ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΕ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ

ΤΕΛΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ

ΤΗΡΗΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΤΩΝ ΟΡΓΑΝΙΣΜΩΝ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ, ΕΞΕΛΙΞΕΙΣ ΚΑΙ Ο ΝΕΟΣ ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΤΜ. ΕΞΕΙΔΙΚΕΥΣΗΣ ΔΙΟΙΚΗΣΗΣ ΟΡΓΑΝΙΣΜΩΝ ΚΟΙΝΩΝΙΚΗΣ ΦΡΟΝΤΙΔΑΣ

Επιβλέπων/ουσα:
Μιχαήλ Δαγιακίδης

Σπουδαστής:
Γεώργιος Παππάς

ΑΘΗΝΑ - 2018

Τήρηση Προσωπικών Δεδομένων στα Πληροφοριακά Συστήματα των Οργανισμών Κοινωνικής Ασφάλισης. Ιστορική Αναδρομή, Εξελίξεις και ο Νέος Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων

Δήλωση

«Δηλώνω ρητά ότι η παρούσα εργασία αποτελεί προϊόν προσωπικής εργασίας, δεν παραβιάζει καθ' οιονδήποτε τρόπο πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής»

Αθήνα, 12/12/2018

Υπογραφή

Περίληψη

Η είσοδος και αξιοποίηση των Τεχνολογιών Πληροφορίας και Επικοινωνιών στην ελληνική Δημόσια Διοίκηση αποτελεί διαχρονικό ζητούμενο. Παρά την σχετική υστέρηση σε σχέση με τον ευρωπαϊκό μέσο όρο, οι προσπάθειες αξιοποίησης των νέων τεχνολογιών και δημιουργίας Πληροφοριακών Συστημάτων, ειδικά στον τομέα της Κοινωνικής Ασφάλισης, μετρούν πλέον δεκαετίες,. Η λειτουργία των συστημάτων αυτών είναι συνηφασμένη με την επεξεργασία προσωπικών δεδομένων. Τις τελευταίες δεκαετίες η δυνατότητα μαζικής επεξεργασίας και μετάδοσης των δεδομένων αυτών έχει δημιουργήσει ανησυχίες για τις επιπτώσεις στην προστασία της ιδιωτικότητας του ατόμου, ακόμα και στην λειτουργία της ίδιας της δημοκρατικής διαδικασίας. Παγκοσμίως έχει αναπτυχθεί ένα νομοθετικό πλαίσιο το οποίο θέτει περιορισμούς και κατευθύνσεις ως προς την τήρηση και επεξεργασία των προσωπικών δεδομένων, το οποίο αναπόφευκτα επηρεάζει και την λειτουργία των Φορών Κοινωνικής Ασφάλισης.

Ο στόχος της παρούσας εργασίας είναι διττός· Αφενός επιχειρείται να παρουσιαστεί η έννοια των προσωπικών δεδομένων και του κανονιστικού πλαισίου που αφορά την προστασία τους. Αφετέρου, να χαρτογραφηθεί η τήρηση και επεξεργασία τους στα πληροφοριακά συστήματα των Φορέων Κοινωνικής Ασφάλισης. Τέλος, προτείνονται κάποια επόμενα βήματα προκειμένου οι Φορείς να προσαρμοστούν στις νέες απαιτήσεις που επιφέρει ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων, ευρύτερα γνωστός με το λατινικό ακρονύμιο GDPR.

Η έρευνα και η ανάπτυξη του θέματος βασίστηκε στην ανάλυση γραπτων τεκμηρίων, περιλαμβανομένης νομοθεσίας, βιβλιογραφίας περί της ιδιωτικότητας και της ασφάλειας των Πληροφοριακών Συστημάτων, παρουσιάσεων σε συνεδρια, εκθέσεων καθώς και σε συνοδευτικά έγγραφα δημόσιων διαγωνισμών για την προμήθεια Πληροφοριακών Συστημάτων.

Λέξεις-Κλειδιά: **Προσωπικά Δεδομένα, Πληροφοριακά Συστήματα, Φορείς Κοινωνικής Ασφάλισης, Προστασία Ιδιωτικότητας, Προστασία Πληροφοριακών Συστημάτων, Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων**

Executive Summary

The introduction and utilization of Information and Communication Technologies in the Greek Public Administration is an everlasting demand. Despite the relative lag in relation to the European νορμ, attempts to exploit new technologies and create Information Systems have been in place since many years, especially in the field of Social Insurance . The operation of such systems is intrinsically linked to the processing of personal data. During the last decades the mass processing and transmission of these data have raised concerns about its impact on the protection of the individual, even in the functioning of the democratic process. Globally, legislative frameworks have been developed that set limits and guidelines for keeping and processing personal data, which inevitably affect the functioning of Social Insurance.

The aim of this work is threefold. Firstly, the concept of personal data and the regulatory framework for protecting them is presented. Secondly, it attempts a mapping of the ICT systems of Social Insurance Institutions. Finally, some further steps are proposed to bring the Institutions in line with the requirements of the new General Data Protection Regulation, more widely known with its abbreviation GDPR.

The research on the topic was based on written evidence analysis, including legislature, studies on the privacy and security of Information Systems, conference presentations , reports and public tender documents.

Keywords: **Personal Data, Information Systems, Social Security Institutions, Privacy Protection, Information Systems Protection, General Data Protection Regulation**

Περιεχόμενα

Πίνακας Εικονογράφησης

Πίνακας Συντμήσεων και Συντομογραφιών

Ελληνικές

ΑΔΔΥ:	Ασφαλής Διάταξη Δημιουργίας Υπογραφής
ΑΜΚΑ:	Αριθμός Μητρώου Κοινωνικής Ασφάλισης
ΑΠΔ:	Αναλυτική Περιοδική Δήλωση
ΑΠΔΠΧ:	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΑΠΕΔ:	Αρχή Πιστοποίησης Ελληνικού Δημοσίου
ΑΦΜ:	Αριθμός Φορολογικού Μητρώου
ΓΓΠΣ:	Γενική Γραμματεία Πληροφοριακών Συστημάτων
ΓΚΠΔ:	Γενικός Κανονισμός Προστασίας Δεδομένων
ΕΜΑΕΣ:	Εθνικά Μητρώα Ασφαλισμένων, Εργοδοτών και Συνταξιούχων
ΕΣΕΠΣ:	Ενιαίο Σύστημα Ελέγχου και Πληρωμών Συντάξεων
ΕΤΑΑ:	Ενιαίο Ταμείο Ανεξάρτητα Απασχολούμενων
ΕΤΑΠ-ΜΜΕ:	Ενιαίο Ταμείο Ασφάλισης Προσωπικού Μέσων Μαζικής Ενημέρωσης
ΕΤΑΤ:	Ενιαίο Ταμείο Ασφάλισης Τραπεζοϋπαλλήλων
ΕΤΕΑΕΠ:	Ενιαίο Ταμείο Επικουρικής Ασφάλισης και Εφάπαξ Παροχών
ΕΦΚΑ:	Ενιαίος Φορέας Κοινωνικής Αλληλεγγύης
ΕΑΠΔ:	Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων
ΕΕ:	Ευρωπαϊκή Ένωση

ΗΔ:	Ηλεκτρονική Διακυβέρνηση
ΗΔΙΚΑ:	Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλιση
ΙΚΑ:	Ίδρυμα Κοινωνικών Ασφαλίσεων
ΙΚΑ-ΕΤΑΜ:	Ίδρυμα Κοινωνικών Ασφαλίσεων-Ενιαίο Ταμείο Ασφάλισης Μισθωτών
ΚΕΑΟ:	Κέντρο Ενοποιημένων Ασφαλιστικών Οφειλών
ΚΗΥΚΥ:	Κέντρο Ηλεκτρονικού Υπολογιστή Κοινωνικών Υπηρεσιών
ΝΑΤ:	Ναυτικό Απομαχικό Ταμείο
ΝΠΔΔ:	Νομικό Πρόσωπο Δημοσίου Δικαίου
ΟΑΕΕ:	Οργανισμός Ασφάλισης Ελεύθερων Επαγγελματιών
ΟΓΑ:	Οργανισμός Γεωργικών Ασφαλίσεων
ΟΟΣΑ:	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
ΟΠΣ:	Ολοκληρωμένο Πληροφοριακό Σύστημα
ΠΣ:	Πληροφοριακό σύστημα
ΤΑΥΤΕΚΩ:	Ταμείο Ασφάλισης Υπαλλήλων Τραπεζών & Επιχειρήσεων Κοινής Ωφέλειας
ΤΕΑΥΕΚ:	Τομέας Επικουρικής Ασφάλισης Υπαλλήλων Εμπορικών Καταστημάτων
ΤΠΕ:	Τεχνολογίες Πληροφοριών και Επικοινωνιών
ΥΕΔ:	Υπεύθυνος Επεξεργασίας Δεδομένων
ΥΠΔ:	Υπεύθυνος Προστασίας Δεδομένων
ΦΚΑ:	Φορέας Κοινωνικής Ασφάλισης

Αγγλικές

CR:	Computer Room
DPO:	Data Protection Officer
DPIA:	Data Protection Impact Assessment
GDPR:	General Data Protection Rule
G2B:	Government to Business
G2C:	Government to Citizen
G2G:	Government to Government
IDS:	Intrusion Detection System
IPS:	Intrusion Prevention System
OTP:	One Time Password
SLA:	Service Level Agreement
RDBMS:	Relational Database Management System
VPN:	Virtual Private Network
WAN:	Wide Area Network

Εισαγωγή

Η έννοια της ιδιωτικότητας είναι αρχαία και νεωτερική ταυτόχρονα. Ξεκινάει από τα αριστοτελικά Ηθικά και ανασηματοδοτείται στο λυκόφως των νέων μέσων μεταφοράς της πληροφορίας του 19ου αιώνα. Το προσωπικό πλέον μπορεί γρήγορα να φύγει από τα προστατευόμενα όρια της οικίας, της πόλης, ακόμα και του κράτους και να γίνει παγκόσμιο. Σε χρόνους που ξεκίνησαν από εβδομάδες και έχουν φτάσει τα δευτερόλεπτα. Η Πληροφορική Επανάσταση εκβιομηχανοποιεί και επιταχύνει ακόμα περισσότερο αυτή τη διαδικασία, επιτρέποντας την μαζική αποθήκευση, επεξεργασία και αναμετάδοση δεδομένων.

