για πάντα κατόπιν της δικής του απαίτησης (ψηφιακή υπογραφή κωδικοποίησης timestamp εκτέλεσης εντολής ύστερα από την επιτυχή ολοκλήρωση της πράξης οριστικής διαγραφής).

- Καταγραφή (Logging) όλων των ενεργειών εκτέλεσης επεξεργασίας ευαίσθητων δεδομένων ανά ρόλο χρήστη, πορεία αίτησης φυσικού προσώπου, ανάκτησης δεδομένων στο πληροφοριακό σύστημα. Μέσω της σωστής καταγραφής σε σύγχρονες μορφές κωδικοποίησης δεδομένων (JSON, XML κτλ.) σε υποδομή immutable database τεχνολογίας blockchain καθώς και του ελέγχου σε 24ωρη βάση (monitoring) των συστημάτων για ανίχνευση απειλών τόσο εξωτερικού και εσωτερικού δικτύου όσο και κακόβουλης χρήσης δύναται να επιτευχθεί ο στόχος του κανονισμού GDPR για αναφορά διαρροής ευαίσθητων δεδομένων (data breach) εντός 72 ωρών αλλά να είναι εφικτή και η μεταφορά των κωδικοποιημένων ευαίσθητων δεδομένων του φυσικού προσώπου σε τρίτα πληροφοριακά συστήματα που εκτελούν επεξεργασία σε αυτά σύμφωνα με διαδικασίες ηλεκτρονικής Διακυβέρνησης (Data Processors).

- Ανωνυμοποίηση των ευαίσθητων προσωπικών δεδομένων στα μητρώα αποθήκευσης τους (Συστήματα Διαχείρισης Βάσεων Δεδομένων) με χρήση διαδικασιών ψευδωνυμοποίησης και κρυπτογράφησης, τεχνολογιών μεταγλωττισμένου πηγαίου κώδικα στην λογική της εφαρμογής (application logic) του πληροφοριακού συστήματος ώστε να αποκρύπτεται ο τρόπος λειτουργίας της συνάρτησης ψευδωνυμοποίησης των ευαίσθητων δεδομένων και διαχείριση των κλειδιών (κωδικών) συμμετρικής κρυπτογράφησης των ψευδωνυμοποιημένων δεδομένων σε τρίτα ασφαλή συστήματα με χρήση τεχνολογιών VPN (Offsite Symmetric Encryption Key Management).

Διαδικασία Εφαρμογής GDPR

Η διαδικασία εφαρμογής του κανονισμού GDPR στα πληροφοριακά συστήματα ενός Δημόσιου Οργανισμού ακολουθεί συγκεκριμένα βήματα τα οποία αριθμούνται και αναλύονται κατωτέρω:

Βήμα 1ο

Καταγραφή για κάθε διαθέσιμο πληροφοριακό σύστημα εν συντομία Π.Σ του αριθμού των ευαίσθητων δεδομένων που αυτό χρησιμοποιεί, το λόγο χρήσης τους συναρτήσει της ανάγκης εύρυθμης και αποτελεσματικής λειτουργίας του πληροφοριακού συστήματος καθώς και το νομικό πλαίσιο που καθορίζει για κάθε δεδομένο ξεχωριστά την έννομη χρήση του (νόμο, υπουργική απόφαση, προεδρικό διάταγμα).

Η διαδικασία αυτή ονομάζεται σύμφωνα με το GDPR, χαρτογράφηση ευαίσθητων δεδομένων (**Data Mapping**) και διενεργείται είτε από τον φορέα είτε από την οντότητα που έχει αναλάβει έργο εκτέλεσης διαδικασίας GDPR συμμόρφωσης (GDPR compliance) για τον εν λόγω δημόσιο οργανισμό, σε αυτήν την περίπτωση η διαδικασία του Data Mapping πραγματοποιείται σε αγαστή συνεργασία των στελεχών της εταιρίας με τα αντίστοιχα επιτελικά στελέχη του δημόσιου οργανισμού για την παροχή κρίσιμων πληροφοριών περί της αρχιτεκτονικής των ενεργών πληροφοριακών συστημάτων.

Ο τρόπος καταγραφής των στοιχείων που αναφέρθηκαν ορίζεται με βάση συγκεκριμένα πρότυπα ISO, ώστε να προκύψουν αρχεία τεκμηρίωσης (PDF, Word) με το απαιτούμενο σχήμα και κωδικοποίηση που ορίζεται για την διαδικασία από το πρότυπο. Στη φάση αυτή σε περίπτωση εκτέλεσης της διαδικασίας από τον ίδιο τον οργανισμό δύναται να παραμετροποιηθούν εργαλεία που δημιουργούν αυτοματοποιημένες αναφορές πραγματοποιώντας συνδέσεις σε πολυάριθμες διαφορετικές πηγές δεδομένων (data sources) όπως Oracle, SQL Server, MySQL, MariaDB συστήματα διαχείρισης βάσεων δεδομένων. Γνωστά εργαλεία είναι τα Reports και BI publisher του οίκου Oracle καθώς και το εργαλείο λογισμικού ανοικτού κώδικα JasperReports. Επιπλέον υπάρχουν και τα εργαλεία λογισμικού που προτείνουν οι επιμέρους εθνικές αρχές προστασίας δεδομένων.

Με χρήση ενός εκ των εργαλείων λογισμικού που αναφέρθηκαν οι υπεύθυνοι χαρτογράφησης δεδομένων συνδέονται στα συστήματα διαχείρισης βάσεων δεδομένων των πληροφοριακών συστημάτων του Οργανισμού για να δημιουργήσουν τις απαιτούμενες αναφορές τεκμηρίωσης περί των πεδίων σχεσιακών ή μη σχεσιακών πινάκων της βάσης στα οποία αποθηκεύονται ευαίσθητα δεδομένα.

Βήμα 2ο

Με χρήση της τεκμηρίωσης που προέκυψε από το πρώτο βήμα, της καταγραφής των στοιχείων εξασφάλισης ασφαλείας υπολογιστικών και δικτυακών υποδομών του οργανισμού, της καταγραφής των εφαρμοζόμενων τεχνικών ανάρρωσης από απώλεια δεδομένων λόγω καταστροφής (Disaster Recovery) και ακολουθώντας τις διαδικασίες που καθορίζει το πρότυπο **ISO/IEC 29134:2017** διενεργείται η ανάλυση εκτίμησης αντικτύπου/επιπτώσεων από απώλεια/διαρροή/υποκλοπή/κακόβουλη χρήση ευαίσθητων δεδομένων που ονομάζεται **DPIA** (Data Protection Impact Assesment).
Με το πέρας της ανάλυσης δημιουργείται και η αναφορά εκτίμησης αντικτύπου στην ιδιωτικότητα που ονομάζεται **PIA** (Privacy Impact Assesment).

Ο υπεύθυνος προστασίας δεδομένων εν συντομία DPO (**Data Protection Officer)** χρησιμοποιώντας την αναφορά **PIA** αλλά και τα υπόλοιπα στοιχεία των καταγραφών και λοιπών αναφορών καθορίζει την **πολιτική ασφαλείας** που πρέπει να ακολουθηθεί από τον οργανισμό καθώς και τις πιθανές ενέργειες **τροποποιήσεων** που πρέπει να πραγματοποιηθούν στα **πληροφοριακά συστήματα** και τα συστήματα ασφαλείας δικτύων και δημιουργίας αντιγράφων ασφαλείας δεδομένων του οργανισμού ώστε αυτός να καταστεί πλήρως συμβατός με τις απαιτήσεις του κανονισμού **GDPR**.