Από τους πρώτους που σπεύδουν να επωφεληθούν από τις τεχνολογίες αυτές είναι οι Φορείς Κοινωνικής Ασφάλισης. Τα ερμάρια αρχίζουν να παραχωρούν τη θέση τους στις διάτρητες κάρτες ήδη από την δεκαετία του ‘60 σε οργανισμούς όπως η Social Security Administration, ο ομοσπονδιακός Φορέας Κοινωνικής Ασφάλισης (ΦΚΑ) των ΗΠΑ, ο οποίος είναι επιφορτισμένος με την τήρηση των ασφαλιστικών δεδομένων εκατομμυρίων Αμερικανών. Όπως όμως υποστηρίζει ο φιλόσοφος Paul Virilio (2007), κάθε νέα τεχνολογία δημιουργεί και νέα ατυχήματα. Στην περίπτωση των Πληροφοριακών Συστημάτων (ΠΣ) η κατάχρηση των προσωπικών δεδομένων μπορεί να απειλήσει την ιδιωτική σφαίρα του ατόμου και τη λειτουργία του ως πολίτη. Γι’αυτό παράλληλα με την μαζίκή διάθεση των Πληροφοριακών Συστημάτων (ΠΣ) ξεκινά και η ανάπτυξη της νομοθεσίας για την προστασία των δεδομένων προσωπικού χαρακτήρα ή προσωπικών δεδομένων για συντομία. Μια διαδικασία της οποίας το πλέον πρόσφατο ορόσημο είναι η ψήφιση του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ ή πιο γνωστός ως GDPR).

Η παρούσα εργασία ξεκινά με μια περιγραφή των εννοιών της Ηλεκτρονικής Διακυβέρνησης και του Πληροφοριακού Συστήματος στο Πρώτο κεφάλαιο, το οποίο περιλαμβάνει και μια συνοπτική καταγραφή των ΠΣ τα οποία χρησιμοποιούν οι Φορείς Κοινωνικής Ασφάλισης (ΦΚΑ) στην Ελλάδα. Το Δεύτερο κεφάλαιο τεκμηριώνει την έννοια της ιδιωτικότητας, του προσωπικού δεδομένου και περιλαμβάνει μια επισκόπηση της προστασίας τους, παρουσιάζοντας τη σχετική νομοθεσία με έμφαση

στις αλλαγές που επιφέρει ο GDPR. Το Τρίτο κεφάλαιο ασχολείται με τις πρακτικές τήρησης και προστασίας των προσωπικών δεδομένων στα ΠΣ των ΦΚΑ. Τέλος, το Τέταρτο κεφάλαιο παραθέτει μερικές προτάσεις προκειμένου να προσαρμοστούν οι ΦΚΑ στις απαιτήσεις του GDPR και, ίσως σημαντικότερο, να βελτιώσουν τις πρακτικές και διαδικασίες ασφάλειας των προσωπικών δεδομένων τα οποία τηρούν προς εκπλήρωση του ρόλου τους.

1.Πληροφοριακά Συστήματα Κοινωνικής Ασφάλισης

1.1 Οι έννοιες της Ηλεκτρονικής Διακυβέρνησης και του Πληροφοριακού Συστήματος

1.1.1 Ηλεκτρονική Διακυβέρνηση

1.1.1.1 Ορισμός

Ο όρος «Ηλεκτρονική Διακυβέρνηση» (ΗΔ) (*electronic Government – e-Government*) περιγράφει τη χρήση και εφαρμογή Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ) σε διαδικασίες και υπηρεσίες της Δημόσιας Διοίκησης. Αν και ο όρος είναι σχετικά νέος, χρησιμοποιείται για να περιγράψει μια αλληλεπίδραση η οποία ξεκίνησε σχεδόν από την εμφάνιση των πρώτων Πληροφοριακών Συστημάτων (Grönlund & Horan, 2005)

Υπάρχει πληθώρα ορισμών της ΗΔ, παρεπόμενο των πολλαπλών προσεγγίσεων ως προς αυτήν στην εκάστοτε χώρα. Κάποιοι από τους ορισμούς επικεντρώνονται στην χρήση των ΤΠΕ ενώ άλλοι στο πως μετασχηματίζεται γενικότερα η Δημόσια Διοίκηση λόγω της χρήσης τους.

Κινούμενη στην δεύτερη κατεύθυνση, στην Ανακοίνωση 567/2003, η Ευρωπαϊκή Επιτροπή ορίζει την Ηλεκτρονική Διακυβέρνηση ως «(τ)η χρήση των ΤΠΕ στις δημόσιες διοικήσεις, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού. Σκοπός είναι η βελτίωση των δημόσιων υπηρεσιών, καθώς και η ενίσχυση των δημοκρατικών διαδικασιών και των διαδικασιών στήριξης των δημόσιων πολιτικών.»

Παρομοίως, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ, 2015) ορίζει ως ηλεκτρονική διακυβέρνηση «την χρήση από τις κυβερνήσεις των ΤΠΕ, και ιδιαίτερα του Διαδικτύου, σαν εργαλείο για την επίτευξη καλύτερης διακυβέρνησης». Ο ΟΟΣΑ έχει ξεχωριστό ορισμό για την Ψηφιακή Διακυβέρνηση (*Digital Governance*) την οποία ορίζει ως «τη χρήση ψηφιακών τεχνολογιών, σαν νευραλγικό τμήμα των στρατηγικών εκμοντερνισμού των κυβερνήσεων, για να

δημιουργήσουν δημόσια προστιθέμενη αξία. Βασίζεται σε ένα οικοσύστημα ψηφιακής διακυβέρνησης που το αποτελούν κυβερνητικοί δρώντες, Μη Κυβερνητικές Οργανώσεις, επιχειρήσεις, ενώσεις πολιτών και ιδιώτες που υποστηρίζει την παραγωγή και την πρόσβαση σε δεδομένα, υπηρεσίες και περιεχόμενο μέσω αλληλεπιδράσεων με την κυβέρνηση.»

Κοινά στοιχεία και στους τρεις ορισμούς που παρατέθηκαν είναι η χρήση ΤΠΕ από τη Δημόσια Διοίκηση και η αντιμετώπιση τους ως εργαλείο, όχι αυτοσκοπό, με στόχο την βελτίωση της δημόσιας διακυβέρνησης και των υπηρεσιών που αυτή προσφέρει.

1.1.1.2 Χαρακτηριστικά και βασικοί τομείς

Ως προς τα χαρακτηριστικά των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, τα βασικά είναι (Κοινωνία της Πληροφορίας, 2008):

Έχει χρήστη: Ο χρήστης της υπηρεσίας μπορεί να είναι ο πολίτης, μια επιχείρηση, ένας άλλος φορέας της Δημόσιας Διοίκησης ή ακόμα και άλλες υπηρεσιακές μονάδες ή στελέχη του ιδίου Φορέα.

Έχει παραδοτέο: Το παραδοτέο πρέπει να είναι αυτοτελές και ο χρήστης που το παραλαμβάνει πρέπει μπορεί να το αξιοποιήσει χωρίς να απαιτούνται επιπλέον εργασίες, συναλλαγές ή παραδοτέα.

Έχει πάροχο: Η υπηρεσία παρέχεται από μια Υπηρεσιακή Μονάδα ενός Φορέα της Δημόσιας Διοίκησης

Έχει ρυθμιστή: Υπάρχει τουλάχιστον μια Υπηρεσιακή Μονάδα με αρμοδιότητα για το ρυθμιστικό πλαίσιο της υπηρεσίας.

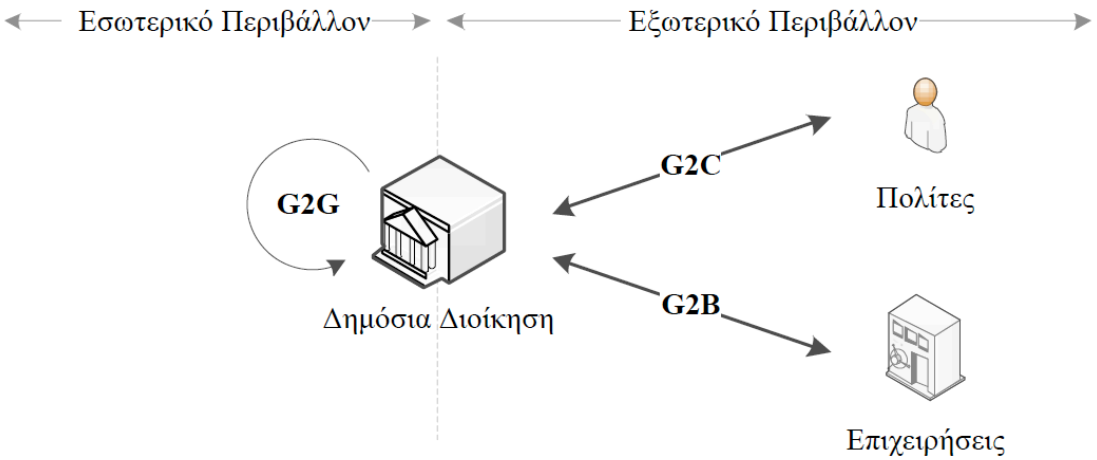
Οι υπηρεσίες της ηλεκτρονικής διακυβέρνησης λοιπόν μπορεί να απευθύνονται σε διάφορους χρήστες που κινούνται τόσο στο εξωτερικό περιβάλλον της Δημόσιας Διοίκησης (πολίτες, επιχειρήσεις, Μη Κυβερνητικές Οργανώσεις κ.α.) όσο και στο εσωτερικό της. Μια διαδεδομένη κατηγοριοποίηση των υπηρεσιών βάσει των τελικών χρηστών είναι η ακόλουθη:

Government to Citizen (G2C): Αναφέρεται στις αλληλεπιδράσεις της Δημόσιας Διοίκησης με τους μεμονωμένους πολίτες όπως είναι πχ η ηλεκτρονική αίτηση συνταξιοδότησης

Government to Business (G2B): Περιγράφει τις αλληλεπιδράσεις ανάμεσα στους οργανισμούς του ιδιωτικού τομέα και την Δημόσια Διοίκηση, όπως π.χ. η ηλεκτρονική καταβολή εισφορών των εργαζομένων

Government to Government (G2G): Η τρίτη κατηγορία περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ φορέων και οργανισμών που εμπίπτουν στη δικαιοδοσία της Δημόσιας Διοίκησης, όπως είναι π.χ. η χρήση του μητρώου Αριθμών Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ) της Ηλεκτρονικής Διακυβέρνησης Κοινωνικής Ασφάλισης (ΗΔΙΚΑ) από τον Ενιαίο Φορέα Κοινωνικής Ασφάλισης.