Ο DPO συνεργάζεται απευθείας με το διευθύνοντα σύμβουλο/διοικητή/υπουργό του οργανισμού και αποτελεί τον ενδιάμεσο επικοινωνίας με την εκάστοτε εθνική αρχή προστασίας δεδομένων (ΑΠΔΠΧ www.dpa.gr) όπου πέρα από την πολιτική ασφαλείας είναι υποχρεωμένος να κοινοποιεί εντός **72 ωρών** τυχόν διαρροές ευαίσθητων δεδομένων που συνέβησαν στον οργανισμό.
Ο DPO δύναται είτε να ορισθεί σαν μόνιμος υπάλληλος στο οργανόγραμμα του δημόσιου οργανισμού που εκτελεί επεξεργασία σε ευαίσθητα δεδομένα είτε να εκμισθωθεί στον οργανισμό για συγκεκριμένο χρονικό διάστημα στα πλαίσια ολοκλήρωσης έργου υλοποίησης GDPR.
Για οργανισμούς με πολυάριθμα πληροφοριακά συστήματα εκτέλεσης επεξεργασίας σε ευαίσθητα δεδομένα το έργο ανάλυσης και επίβλεψης του DPO δύναται να συνεπικουρείται από το προσωπικό αυτοτελούς εξειδικευμένου τμήματος στο οργανόγραμμα του οργανισμού το οποίο απαιτείται να στελεχώνεται με υπαλλήλους που κατέχουν πιστοποιημένη εξειδίκευση σε θέματα δικαίου προστασίας δεδομένων, αρχιτεκτονικής πληροφοριακών συστημάτων και ασφάλειας δεδομένων.

Βήμα 3ο

Η διεύθυνση Πληροφορικής ή Ηλεκτρονικής Διακυβέρνησης του Δημόσιου Οργανισμού ακολουθώντας την προτεινόμενη πολιτική του DPO είτε τροποποιεί κατάλληλα τα πληροφοριακά συστήματα σε περίπτωση που έχουν αναπτυχθεί με ιδία μέσα (in-house) είτε προκηρύσσει κατάλληλους ανοικτούς μειοδοτικούς διαγωνισμούς ώστε να τα τροποποιήσουν είτε οι οίκοι ανάπτυξης λογισμικού που τα υλοποίησαν αρχικά είτε οι νέοι ανάδοχοι μειοδότες των προκυρηχθέντων διαγωνισμών τροποποίησης.

Το τμήμα ασφαλείας του Δημόσιου Οργανισμού είτε ενεργοποιεί αν υπάρχει διαθέσιμο το αντίστοιχο υλισμικό και λογισμικό (IPS/IDS, Carrier Grade Network Security Appliance (Active SPI Firewall, HTTP/HTTPS interception, deep packet inspection, DOS/DDOS attack mitigation)) που προσφέρει την δυνατότητα επίβλεψης, αναφοράς και καταγραφής (logging) σε 24ώρη βάση τυχών εισβολών/διαρροών μέσω εξωτερικού δημόσιου δικτύου ή επιθέσεων άρνησης υπηρεσίας (DOS/DDOS attacks) είτε διενεργεί ανοιχτό διαγωνισμό για ανάθεση σε τρίτη εταιρία ασφαλείας την παροχή εξωτερικής υπηρεσίας επίβλεψης δικτυακής ασφαλείας 24ώρης βάσης, αρχιτεκτονικής (**Security as a Service**).

Βήμα 4ο

Ο DPO είναι έτοιμος τόσο να αναφέρει οποιαδήποτε περίπτωση κακόβουλης χρήσης ή διαρροής δεδομένων μέσω των τεχνολογικών δυνατοτήτων καταγραφής και επίβλεψης που ολοκληρώθηκαν στα προηγούμενα βήματα όσο και να πιστοποιήσει την διασφάλιση προστασίας των ευαίσθητων προσωπικών δεδομένων στην ΑΠΔΠΧ σύμφωνα με την κοινοποιηθείσα και εφαρμοσθείσα πολιτική ασφαλείας που ακολουθεί όλα τα τελευταία τεχνολογικά στάνταρ που προτείνει η αγορά (**Industry Standard Best Practice**).