Οι τομείς του G2C και του G2B θεωρούνται παραδοσιακά πως ανήκουν στο εξωτερικό περιβάλλον της δημόσιας διοίκησης ενώ ο G2G στο εξωτερικό. Στα πλαίσια όμως της πολυεπίπεδης διακυβέρνησης και της διαρκώς στενότερης διακρατικής συνεργασίας σε πληθώρα τομέων, ο διαχωρισμός αυτός σταδιακά χάνει την αξία του.



Σχήμα 1 Τομείς Ηλεκτρονικής Διακυβέρνησης

1.1.2 Πληροφοριακά Συστήματα

Μια από τις πλέον νευραλγικές ΤΠΕ προκειμένου να υλοποιηθούν οι στόχοι της ηλεκτρονικής διακυβέρνησης είναι τα Πληροφοριακά Συστήματα (ΠΣ). Ως ΠΣ μπορεί

να χαρακτηριστεί ένα σύνολο αλληλένδετων στοιχείων τα οποία συλλέγουν (ή ανακτούν), επεξεργάζονται, αποθηκεύουν και διανέμουν πληροφορίες για να υποστηρίξουν τη λήψη αποφάσεων και τον έλεγχο ενός οργανισμού (Laudon & Laudon, 2011).

Σύμφωνα με τον Κιουντούζη (2009), τα βασικά στοιχεία που συναποτελούν ένα πληροφοριακό σύστημα είναι 1) το *λογισμικο* (software) όπως πχ βάσεις δεδομένων, 2) το *υλικό* (hardware) όπως πχ ηλεκτρονικοί υπολογιστές (ΗΥ) 3) οι *διαδικασίες* πχ ο χειρισμός των στοιχείων του υλικού και 4) τα *δεδομένα* (data), δηλαδή καταγραφές οι οποίες δεν έχουν μορφοποιηθεί ακόμα σε πληροφορία αξιοποιήσιμη από ανθρώπους, (πχ τα στοιχεία ενός τιμολογίου).

Για να καταστεί η πληροφορία αξιοποιήσιμη και να συνεισφέρει στη λήψη αποφάσεων απαιτούνται τρεις δραστηριότητες στα πληροφοριακά συστήματα - η *εισροή* (input), δηλαδή η συγκέντρωση και καταγραφή δεδομένων, η *επεξεργασία* τους, δηλαδή η μετατροπή τους σε κάποια μορφή πληροφορίας που να έχει νόημα για τον οργανισμό και η *εκροή* τους, δηλαδή η μεταφορά της πληροφορίας σε αυτούς που θα την αξιοποιήσουν (Laudon & Laudon, 2011).

1.1.3 Πληροφοριακά Συστήματα στους Φορείς Κοινωνικής Ασφάλισης στην Ελλάδα

1.1.3.1 Δομή του Συστήματος Κοινωνικής Ασφάλισης στην Ελλάδα

Σύμφωνα με τον ν. 4387/2016, «Ενιαίο Σύστημα Κοινωνικής Ασφάλειας - Μεταρρύθμιση ασφαλιστικού - συνταξιοδοτικού συστήματος κ.α.» το Εθνικό Σύστημα Κοινωνικής Ασφάλισης είναι ένας από τους τρεις πυλώνες του Ενιαίου Συστήματος Κοινωνικής Ασφάλειας, μαζί με το Εθνικό Σύστημα Υγείας και το Εθνικό Σύστημα Κοινωνικής Αλληλεγγύης. Το Εθνικό Σύστημα Κοινωνικής Ασφάλισης είναι υπεύθυνο για τις ασφαλιστικές παροχές. Η σημερινή δομή του Συστήματος Κοινωνικής Ασφάλισης στην Ελλάδα προέκυψε ύστερα από από την εκ βάθρων αναδιοργάνωση του συστήματος με τον προαναφερθέντα νόμο.

Ο μεγαλύτερος ΦΚΑ, ο οποίος δημιουργήθηκε με τον νόμο είναι ο Ενιαίος Φορέας Κοινωνικής Ασφάλισης (ΕΦΚΑ), το μοναδικό πλέον ταμείο κύριας ασφάλισης. Σε αυτόν συνενώθηκαν οι κλάδοι κύριας ασφάλισης των ΙΚΑ-ΕΤΑΜ, ΕΤΑΠ-ΜΜΕ,

ΕΤΑΑ, ΟΑΕΕ, ΟΓΑ, ΝΑΤ, ΤΑΥΤΕΚΩ, ΕΤΑΤ και οι συνταξιοδοτικές αρμοδιότητες της Γενικής Διεύθυνσης Χορήγησης Συντάξεων Δημοσίου Τομέα του Υπουργείου Οικονομικών. Ο ΕΦΚΑ αναλαμβάνει την ασφάλιση για αναπηρία, γήρας και θάνατο και παρέχει της χρηματικές απολαβές για ασθένεια και μητρότητα.

Συγκροτήθηκε επίσης ένα ταμείο Επικουρικής Ασφάλισης, το Ενιαίο Ταμείο Επικουρικής Ασφάλισης και Εφάπαξ Παροχών (ΕΤΕΑΕΠ), όπως μετονομάστηκε το ΕΤΑΠ. Συγκροτείται από δύο κλάδους, έναν εφάπαξ παροχών και έναν επικουρικής ασφάλισης. Στον τομέα εφάπαξ παροχών εντάχθηκαν όλα τα ταμεία και οι κλάδοι πρόνοιας των προϋπάρχοντων ταμείων ενώ στον κλάδο επικουρικής ασφάλισης όλα τα επικουρικά ταμεία και οι κλάδοι επικουρικής

Υπηρεσίες πληροφορικής στους δύο ασφαλιστικούς φορείς παρέχει και η ΗΔΙΚΑ, μια Ανώνυμη Εταιρεία με μοναδικό μέτοχο το Δημόσιο, η οποία έχει αποστολή της την παροχή λύσεων στον τομέα των ΤΠΕ οι οποίες θα υποστηρίζουν την αποτελεσματική λειτουργία τους.

1.1.3.2 Εξέλιξη των Πληροφοριακών συστημάτων των Φορέων Κοινωνικής Ασφάλισης

Για να εκπληρώσουν το έργο τους, οι ΦΚΑ χρειάζεται να καταχωρήσουν, αποθηκεύσουν και διαχειρηστούν έναν μεγάλο όγκο δεδομένων όπως αυτός προκύπτει από καταγραφές ασφαλισμένων, εισφορές εργαζομένων και εργοδοτών κ.α. Δεν αποτελεί έκπληξη λοιπόν πως τόσο παγκοσμίως όσο και στην Ελλάδα οι οργανισμοί αυτοί ήταν από τους πρώτους που στράφηκαν στην ανάπτυξη ΠΣ προκειμένου να βελτιστοποιήσουν τις διεργασίες τους.

Ήδη από το 1950 το Ίδρυμα Κοινωνικών Ασφαλίσεων (ΙΚΑ) εφοδιάστηκε με διάτρητες κάρτες και τις αντίστοιχες σχετικές διατρητικές μηχανές που «διάβαζαν» τις πληροφορίες, χωρίς όμως η χρήση τους να διαδοθεί λόγω υψηλού κόστους. Παρόμοιες προσπάθειες φαίνεται να έγιναν και στον ΟΓΑ από το 1963. Μια πιο σημαντική προσπάθεια έγινε από το 1965 με τη χρήση πλέον των μαγνητοταινιών (tapes) που τις διάβαζαν οι πρώτοι Ηλεκτρονικοί Υπολογιστές εκείνης της εποχής (Σαγκριώτου, 2000). Το 1969 ιδρύθηκε με το Ν.Δ. 30 390/1969 το Κέντρο Ηλεκτρονικού Υπολογιστή Κοινωνικών Υπηρεσιών (ΚΗΥΚΥ), ένα Νομικό Πρόσωπο Ιδιωτικού Δικαίου (ΝΠΙΔ) με σκοπό τη μηχανογραφική εξυπηρέτηση των φορέων κοινωνικής ασφάλισης και

κοινωνικής πολιτικής. Το ΚΗΥΚΥ, το οποίο θα μετελισσόταν το 2007 στην (ΗΔΙΚΑ), ανέλαβε κατ'αποκλειστικότητα την προμήθεια μηχανογραφικών συστημάτων για τους οργανισμούς κοινωνικής ασφάλισης. Στο νεοσύστατο φορέα εντάχθηκε ο εξοπλισμός και το προσωπικό της πρωτοπόρου για την εποχή μηχανοργάνωσης του ΟΓΑ. Το 1981 όμως με τον Ν.1199/1089 το ΙΚΑ και ο ΟΓΑ, οι δύο μεγαλύτεροι φορείς κοινωνικής ασφάλισης, αυτονομήθηκαν μηχανογραφικά.

Το 1992 θεσμοθετήθηκε η συγκρότηση των Εθνικών Μητρώων Ασφαλισμένων, Εργοδοτών και Συνταξιούχων (ΕΜΑΕΣ) τα οποία θα απέδιδαν και έναν μοναδικό αριθμό σε κάθε εγγεγραμμένο ασφαλισμένο ή συνταξιούχο, τον μετέπειτα ΑΜΚΑ. Η δημιουργία του σχετικού πληροφοριακού συστήματος, του μετέπειτα ΑΜΚΑ-ΕΜΑΕΣ ξεκίνησε το 1993 αλλά η υπηρεσία θα ολοκληρωνόταν μόλις το 2009 (ιστότοπος ΗΔΙΚΑ).[1]

Στο ίδιο διάστημα οι επιμέρους ασφαλιστικοί οργανισμοί ανέπτυσσαν τα δικά τους ΟΠΣ. Το 1999, στα πλαίσια του Περιφερειακού Επιχειρησιακού Προγράμματος «Κλεισθένης» που εντάχθηκε στο Β' Κοινοτικό Πλαίσιο Στήριξης (ΚΠΣ), ξεκίνησε η ανάπτυξη του ΟΠΣ ΙΚΑ - ΙΚΑΝΕΤ. Το φιλόδοξο αυτό σύστημα θα χωριζόταν σε τέσσερα επιμέρους υποσυστήματα, Σύστημα Παροχών, Σύστημα Ασφαλιστικών Εισφορών, Σύστημα Υγείας, και Οικονομικό Πληροφοριακό Σύστημα, ώστε να καλύπτει πλήρως τις ανάγκες του τότε μεγαλύτερου ασφαλιστικού φορέα. Το ΙΚΑΝΕΤ, η πλατφόρμα διεπαφής με πολίτες και επιχειρήσεις θα περιελάμβανε την παροχή ηλεκτρονικών υπηρεσιών τόσο G2B, όπως η ηλεκτρονική Αναλυτική Περιοδική Δήλωση, όσο και G2C όπως ο προγραμματισμός ιατρικών επισκέψεων.

Η συγχώνευση των ασφαλιστικών οργανισμών σε ουσιαστικά δύο φορείς, τον ΕΦΚΑ και το ΕΤΕΑΠ, δημιούργησε μια νέα κατάσταση στα ασφαλιστικά συστήματα των ΦΚΑ.

1.1.3.3 ΗΔΙΚΑ

[1] Μέχρι το 2006 είχε αποδοθεί ΑΜΚΑ σε ποσοστό μικρότερο του 50% των άμεσα ασφαλισμένων και συνταξιούχων στην Ελλάδα κυρίως λόγω έλλειψης των στοιχείων, που είναι υποχρεωτικά για την ένταξή τους στο ΕΜΑΕΣ. Οι βασικοί λόγοι της υστέρησης ήταν η δυσκολία προσέγγισης του πολίτη για την ολοκλή-ρωση της διαδικασίας απογραφής και η έλλειψη επαρκούς αριθμού προσωπικού από τη μεριά των ασφαλιστικών ταμείων για την πραγματοποίηση των διαδικασιών ενημέρωσης απογραφής για τη χορήγηση ΑΜΚΑ.

Εφαρμογές

Η ΗΔΙΚΑ έχει αναπτύξει και διαχειρίζεται μια σειρά από πληροφοριακά συστήματα τα οποία χρησιμοποιούνται από πληθώρα φορέων τόσο Κοινωνικής Ασφάλισης όσο και ευρύτερα του δημοσίου τομέα. Αναφορικά με την Κοινωνική Ασφάλιση, τα σημαντικότερα είναι:

Εθνικό Μητρώο ΑΜΚΑ: Το μοναδικό ηλεκτρονικό μητρώο πολιτών του ελληνικού κράτους, το οποίο αποδίδει τον ΑΜΚΑ και καταχωρεί βασικά στοιχεία που διακρίνουν τον κάθε ασφαλισμένο (Όνομα, ημερομηνία γέννησης, εθνικότητα κ.α.)

Σύστημα ΑΤΛΑΣ: Το Ενιαίο Μητρώο Ασφάλισης-Ασφαλιστικής Ικανότητας. Διαθέτει περιορισμένο ασφαλιστικό ιστορικό και βεβαιώνει την ασφαλιστική ικανότητα.

Ενιαίο Σύστημα Ελέγχου και Πληρωμών Συντάξεων ΕΣΕΠΣ - ΗΛΙΟΣ: Συγκεντρώνει όλα τα αρχεία πληρωμών συντάξεων των επιμέρους φορέων κάθε μήνα, τα ελέγχει για την ορθότητα τους και παράγει τα τελικά αρχεία για το σύστημα πληρωμών ΔΙΑΣ ώστε να πραγματοποιηθούν οι πληρωμές

Για την υποστήριξη των εφαρμογών της, η ΗΔΙΚΑ χρησιμοποιεί τις ακόλουθες υποδομές πληροφορικής:

Τεχνολογίες virtualization

- MS HyperV
- Oracle VM
- VMWare

Λειτουργικά συστήματα

- Oracle Enterprise Linux
- CentOS
- Solaris
- IBM AIX
- MS Windows (Server 2008, Server 2012, Server 2016)

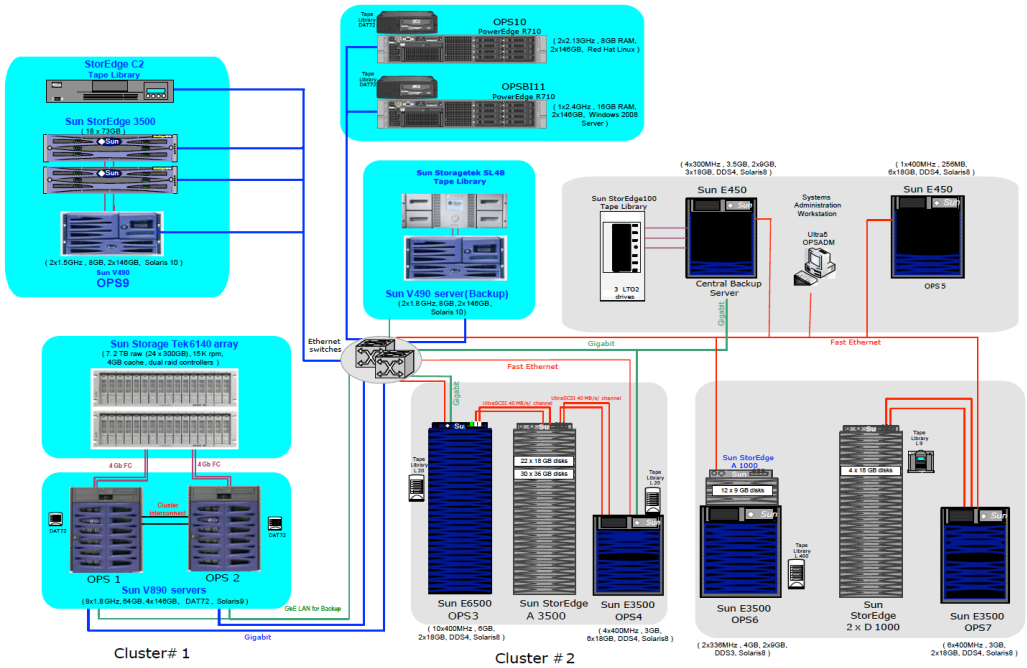
Υλικοτεχνική υποδομή

Η ΗΔΙΚΑ διαθέτει ένα σύγχρονο Κέντρο Δεδομένων (Data Center) που έχει κατασκευαστεί το 2015 το οποίο παρέχει υπηρεσίες φιλοξενίας δικτυακών υποδομών υψηλών προδιαγραφών εξασφαλίζοντας τη διαθεσιμότητα και την ασφάλεια τους και την παροχή υπηρεσιών νεφοϋπολογιστικλης νέφους (cloud computing) στους Φορείς Κοινωνικής Ασφάλισης, Πρόνοιας, Υγείας, το Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης και Κοινωνικής Αλληλεγγύης και τους λοιπούς φορείς που υποστηρίζει.

Διαθέτει 40 και πλέον RACKs που φιλοξενούν Εξυπηρετητές (Servers) (επί το πλείστον τεχνολογίας Blade Servers), SAN storages (FC-Fabric), Tape Backup Libraries, Network & Security systems, κλπ. Συνολικά διαθέτει πάνω από 170 Physical Servers και 320 Virtual Servers.

1.2.3.3 ΕΦΚΑ

Η ευσπευσμένη δημιουργία του ΕΦΚΑ δεν επέτρεψε την έγκαιρη ανάπτυξη ενός Ολοκληρωμένου Πληροφοριακού Συστήματος (ΟΠΣ) προσαρμοσμένου στις ιδιαίτερες ανάγκες του οργανισμού. Οι υποδομές ΤΠΕ του φορέα προήλθαν από αυτές που διέθεταν οι οργανισμοί κοινωνικής ασφάλισης οι οποίοι συγχωνεύτηκαν σε αυτόν. Αν και υπάρχουν σχέδια για την ανάπτυξη του ΟΠΣ-ΕΦΚΑ, στην παρούσα φάση οι πληροφοριακές λειτουργίες του φορέα εκτελού μέσω από την επιλογή, τροποποίηση και εκμετάλλευση των πληρέστερων από τα προϋπάρχοντα ΠΣ, σε συνδυασμό με συστήματα της ΗΔΙΚΑ. Ο κορμός των ΠΣ που χρησιμοποιεί ο νέος φορέας προέρχεται από το ΙΚΑ, το οποίο διέθετε το πλέον εκτενές ΟΠΣ.



Σχήμα 2 Αρχιτεκτονική της Κεντρικής Υπολογιστικής Υποδομής ΟΠΣ-ΕΦΚΑ

Εφαρμογές

Οι κυριότερες εφαρμογές που λειτουργεί ο ΕΦΚΑ είναι οι ακόλουθες:

Ενιαίο Μητρώο ΕΦΚΑ (Web Μητρώο): Το Ενιαίο Μητρώο Ασφαλισμένων (εν ενεργεία και συνταξιούχων) είναι η εφαρμογή Μητρώου που χρησιμοποιείται παράλληλα με τα Μητρώα των ενταχθέντων στον ΕΦΚΑ Φορέων, τα οποία και ομογενοποιεί. Στο Ενιαίο Μητρώο Ασφαλισμένων διατηρούνται τα δημογραφικά στοιχεία σε ελληνικά και λατινικά. Τα στοιχεία τηρούνται σε εξυπηρετητές της ΗΔΙΚΑ, ενώ η διαχείριση του μητρώου γίνεται μέσω διαδικτυακής εφαρμογής.

Συντάξεις: Οι διαδικασίες αίτησης συνταξιοδότησης, ηλεκτρονικής πρωτοκόλλησης και παρακολούθησης πορείας της αίτησης, καθώς και έκδοσης κύριων και προσωρινών συντάξεων βασίζονται στις υφιστάμενες διαδικασίες του ΟΠΣ ΙΚΑ-ΕΤΑΜ, με εξαίρεση τους ασφαλισμένους του Δημοσίου, του τ. ΟΓΑ και του τ.ΝΑΤ, οι οποίοι εξυπηρετούνται από τα ΠΣ των αντίστοιχων τέως ΦΚΑ, νυν τομέων. Η μηνιαία διαδικασία εκκαθάρισης συντάξεων γίνεται κυρίως από πληροφοριακά συστήματα του ΟΠΣ-ΙΚΑ, το Σύστημα Εκκαθάρισης τουΟΑΕΕ και το Σύστημα ΗΔΙΚΑ. Όπως

προαναφέρθηκε, η τελική πληρωμή των συντάξεων γίνεται μέσω του συστήματος ΕΣΕΠΣ/ΗΛΙΟΣ που διατηρεί η ΗΔΙΚΑ.

Εισφορές Μισθωτών-Απογραφή Εργοδοτών: Οι διαδικασίες για την απογραφή εργοδοτών και τη δήλωση των εισφορών των μισθωτών εργαζομένων υποστηρίζονται μηχανογραφικά από την υπηρεσία υποβολής Αναλυτικών Περιοδικών Δηλώσεων (ΑΠΔ) του ΟΠΣ ΙΚΑ

Εισφορές Μη Μισθωτών: Ο υπολογισμός των εισφορών των μη μισθωτών βασίστηκε στην αναβάθμιση του ΠΣ του τ.ΟΓΑ από την ΗΔΙΚΑ ΑΕ.