Εκτίμηση Μέσου Κόστους Εφαρμογής GDPR

Με παράδειγμα ανώνυμο εταιρία (Α.Ε) οικονομικού ενδιαφέροντος του ευρύτερου δημόσιου τομέα που διαθέτει πέντε (5) ολοκληρωμένα πληροφοριακά συστήματά επεξεργασίας ευαίσθητων οικονομικών δεδομένων αρχιτεκτονικής τριών επιπέδων (3-tier), μια πλήρης μελέτη εφαρμογής κανονισμού GDPR (GDPR Compliance) με εκπόνηση χαρτογράφησης ευαίσθητων δεδομένων (Data Mapping) μαζί με ετήσια υπηρεσία Security as a Service με carrier grade εξοπλισμό για επίβλεψη και αναφορά σε 24ώρη βάση συμβάντων διαρροής δεδομένων, εκμίσθωση DPO για πενήντα δύο (52) εβδομάδες, συγγραφή πολιτικής ασφαλείας για τις αλλαγές που πρέπει να πραγματοποιηθούν στα πέντε (5) πληροφοριακά συστήματά και συγγραφή όλης της επιπλέον απαραίτητης τεκμηρίωσης σύμφωνα με τα πρότυπα ISO που αναφέρθηκαν, κυμαίνεται στα **75.000 Ευρώ πλέον ΦΠΑ**.

Επειδή τα πέντε (5) Πληροφοριακά Συστήματα δεν έχουν αναπτυχθεί εσωτερικά στην Α.Ε με ιδίους πορους **(in-house)** το εκτιμώμενο κόστος τροποποίησης από τους οίκους λογισμικού που τα ανέπτυξαν αρχικά, ώστε να είναι συμβατά με το GDPR και να υλοποιήσουν τους τέσσερις (4) βασικούς άξονες που αναφέρθηκαν στην εισαγωγή κυμαίνεται πέριξ του ενός εκατομμυρίου ευρώ (**1.000.000 Ευρώ**).

Τεχνολογικές Απαιτήσεις Αρχιτεκτονικής Π.Σ για Εφαρμογή GDPR

Τα πληροφοριακά συστήματα που είτε θα σχεδιαστούν από την αρχή είτε θα τροποποιηθούν μεταγενέστερα ώστε να είναι συμβατά με το κανονισμό GDPR, απαιτείται να ακολουθούν ορισμένες αρχιτεκτονικές υλοποίησης που αναλύονται κατωτέρω:

- Υλοποίηση των πληροφοριακών συστημάτων ακολουθώντας αρχιτεκτονική **micro services** αποσύνδεσης επιπέδου λογικής της εφαρμογής (application logic layer (server side)) από επίπεδο παρουσίασης της εφαρμογής (presentation logic tier (client side/web browser, mobile app)).
  Σύμφωνα με την αρχιτεκτονική αυτή όλες οι λειτουργίες του backend (server side) της λογικής της εφαρμογής υλοποιούνται στη μορφή υπηρεσιών ιστού (Web Services) αρχιτεκτονικής **Rest** όπως συμβαίνει και σε όλες τις λειτουργίες αποθήκευσης, ανάκτησης και διαγραφής δεδομένων από το σύστημα διαχείρισης βάσης δεδομένων, ώστε να δύναται να εφαρμοσθεί έλεγχος και εκτενής καταγραφή όλων των πράξεων επεξεργασίας στα ευαίσθητα δεδομένα που αποθηκεύονται, σύμφωνα με το ρόλο του χρήστη του πληροφοριακού συστήματος εκτελούντα την εκάστοτε επεξεργασία καθώς και να αποθηκεύεται σε κατάλληλη κωδικοποίηση, η χρονική πληροφορία της ημερομηνίας της πράξης εκτέλεσης της επεξεργασίας, πχ timestamp (ημερομηνία) σε μορφή κωδικοποίησης προτύπου **ISO 8601 μέσα στο πολυπλοκότερο JSON αντικείμενο καταγραφής (logging)**.

- Υλοποίηση σχεσιακών πινάκων πλήρους καταγραφής των ενεργειών χρήστη στο πληροφοριακό σύστημα σε ξεχωριστούς υβριδικούς πίνακες με πεδία κωδικοποίησης JSON αντικειμένων. Απαιτείται υβριδική σχεδίαση βάσης δεδομένων και ειδική έκδοση συστήματος διαχείρισης βάσης δεδομένων που να υποστηρίζει συναρτήσεις επεξεργασίας και πεδία αντικειμένων τύπου JSON (JavaScript Object Notation).