Παροχές: Οι παροχές ασθενείας σε χρήμα που καταβάλλει ο ΕΦΚΑ υποστηρίζονται από τα ΠΣ Παροχών που υπήρχαν και λειτουργούσαν στους φορείς που εντάχθηκαν στον ΕΦΚΑ μέχρι τη θέσπιση Ενιαίου Κανονισμού Ασφάλισης και Παροχών του ΕΦΚΑ και τη δημιουργία αντίστοιχου ΠΣς.

Οικονομική Διαχείριση: Για τη μηχανογραφική κάλυψη των εργασιών των οικονομικών υπηρεσιών του ΕΦΚΑ, χρησιμοποιείται το ΠΣ Οικονομικής Διαχείρισης του ΟΠΣ ΙΚΑ με τις απαραίτητες τροποποιήσεις λογισμικού εφαρμογών.

Διαχείριση Προσωπικού και Μισθοδοσίας: Η διαχείριση προσωπικού και μισθοδοσίας του ΕΦΚΑ, γίνεται με το Ολοκληρωμένο Πληροφοριακό Σύστημα Διαχείρισης Ανθρώπινου Δυναμικού «COMPASS».

*Σύστημα Κέντρου Είσπραξης Ανεξόφλητων Οφειλών (ΚΕΑΟ***)**: Πρόκειται για το μηχανογραφικό σύστημα που υποστηρίζει τις επιχειρησιακές ανάγκες λειτουργίας του ΚΕΑΟ.

Ιστότοπος και ηλεκτρονικές υπηρεσίες: Για την εξυπηρέτηση των πολιτών λειτουργεί ο ιστότοπος του ΕΦΚΑ (www.efka.gov.gr), στον οποίο παρέχονται επί 24ώρου βάσεως ενημερωτικές πληροφορίες και ηλεκτρονικές υπηρεσίες. Στον ιστότοπο υπάρχουν παραπομπές σε ηλεκτρονικές υπηρεσίες των πρώην ΦΚΑ και της ΗΔΙΚΑ, οι οποίες δεν έχουν ακόμα μεταφερθεί στις υποδομές του ΕΦΚΑ. Οι παλαιότερες Ηλεκτρονικές Υπηρεσίες, οι οποίες εξυπηρετούνται από την Υποδομή Internet είχαν χρησιμοποιήσει το Σύστημα Διαχείρισης Βάσεων Δεδομένων (RDBMS) SQL Server Standard SP1 της Microsoft. Οι νέες χρησιμοποιούν το Σύστημα Διαχείρισης Βάσεων Δεδομένων (RDBMS) Oracle, έκδοση 11g, ενώ το σχετικό Λογισμικό Εφαρμογών έχει

αναπτυχθεί με χρήση του Περιβάλλοντος Oracle Web Logic Suite. Ο ιστότοπος έχει αναπτυχθεί με χρήση του περιβάλλοντος Coldfusion version 5 Enterprise.

Υλικοτεχνική Υποδομή

Η κεντρική υπολογιστική υποδομή του ΕΦΚΑ αποτελείται από τις αντίστοιχες κεντρικές υποδομές των ενταχθέντων ΦΚΑ.

Κεντρικά Κέντρα Δεδομένων: Το κεντρικό Κέντρο Δεδομένων (Computer Room, CR) του ΕΦΚΑ λειτουργεί στο κτίριο της Γενικής Διεύθυνσης Πληροφορικής του οργανισμού στην οδό Παπαδιαμαντοπούλου. Διαθέτει εξειδικευμένα συστήματα ηλεκτρικής παροχής (κύριας και εφεδρικής), ψύξης, πυρανίχνευσης-πυρασφάλειας καθώς και όλα τα απαραίτητα χαρακτηριστικά ασφάλειας και φύλαξης. Μέρος κρίσιμων υποδομών λειτουργούν σε δεύτερο CR, σε κτίριο του ΕΦΚΑ, στην οδό Πατησίων 12. Επιπρόσθετα κεντρικές υποδομές του ΕΦΚΑ συνεχίζουν να λειτουργούν σε υποδομές των πρώην ΦΚΑ. Τέλος εφαρμογές που λειτουργούν από την ΗΔΙΚΑ ΑΕ για λογαριασμό του ΕΦΚΑ φιλοξενούνται στο CR της ΗΔΙΚΑ, το οποίο περιγράφηκε νωρίτερα.

Η κεντρική υπολογιστική υποδομή αποτελείται από:

- Unix-based και Windows-based Servers διαφόρων εκδόσεων
- Εγκαταστάσεις πλήθους προϊόντων Oracle
- Υποδομή Virtualization
- Πλατφόρμες και εργαλεία ανάπτυξης
- Υποδομές ασφάλειας (firewall, πλατφόρμα antivirus)
- Δικτυακό εξοπλισμό (router, switch)
- Υποδομή για τη κεντρική δημιουργία και διαχείριση των ψηφιακών υπογραφών
- Υποδομή λήψης αντιγράφων ασφάλειας
- Υποδομή αποθήκευσης δεδομένων.

Ενοποιημένο Περιβάλλον Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών: Στον Εξυπηρετητή του Ενοποιημένου Περιβάλλοντος τηρούνται επιμέρους αντίγραφα

των δεδομένων της Κεντρικής Υπολογιστικής Υποδομής και εγκαθίστανται τα αντικείμενα Λογισμικού, τα οποία είναι σε φάση ελέγχου από τα στελέχη του ΕΦΚΑ, πριν την τελική εγκατάσταση αυτών στο περιβάλλον παραγωγής.

Ενοποιημένο Περιβάλλον τοπικού δικτύου (domain) της Κεντρικής Υπηρεσίας ΚΕΑΟ: Στο Ενοποιημένο Περιβάλλον του τοπικού δικτύου της Κεντρικής Υπηρεσίας ΚΕΑΟ συνδέονται σταθμοί εργασίας, με σκοπό την κοινή χρήση των μέσων (εκτυπωτών) και την ανταλλαγή πληροφοριών (κοινή χρήση αρχείων και φακέλων μέσω του δικτύου). Ο Server παρέχει τους κοινόχρηστους πόρους στο τοπικό δίκτυο.

Ασφαλής Διάταξη Δημιουργίας Υπογραφής/Κεντρικό ΑΔΔΥ: Πρόκειται για την ασφαλή διάταξη ARX Cosign Central FIPS v 7.1, η οποία έχει πιστοποιηθεί κατά ETSI TS 14167-5/Common Criteria EAL4+ καθώς και από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων ότι καλύπτει τις απαιτήσεις των ασφαλών διατάξεων δημιουργίας υπογραφής.

Στο Κεντρικό ΑΔΔΥ βρίσκονται αποθηκευμένα αναγνωρισμένα ψηφιακά πιστοποιητικά για τους υπαλλήλους του ΕΦΚΑ, τα οποία έχουν εκδοθεί από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)-ΕΡΜΗΣ. Η διαχείριση χρηστών στο κεντρικό ΑΔΔΥ έχει ολοκληρωθεί με τη διαχείριση χρηστών του ΕΦΚΑ (χρήστες εφαρμογής ΟΠΣ Μισθωτών και χρήστες της εφαρμογής ηλεκτρονικών καταθέσεων εις χείρας πιστωτικών ιδρυμάτων).

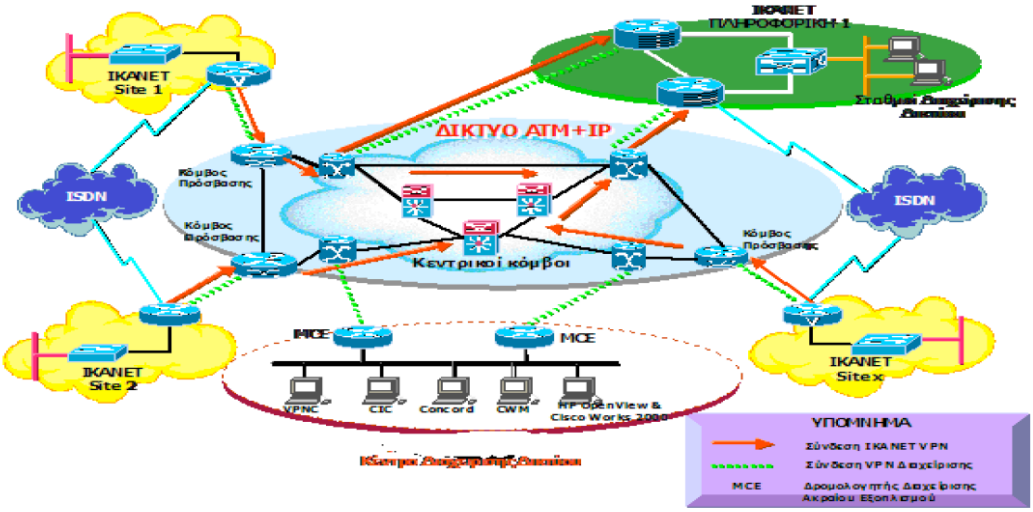
*Πλατφόρμα αυθεντικοποίησης με κωδικό πρόσβασης μιας χρήσης (OTP)***:** Πρόκειται για την πλατφόρμα LinOTP v2.8, η οποία επικοινωνεί με το Κεντρικό ΑΔΔΥ μέσω του τυποποιημένου πρωτόκολλου RADIUS, παρέχοντας τη δυνατότητα επέκτασης της πιστοποίησης χρηστών του Cosign με χρήση Ελέγχου Ταυτότητας Δύο Παραγόντων - Κωδικού Πρόσβασης Μιας Χρήσης (*Two Factor Authentication – One Time Passwords (OTP)*)

*Δίκτυο Ευρείας Περιοχής (Wide Area Network-WAN)***:** Το δίκτυο λειτουργεί ως ένα ενός Εικονικό Ιδιωτικό Δίκτυο (*Virtual Private Network, VPN*) πολλαπλών υπηρεσιών (διακίνηση δεδομένων, φωνής και εικόνας), συνδέοντας όλες τις Διοικητικές Μονάδες του ΕΦΚΑ Μισθωτών (Περιφερειακές, Τοπικές, Παραρτήματα) με τις Κεντρικές Υπηρεσίες του ΕΦΚΑ, ενώ σταδιακά και άλλες υπηρεσίες συνδέονται με αυτό. Το δίκτυο είναι τεχνολογίας IP-VPN. Η αρχιτεκτονική του δικτύου έχει ως εξής:

• Επίπεδο κορμού (Backbone)

• Επίπεδο Διανομής (Distribution)

• Επίπεδο Πρόσβασης (Access).



Σχήμα 3 Απεικόνιση δικτύου WAN ΕΦΚΑ

Σύζευξις: Πρόκειται για εθνικό δίκτυο της δημόσιας διοίκησης, το οποίο προσφέρει ευρυζωνικές υπηρεσίες δικτύου και διακίνησης Φωνής-Εικόνας-Δεδομένων σε φορείς του ελληνικού δημοσίου. Περιφερειακές και κεντρικές υπηρεσίες του ΕΦΚΑ συνδέονται στο δημόσιο δίκτυο Σύζευξις, αξιοποιώντας τις υπηρεσίες που αυτό προσφέρει.

1.2.3.4 ΕΤΕΑΕΠ

Όπως και στην περίπτωση του ΕΦΚΑ, το ΕΤΕΑΕΠ χρησιμοποιεί τα πληροφοριακά συστήματα των οργανισμών οι οποίοι συγχωνεύτηκαν σε αυτό.

Εφαρμογές

Εσοδα-Έλεγχος-Ασφάλιση-Απονομές: Για την πλειοψηφία των αναγκών του το ΕΤΕΑΕΠ χρησιμοποιεί το Πληροφοριακό Σύστημα του ΤΕΑΥΕΚ.

Πληρωμή Συντάξεων: Για την πληρωμή συντάξεων χρησιμοποιούνται τα συστήματα των επιμέρους ταμείων

Υλικοτεχνική Υποδομή

Το υλικό του ΠΣ του ΕΤΕΑΕΠ αποτελείται από servers σε περιβάλλοντα Linux και Windows, αποθηκευτικά μέσα και 133 σταθμούς εργασίας σε περιβάλλον Windows.

1.2.3.5 Διαλειτουργικότητα με Δημόσια Πληροφοριακά Συστήματα

Η διαλειτουργικότητα των ηλεκτρονικών συστημάτων των δημόσιων οργανισμών μπορεί να παραμένει ένα ζητούμενο και πεδίο με σημαντικά περιθώρια ανάπτυξης, αλλά έχουν ήδη γίνει βήματα σε αυτή την κατεύθυνση. Η σημαντικότερη διασύνδεση των πληροφοριακών συστημάτων των ΦΚΑ είναι με την Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ) και το μητρώο ταυτοτήτων της Ελληνικής Αστυνομίας.

Η διασύνδεση με την Αστυνομία δίνει στοιχεία ταυτότητας, διαβατηρίου, και σε ορισμένες περιπτώσεις στοιχεία των αλλοδαπών ασφαλισμένων. Έτσι ο ΕΦΚΑ μπορεί να βεβαιώσει εάν η ταυτότητά που δηλώνει ο ασφαλισμένος είναι ενεργή, δηλωμένη χαμένη, κλεμμένη κλπ.

Η διαλειτουγικότητα με τη ΓΓΠΣ έχει πολλές εφαρμογές:
Λειτουργία ταυτοποίησης για όλους τους ασφαλισμένους και συνταξιούχους που κάνουν χρήση των ηλεκτρονικών υπηρεσιών καθώς και τους εργοδότες και επιχειρήσεις
Υπολογισμός των ασφαλιστικών εισφορών των μη μισθοτών απευθείας από τα εισοδήματα που στέλνει η ΓΓΠΣ (δ4)

Στο μέλλον προβλέπεται να υπάρξει ενιαίος υπολογισμός Οφειλών προς Ασφαλιστική και Φορολογική Διοίκηση.

2. Η έννοια του προσωπικού δεδομένου και το ρυθμιστικό νομικό του πλαίσιο στην Ελλάδα

2.1 Η έννοια της ιδιωτικότητας

Η ιστορία των προσωπικών δεδομένων μπορεί να αναχθεί στην έννοια της διάκρισης του ιδιωτικού από το δημόσιο, η οποία συναντάται για πρώτη φορά στον Αριστοτέλη (Ηθικά Νικομάχεια), ο οποίος αναφέρεται στην "…απόσταση, χώρο και απομόνωση από τη δημόσια ζωή", οριοθετώντας έτσι μια σφαίρα του βίου ξεχωριστή από την τελευταία. Η σύγχρονη έννοια της ιδιωτικότητας εντοπίζεται για πρώτη φορά στη φιλελεύθερη παράδοση από στοχαστές όπως ο John Stuart Mills, ο οποίος στο έργο του Περί Ελευθερίας θέτει τη διάκριση ανάμεσα στο δημόσιο ως το πεδίο δράσης της κρατικής εξουσίας και το ιδιωτικό ως το πεδίο της αυτορρύθμισης (DeCew, 2018). Η διάκριση αυτή βρίσκεται και στον John Locke, ο οποίος θεώρησε πως στη φυσική κατάσταση τα πάντα είναι δημόσια. Εντόπισε την ιδιωτική σφαίρα στην ιδιοκτησία από κάθε άτομο του ίδιου του εαυτού του και της εργασίας του, μέσω της οποίας μπορεί να ιδιοποιηθεί άλλα αγαθά.

Αναφορικά με την προστασία της ιδιωτικότητας, η πρώτη σύγχρονη σοβαρή εξέλιξη εντοπίζεται στη δημοσίευση του άρθρου "The right to privacy" των Αμερικανών δικαστών του Ανωτάτου Δικαστηρίου Louis Brandeis και Samuel Warren (1890). Για πρώτη φορά αναγνώρισαν το "δικαίωμα του να μην δέχεσαι οχλήσεις" (The right to be left alone), η προστασία του οποίου υποστήριξαν πως βασιζόταν στην αρχή του "απαραβίαστου της προσωπικότητας" (inviolate personality) . Σημαντική αφορμή για το κείμενο τους ήταν οι τεχνολογικές εξελίξεις στα Μέσα Μαζικής Ενημέρωσης (ΜΜΕ) της εποχής με την ανάπτυξη της φωτογραφίας και την μείωση του κόστος εκτύπωσης και συνεπαγόμενη διάδοση των εφημερίδων. Οι Brandeis και Warren θεώρησαν πως οι νέες δυνατότητες των ΜΜΕ δημιουργούσαν την ανάγκη να διατυπωθεί ξεκάθαρα το δικαίωμα της προστασίας της ιδιωτικότητας. Από το ξεκίνημα της λοιπόν η έννοια της ιδιωτικότητας συνδέθηκε με την εξέλιξη της τεχνολογίας.

Το 1948 το άρθρο 12 της «*Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα*» ανάφερε πως «Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε

προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους,» αποτελώντας ένα σημαντικό βήμα για την προστασία της ιδιωτικής ζωής από παρεμβάσεις. Το 1950 η «*Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου*» με το άρθρο 8 θέσπισε το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής των πολιτών, της κατοικίας και της αλληλογραφίας τους, θέτοντας περιορισμούς στο δικαίωμα επέμβασης του δημοσίου σε αυτές. Και στα δύο κείμενα γίνεται αναφορά στην αλληλογραφία και έτσι αποτελούν από τις πρώτες εκφάνσεις νομικής προστασίας μιας συγκεκριμένης μορφής ιδιωτικότητας, της ιδιωτικότητας των πληροφοριών.

Ως προς τις μορφές αυτές τις ιδιωτικότητας, υπάρχουν αρκετές κατηγοριοποιήσεις. Η κατηγοριοποίηση των Anton-Earp (Massey, A. & Antón, A., 2008) χρησιμοποιεί ως κριτήρια το πως προστατεύεται η ιδιωτικότητα, όπως γνώση της κατεργασίας και επιλογή διάθεσης δεδομένων, και ποιες είναι οι απειλές για την τελευταία, όπως η αποθήκευση των πληροφοριών. Σε παρόμοιους δρόμους η κατηγοριοποίηση του Solove (2006) στηρίζεται στον εντοπισμό δραστηριοτήτων που ενέχουν κινδύνους για την ιδιωτικότητα.

Για τους σκοπούς αυτής της εργασίας θα παρουσιαστεί η κατηγοριοποίηση του Rosenberg (1992) η οποία εντοπίζει τέσσερεις εκφάνσεις της ιδιωτικότητας:

Ιδιωτικότητα Πληροφοριών (Informational Privacy): αφορά τα προσωπικά δεδομένα ενός προσώπου και τον τρόπο που αυτά μπορούν να συγκεντρωθούν, να αποθηκευτούν, να επεξεργαστούν ή να διαδοθούν.

Εδαφική Ιδιωτικότητα (Territorial Privacy): Αναφέρεται στην προστασία του φυσικού χώρου που περιβάλλει ένα άτομο, τόσο την κατοικία όσο και άλλα περιβάλλοντα, όπως ο εργασιακός ή ο δημόσιος χώρος.

Σωματική Ιδιωτικότητα (Bodily Privacy): αφορά στην προστασία ενός ατόμου από αδικαιολόγητες παρεμβάσεις που σχετίζονται με την φυσική του υπόσταση όπως ο σωματικός έλεγχος, η υποχρεωτική υποβολή σε εξέταση/επέμβαση, σε δοκιμή φαρμάκων και η διακίνηση πληροφοριών που παραβιάζουν την ηθική αίσθηση του ατόμου.

Επικοινωνιακή ιδιωτικότητα (Communication Privacy): αφορά την προστασία από μη εξουσιοδοτημένη παρακολούθηση της επικοινωνίας ενός προσώπου.

2.2 Από την ιδιωτικότητα στα προσωπικά δεδομένα

Η ανάπτυξη της πληροφορικής και η αυτοματοποίηση της καταχώρησης στοιχείων, η οποία επέτρεψε την μαζική επεξεργασία δεδομένων δημιούργησαν νέους κινδύνους για την έννοια της ιδιωτικής ζωής και την προστασία της ιδιωτικότητας. Η λέξη «δεδομένα» (*Data*) σημασιοδοτήθηκε και καθιερώθηκε σε συνάρτηση με την ανάπτυξη της αυτοματοποιημένης επεξεργασίας δεδομένων. Τα «δεδομένα» προσδιορίζονται ως στοιχεία της πληροφορίας που έγινε αντικείμενο αυτοματοποιημένης επεξεργασίας, σε βαθμό που οι έννοιες «δεδομένα» και «πληροφορία» να έχουν καταστεί ουσιαστικά συνώνυμες (Μήτρου, 2006).