- Ενεργοποίηση στο σύστημα διαχείρισης βάσεων δεδομένων εν συντομία DBMS λειτουργίας κρυπτογράφησης στρατιωτικών προδιαγραφών (military grade encryption) των δομών φυσικής αποθήκευσης δεδομένων στην μονάδα αποθήκευσης δεδομένων (σκληρός δίσκος, NAS) του λειτουργικού συστήματος/ων στο οποίο/α εκτελείται το λογισμικό του DBMS. Σε περίπτωση DBMS που διαχειρίζονται μεγάλο όγκο εγγραφών η ενεργοποίηση τέτοιας λειτουργίας έχει επίπτωση στους χρόνους αναζήτησης δεδομένων αν δεν χρησιμοποιηθεί επαγγελματική τεχνολογία συστήματος DBMS με υποστήριξη της εν λόγω λειτουργίας από τον κατασκευαστή σε αρχιτεκτονική λειτουργίας cluster.

- Χρήση συνάρτησης two-way ψευδωνυμοποίησης (scramble function) των ευαίσθητων προσωπικών δεδομένων ακολουθώντας τις προδιαγραφές που προτείνουν τα πρότυπα FIPS. Η συνάρτηση είναι two-way διότι υποστηρίζει και αντίστροφη διαδικασία μετατροπής της ψευδωνυμοποιημένης πληροφορίας στην αρχική της μορφή χωρίς να μεταβάλλει το μήκος της ή τον τύπο των αρχικών δεδομένων όπως συμβαίνει στις κρυπτογραφικές συναρτήσεις.

- Υλοποίηση διαδικασίας συμμετρικής κρυπτογράφησης των ψευδωνυμοποιημένων δεδομένων από τις

λειτουργίες του πληροφοριακού συστήματος πριν αυτά αποθηκευθούν στα αντίστοιχα πεδία των υβριδικών πινάκων της βάσης που διαχειρίζεται το DBMS. Απαιτείται η χρήση αλγορίθμων συμμετρικής κρυπτογράφησης τελευταίων προδιαγραφών (latest Industry Standard Practice) με μεγάλο μήκος κλειδιού συμμετρικής κρυπτογράφησης π.χ αλγόριθμος AES με κλειδί 256bit σε λειτουργία CBC.

- Χρήση τελευταίας γενιάς αλγορίθμων κατακερματισμού (hashing) στις συναρτήσεις κατακερματισμού one-way που χρησιμοποιούνται για την κρυπτογραφική αποθήκευση των κωδικών πρόσβασης (Login Passwords) των χρηστών του πληροφοριακού συστήματος στην βάση δεδομένων, πχ κατ' ελάχιστον αλγόριθμος συνάρτησης κατακερματισμού (hash) SHA (Secure Hash Algorithm) έκδοσης 2 που παράγει έξοδο μήκους 512bit.

- Χρήση Carrier-Grade τεχνολογιών γλωσσών προγραμματισμού (Java Enterprise Edition, .NET) για την υλοποίηση των λειτουργιών της λογικής της εφαρμογής (application logic) στον εξυπηρετητή εφαρμογών Web που στεγάζει το backend της εφαρμογής, οι οποίες παράγουν μεταγλωττισμένα εκτελέσιμα, ώστε ο πηγαίος κώδικας της εφαρμογής να είναι κατακερματισμένος (obsfuscated) και κωδικοποιημένος και ο επιτιθέμενος που ενδέχεται να τον πάρει στα χέρια του σύμφωνα με τα σενάρια της ανάλυσης ρίσκου DPIA να μην μπορεί να ανακαλύψει τον τρόπο λειτουργίας της συνάρτησης ψευδωνυμοποίησης ευαίσθητου δεδομένου π.χ ΑΦΜ.
  Κατά αυτόν τον τρόπο σε περίπτωση που πέσει στα χέρια του επιτιθέμενου η βάση με τα ευαίσθητα δεδομένα ακόμα και να την αποκρυπτογραφήσει (αν ανακαλύψει τα κλειδιά συμμετρικής κρυπτογράφησης) δεν δύναται να αναδημιουργήσει το ευαίσθητο δεδομένο από την ψευδωνυμοποιημένη πληροφορία που προκύπτει έπειτα από την διαδικασία αποκρυπτογράφησης, εφόσον δεν μπορεί να ανακαλύψει στον πηγαίο κώδικα πως λειτουργεί η two-way συνάρτηση ψευδωνυμοποίησης.
  Σε περίπτωση χρήσης τεχνολογίας interpeted γλωσσάς προγραμματισμού (PHP, Python) για την δημιουργία των λειτουργιών του backend της εφαρμογής απαιτείται η χρήση επαγγελματικής βιβλιοθήκης για την μετατροπή του interpreted πηγαίου κώδικα σε κωδικοποιημένη μη καταληπτή μορφή στον παραγωγικό εξυπηρετητή της εφαρμογής.