Αρχικά, τα υπολογιστικά συστήματα χρησιμοποιήθηκαν σε πανεπιστημιακά περιβάλλοντα για ερευνητικούς σκοπούς και η περιορισμένη αυτή χρήση σε συνδυασμό με τη μικρή ισχύ τους δεν δημιουργούσε κινδύνους για την ιδιωτικότητα του πολίτη. Από τα μέσα της δεκαετίας του ‘60 όμως οι υπολογιστές ξεκίνησαν να εισέρχονται στη δημόσια διοίκηση με σκοπό την καλύτερη διαχείριση των αρχείων. Αυτή η εξέλιξη δημιούργησε και τις πρώτες ανησυχίες για τους κινδύνους που επέσειε για την ιδιωτικότητα η μαζική επεξεργασία προσωπικών δεδομένων που επέτρεπε η νέα τεχνολογία. Ένα από τα πρώτα κείμενα που ασχολήθηκε με τα προβλήματα αυτά ήταν η απόφαση 2450/19.12.1968 της Γενικής Συνέλευσης του ΟΗΕ (Αλεξανδροπούλου-Αιγυπτιάδου 2002 σελ. 48) η οποία επεσήμανε τις ανησυχίες που προέκυπταν από τις τεχνολογικές και επιστημονικές εξελίξεις ανάμεσα σε άλλα για την ιδιωτικότητα των ατόμων και έθετε προς μελέτη τα όρια που πρέπει να τίθενται στη χρήση των ηλεκτρονικών συστημάτων σε μια δημοκρατική κοινωνία προκειμένου να μην καταπατούνται τα ατομικά δικαιώματα. Η πρώτη νομοθεσία η οποία ασχολήθηκε και έθεσε προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα εμφανίστηκε στο γερμανικό ομόσπονδο κρατίδιο της Έσσης ενώ το 1973 η Σουηδία εισήγαγε σχετική νομοθεσία σε εθνικό επίπεδο.

Το πιο επιδραστικό όμως κείμενο της περιόδου ήταν ο «Κώδικας Θεμιτών Πρακτικών στη Διαχείριση της Πληροφορίας» (Αγγλικά: Code of Fair Information Practices) τον οποίο συνέταξε το 1972 στις ΗΠΑ μια συμβουλευτική επιτροπή του Υπουργείου Υγείας, Παιδείας και Πρόνοιας. (Welfare. Secretary's Advisory Committee on Automated Personal Data Systems, 1973). Ο Κώδικας της επιτροπής έθεσε πέντε αρχές για την θεμιτή διαχείριση των προσωπικών δεδομένων:

1. Τα συστήματα καταγραφής-αρχειοθέτησης πληροφοριών δεν πρέπει να είναι κρυφά
2. Το άτομο πρέπει να γνωρίζει τις πληροφορίες που το αφορούν και έχουν καταγραφεί καθώς και το πως αυτές θα χρησιμοποιηθούν
3. Πρέπει να υπάρχει τρόπος το άτομο να εμποδίσει τη χρήση πληροφοριών που το αφορούν χωρίς τη συγκατάθεση του για σκοπό άλλο από αυτόν για τον οποίο δόθηκαν
4. Πρέπει να υπάρχει τρόπος ώστε το άτομο να μπορεί να διορθώσει ή μεταβάλλει μια εγγραφή δεδομένων η οποία μπορεί να το ταυτοποιήσει
5. Κάθε οργανισμός ο οποίος δημιουργεί, τηρεί, χρησιμοποιεί ή διαδίδει αρχεία ταυτοποιήσιμων προσωπικών δεδομένων πρέπει να εγγυάται την αξιοπιστία των δεδομένων για την χρήση για την οποία προορίζονται και να λαμβάνει τα κατάλληλα μέτρα για να εμποδίζει την κατάχρηση των δεδομένων αυτών.

Ο κώδικας αυτός αποτέλεσε τη βάση του Freedom of Information Act των ΗΠΑ. Το 1980 ο ΟΟΣΑ εξέδωσε τις λεγόμενες «*Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων*», το οποίο ακολούθησε σε γενικές γραμμές τις αρχές που είχε θέσει ο Κώδικας και έθεσε επτά αρχές. Ο, ελάχιστος, αυτός κώδικας υιοθετήθηκε από πολλές χώρες και αποτέλεσε πρότυπο για μετέπειτα νομοθεσίες σχετικά με τα προσωπικά δεδομένα.

2.3 Αρχές Ασφάλειας και Ιδιωτικότητας Δεδομένων

Οι γενικές αρχές της ασφάλειας και ιδιωτικότητας των πληροφοριών και δεδομένων είναι οι ακόλουθες (Γκρίτζαλης, 2004):

Εμπιστευτικότητα (Confidentiality): Η διασφάλιση πως η πληροφορία δεν είναι διαθέσιμη σε ή προσβάσιμη από μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες

Διαθεσιμότητα (Availability): Αναφέρεται στην ανάγκη να είναι διαρκώς διαθέσιμη η πληροφορία όταν χρειάζεται

Ακεραιότητα (Integrity) Αφορά την προστασία της ακρίβειας και της πληρότητας των δεδομένων και επομένως την προστασία τους από μη εξουσιοδοτημένη ή καταγεγραμμένη τροποποίηση

Αυθεντικότητα (Authenticity): Αναφέρεται στη διασφάλιση της ταυτότητας κάθε εμπλεκόμενης οντότητας

Μη Αποποίηση (Non Repudiation): Μια κατα βάση νομική έννοια που εννοεί πως σε ένα ασφαλές σύστημα ένα εμπλεκόμενο μέρος δεν πρέπει να δύναται να αρνηθεί πως πραγματοποίησε μια δραστηριότητα. Προϋποθέτει την Αυθεντικότητα

Για την μετατροπή της ιδιωτικότητας από μία γενική έννοια σε τεχνική απαίτηση έχουν ορισθεί οι επιμέρους απαιτήσεις ιδιωτικότητας (Καλλονιάτης, 2011) :

Αυθεντικοποίηση (Authenticity): η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας. Αποτελεί κυρίως απαίτηση ασφάλειας, παρά ιδιωτικότητας ενός ΠΣ.

Εξουσιοδότηση (Authorization): η διαδικασία μέσω της οποίας μία οντότητα αποκτά δικαιώματα - πρόσβαση σε συγκεκριμένες λειτουργίες και δεδομένα ενός πληροφοριακού συστήματος.

Αναγνώριση (Identification): η διαδικασία μέσω της οποία ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.

Προστασία Δεδομένων (Data Protection): Η τήρηση, σύμφωνα και με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ, των ακόλουθων αρχών:

- Αρχή της νομιμότητας και της δικαιοσύνης.
- Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν.
- Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων.
- Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων.
- Αρχή της ασφάλειας και της ακεραιότητας.

- Εποπτεία και Επικύρωση.

Ανωνυμία (Anonymity): η διαδικασία μέσω της οποίας διασφαλίζεται η χρήση μιας υπηρεσίας ή η επικοινωνία με άλλους χρήστες χωρίς να αποκαλύπτεται η ταυτότητά του χρήστη

Ψευδωνυμία (Pseydonymity): η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση μιας οντότητας από μη εξουσιοδοτημένες τρίτες οντότητες με τη χρήση ενός ψευδώνυμου για την προστασία της ταυτότητας.

Μη-συνδεσιμότητα (Unlinkability): η προστασία της ιδιωτικότητας μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, που θα μπορούσαν να οδηγήσουν στην αποκάλυψη της ταυτότητάς της.

Μη-παρατηρησιμότητα (Unobservability): η προστασία της ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους μέσω της απαγόρευσης παρατήρησης της ή εντοπισμού των ιχνών της.

2.4 Νομικό πλαίσιο προστασία προσωπικών δεδομένων

Η ανάπτυξη της προστασίας της ιδιωτικότητας συνδέθηκε με αυτή της προστασίας των προσωπικών δεδομένων ύστερα από την ανάπτυξη των πληροφοριακών συστημάτων και του διαδικτύου, τα οποία δημιούργησαν νέους κινδύνους για τον ιδιωτικό χώρο του ατόμου, την ελευθερία του να αναπτύσσει απρόσκοπτα την προσωπικότητά του και την αυτονομίας του να διαμορφώνει και να απολαμβάνει τις σχέσεις του με τους οικείους του, καθώς και τις επιλογές εκείνες μέσα από τις οποίες τελικά αυτοπροσδιορίζεται.

2.4.1 Κατευθυντήριες Αρχές που διέπουν την Προστασία της Ιδιωτικότητας

Εμπνευσμένες από τον «*Κώδικα Θεμιτών Πρακτικών στη Διαχείριση της Πληροφορίας*», οι βασικές αρχές που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων που όρισε ο ΟΟΣΑ το 1980 (OECD 1980) αποτέλεσαν τη βάση για μια σειρά από εθνικές, και όχι μόνο, νομοθεσίες σχετικά με την επεξεργασία και διακίνηση των προσωπικών δεδομένων και την ιδιωτικότητα. Οι αρχές αυτές είναι:

Αρχή του περιορισμού της συλλογής (Collection Limitation Principle): Θα πρέπει να υπάρχουν όρια στη συλλογή προσωπικών δεδομένων, η συλλογή τους θα πρέπει να γίνεται με χρήση σύννομων και θεμιτών μέσων και, στις περιπτώσεις που είναι δυνατόν, με τη συναίνεση ή την ενημέρωση του υποκείμενου των δεδομένων.

Αρχή της ποιότητας των δεδομένων (Data Quality Principle): Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με τους σκοπούς για τους οποίους προορίζονται να χρησιμοποιηθούν ενώ – στο βαθμό που είναι απαραίτητο για το σκοπό αυτό – θα πρέπει να είναι πλήρη, ακριβή και ενημερωμένα.

Αρχή του προσδιορισμού του σκοπού (Purpose Specification Principle): Οι σκοποί για τους οποίους συλλέγονται τα προσωπικά δεδομένα θα πρέπει να προσδιορίζονται κατά τη χρονική στιγμή της συλλογής τους, ενώ η συνακόλουθη χρήση τους θα πρέπει να περιορίζεται στην εκπλήρωση των σκοπών αυτών ή κάποιων άλλων που προσομοιάζουν.

Αρχή του περιορισμού της χρήσης (Use Limitation Principle): Τα προσωπικά δεδομένα δε θα πρέπει να κοινοποιούνται ή γενικά να χρησιμοποιούνται για άλλο σκοπό εκτός από τον προσδιορισμένο, εκτός εάν

- υπάρχει η σχετική συναίνεση του χρήστη ή
- νομική εξουσιοδότηση.