- Μη αποθήκευση των κλειδιών (κωδικών) συμμετρικής κρυπτογράφησης των ψευδωνυμοποιημένων δεδομένων στον εξυπηρετητή εφαρμογών που εκτελεί την λογική της εφαρμογής του πληροφοριακού συστήματος. Η λογική της εφαρμογής που είναι υλοποιημένη σε τεχνολογία γλώσσας προγραμματισμού που παράγει κωδικοποιημένο εκτελέσιμο συνδέεται σε τρίτο backend με χρήση τεχνολογιών VPN κατά προτίμηση SSL VPN, από όπου αντλεί τα κλειδιά συμμετρικής κρυπτογράφησης (Offsite Key Management) όποτε απαιτείται να εκτελέσει διαδικασίες κρυπτογράφησης/αποκρυπτογράφησης ψευδωνυμοποιημένων δεδομένων πριν την υλοποίηση λειτουργιών αποθήκευσης/ανάκτησης τους στο DBMS.

- Χρήση των ψηφιακών πιστοποιητικών του οργανισμού για την ψηφιακή υπογραφή των αντικειμένων καταγραφής JSON με χρονική πληροφορία (timestamp) εκτέλεσης πράξης οριστικής διαγραφής ευαίσθητων δεδομένων στα πλαίσια υλοποίησης του δικαιώματος στη λήθη του χρήστη.

- Παροχή Κατάλληλων API (Application Programmer Interface) Υπηρεσιών Ιστού (Web Services) αρχιτεκτονικής Rest, με μεθόδους που να επιστρέφουν πληροφορίες καταγραφής ενεργειών επεξεργασίας ευαίσθητων δεδομένων, προς κατανάλωση από τους αρμοδίους της εθνικής αρχής προστασίας δεδομένων κατά την διαδικασία πραγματοποίησης δειγματοληπτικών ελέγχων συμμόρφωσης με το GDPR.

- Πρόσβαση στις υπηρεσίες των πληροφοριακών συστημάτων και κατανάλωση όλων των υπηρεσιών Ιστού (Web Services) αποκλειστικά πάνω από τις τελευταίες τεχνολογίες μεταφοράς HTTPS αρχιτεκτονικής SSL/TLS με χρήση των τελευταίων πρωτοκόλλων HSTS (HTTP Strict Transport Security).

- Πρόβλεψη υλοποίησης μηχανισμού δια-λειτουργίας με IAM (Identity and Access Management) εξυπηρετητή για υλοποίηση Consent Management Portal με χρήση εξειδικευμένων GDPR privacy toolkit SDK's (Software Development Kit) που προσφέρουν οι οίκοι λογισμικού που αναπτύσσουν εξυπηρετητές IAM.

- Υλοποίηση επικαιροποιημένων τεχνολογιών ελέγχου αυθεντικοποίησης/εξουσιοδότησης εξωτερικών/εσωτερικών χρηστών στο σύνολο των πληροφοριακών συστημάτων χρησιμοποιώντας μεθόδους αυθεντικοποίησης δύο παραγόντων (Two-Factor Authentication, SMS/Messenger/Mail) με κωδικούς μιας χρήσης (OTP, one time password) και πρωτόκολλα OAUTH κατά προτίμηση έκδοσης 2.0