Αρχή των εγγυήσεων ασφάλειας (Security Safeguards Principle): Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με χρήση κατάλληλων εγγυήσεων ασφάλειας απέναντι σε κινδύνους όπως η απώλεια, η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση.

Αρχή της διαφάνειας (Openness Principle): Θα πρέπει να υπάρχει μια γενική πολιτική διαφάνειας αναφορικά με τις εξελίξεις, τις πρακτικές και τις πολιτικές που σχετίζονται με τη συλλογή και επεξεργασία των προσωπικών δεδομένων. Θα πρέπει να υπάρχουν άμεσα διαθέσιμοι τρόποι εξακρίβωσης της ύπαρξης, της φύσης και της συνήθους χρήσης των δεδομένων καθώς και την ταυτότητα και έδρα του υπεύθυνου επεξεργασίας.

Αρχή της ατομικής συμμετοχής (Individual Participation Principle): Το κάθε άτομο θα πρέπει να έχει το δικαίωμα:

- Να αποκτά είτε απ' ευθείας από τον υπεύθυνο της επεξεργασίας είτε με άλλο τρόπο, επιβεβαίωση αναφορικά με το αν ο υπεύθυνος της επεξεργασίας διαθέτει δεδομένα που σχετίζονται με αυτο.

- Να του ανακοινώνονται δεδομένα που σχετίζονται με αυτό μέσα σε εύλογο χρονικό διάστημα, με εύλογο κόστος, με εύλογο τρόπο και σε μορφή που του είναι κατανοητή

- Να του παρέχεται αιτιολόγηση εφόσον απορριφθούν αιτήσεις του σχετικες με τις δύο παραπάνω παραγράφους και να διατηρεί στην περίπτωση αυτή τη δυνατότητα ένστασης.

- Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτό, και, σε περίπτωση επιτυχημένης ένστασης, να μπορεί να προχωρεί σε εξάλειψη, διόρθωση ή ολοκλήρωση ή τροποποίηση των δεδομένων αυτών.

Αρχή της ευθύνης (Accountability Principle): Κάθε υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να είναι υπόλογος για την συμμόρφωση με τα μέτρω εκείνα που προάγουν τις παραπάνω αρχές.

2.4.2 Ευρωπαϊκή Οδηγία 1995/46/ΕΚ

Ακολουθώντας σε γενικές γραμμές τις κατευθύνσεις του ΟΟΣΑ, Η Ευρωπαϊκή Οδηγία 1995/46/ΕΚ αποτέλεσε το νομοθέτημα με το οποίο εναρμονίστηκε η νομοθεσία των κρατών-μελών της ΕΕ, μεταξύ των οποίων και η Ελλάδα. Όπως διαφάνηκε από το Άρθρο 1, οι προβλέψεις της κινήθηκαν σε γενικές γραμμές σε δύο κατευθύνσεις. Καταρχάς προς την προστασία του ατόμου και των δικαιωμάτων του από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Όντας ένα κείμενο της ΕΕ όμως, έδωσε βάρος και στη λειτουργία και ολοκλήρωση της ενιαίας αγοράς με την θέσπιση όρων για την διακίνηση των δεδομένων εντός αυτής.

Η οδηγία ορίζει ως εξής τις προϋποθέσεις ώστε να είναι νόμιμη η επεξεργασία δεδομένων:

- Το υποκείμενο των δεδομένων έχει δώσει ρητή άδεια να επεξεργαστεί κάποιος τα δεδομένα του.

- Απαιτείται επεξεργασία δεδομένων για την εκτέλεση μιας υπηρεσίας με σκοπό την ικανοποίηση αιτήματος του υποκειμένου των δεδομένων.
- Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα θα πρέπει να έχει συμφωνήσει ρητά για τη χρήση αυτής της υπηρεσίας.
- Η επεξεργασία δεδομένων απαιτείται για την ολοκλήρωση μιας διαδικασίας για το δημόσιο συμφέρον ή κατόπιν αιτήματος δημόσιας αρχής.

Η οδηγία επίσης διακρίνει ειδικές κατηγορίες δεδομένων τα οποία εμπίπτουν σε αυστηρότερες προϋποθέσεις επεξεργασίας. Καθορίζει τα δικαιώματα του προσωπου στο οποίο αναφέρονται τα δεδομένα ως προς την ενημέρωση περί αυτών, την πρόσβαση και την αντίταξη. Στα πλαίσια της λειτουργίας της ενιαίας αγοράς, ρυθμίζει την διαβίβαση των προσωπικών δεδομένων σε τρίτες χώρες ενώ προβλέπει τη λειτουργία, σε κάθε χώρα, μιας αρχής ελέγχου για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Αναφορικά με την τήρηση των δεδομένων, τα πλέον σχετικά εδάφια είναι το Άρθρο 6 για τις αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων και το Τμήμα VII περί του Απόρρητου και Ασφάλειας της Επεξεργασίας. Ως προς την ποιότητα, προβλέπονται πέντε αρχές:

1. Σύννομη και θεμιτή επεξεργασία
2. Συλλογή για καθορισμένους, σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς, με κάποιες εξαιρέσει για μεταγενέστερη επεξεργασία για ιστορικούς, στατιστικούς ή επιστημονικούς σκοπούς
3. Τα δεδομένα να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς της συλλογής και επεξεργασίας (*Αρχή της ποιότητας των δεδομένων)*
4. Να είναι ακριβή και, εφόσον χρειάζεται, να ενημερώνονται. Αναφέρεται ρητά πως πρέπει να λαμβάνονται όλα τα εύλογα μέτρα ώστε δεδομένα ανακριβή ή ελλιπή να διαγράφονται ή να διορθώνονται

5. Να διατηρούνται με μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται μόνο κατά τη διάρκεια περιόδου που δεν υπερβαίνει την απαιτούμενη για την επίτευξη των σκοπών για τους οποίους έχουν συλλεγεί ή για τους οποίους αργότερα υφίστανται επεξεργασία.

Ως προς το απόρρητο και ασφάλεια της επεξεργασίας, το Άρθρο 16 επιτρέπει την επεξεργασία μόνο κατά ρητή εντολή του υπεύθυνου της επεξεργασίας. Για την ασφάλεια, το άρθρο 17 ορίζει πως ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση. Αναφέρεται πως τα μέτρα ασφάλειας πρέπει να εξασφαλίζουν, λαμβάνοντας υπόψη την τεχνολογία και το κόστος, επίπεδο ασφάλειας ανάλογο με τους κινδύνους που απορρέουν. Επιπλέον, ο υπεύθυνος της επεξεργασίας οφείλει να επιλέγει για την εκτέλεση της επεξεργασίας πρόσωπα τα οποία παρέχουν επαρκείς εγγυήσεις όσον αφορά τα μέτρα τεχνικής ασφάλειας και οργάνωσης της επεξεργασίας και να εξασφαλίζει την τήρηση των μέτρων αυτών.

Τέλος, το άρθρο επιτρέπει την επεξεργασία από τρίτους μόνο κατόπιν σύμβασης, ενώ οι όποιες νόμιμες υποχρεώσεις βαρύνουν και τον εκτελούντα την επεξεργασία. Παρά τις παραπάνω αναφορές όμως το άρθρο δεν υπεισέρχεται σε επιπλέον λεπτομέρειες ως προς τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας, αφήνοντας τα στη διακριτική ευχέρεια των κρατών-μελών.

2.4.3 Νόμος 2472/97

Στην ελληνική έννομη τάξη τα προσωπικά δεδομένα προστατεύονται και συνταγματικά από το άρθρο 9Α, το οποίο προστέθηκε κατά την αναθεώρηση του 2001. Η Ελλάδα κατά την εισαγωγή της Οδηγία 1995/46/ΕΚ όμως ήταν, μαζί με την Ιταλία, τα μόνα κράτη-μέλη της ΕΕ που δεν διέθεταν εθνική νομοθεσία για την προστασία των προσωπικών δεδομένων. Ως εκ τούτου, υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική στο εσωτερικό δίκαιο (Μήτρου, 2010). Το κείμενο που ψηφίστηκε ήταν ο νόμος 2472/97 (ΦΕΚ Α' 50/10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ακολούθησε νόμο 3471/06 (ΦΕΚ Α' 133/28.06.2006) που – εκτός των τροποποιήσεων που επέφερε στον Ν. 2472/97 – αφορούσε στην προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Όπως αναφέρει το Άρθρο 1 του νόμου, αντικείμενο του είναι «η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.» Ο νομοθέτης οριοθετεί με ουσιαστικούς, οργανωτικούς, διαδικαστικούς και κυρωτικούς κανόνες τη συνταγματικά ανεκτή επεξεργασία προσωπικών δεδομένων και με τον τρόπο αυτό ρυθμίζει τη ροή των προσωπικών δεδομένων στο πλαίσιο του κράτους, της οικονομίας και της κοινωνίας και οργανώνει τις πληροφοριακές σχέσεις μεταξύ των προσώπων (Μήτρου, 2010).

Ο νόμος περιέχει τον πρώτο ορισμό της έννοιας του προσωπικού δεδομένου στην ελληνική έννομη τάξη. Ως τέτοιο ορίζεται «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων». Ο νόμος όμως διακρίνει μια ξεχωριστή κατηγορία προσωπικών δεδομένων, τα οποία χαρακτηρίζει ως *ευαίσθητα δεδομένα*. Πρόκειται για «τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων», όπως τροποποιήθηκε ο σχετικός ορισμός με τον ν. 3471/2006.

Το πλαίσιο κανόνων που προβλέπει ο νόμος κινείται σε τρεις κατευθύνσεις:

1. Περιλαμβάνει ένα σύνολο ουσιαστικών ρυθμίσεων που θέτει τις προϋποθέσεις νομιμότητας της επεξεργασίας
2. Απονέμει δικαιώματα στα άτομα ως προς τα προσωπικά τους δικαιώματα
3. Εισάγει ένα θεσμικό πλαίσιο, ανάμεσα τους και την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), ώστε να εξασφαλίζεται η εφαρμογή της νομοθεσίας.

Ως προς την τήρηση των δεδομένων από τους οργανισμούς κοινωνικής ασφάλισης, ιδιαίτερο ενδιαφέρον έχουν τα Άρθρα 5 και 7. Όπως και στην Οδηγία 1995/46/ΕΚ, η επεξεργασία επιτρέπεται μόνο με τη συγκατάθεση του υποκειμένου, ενώ το άρθρο 7 το οποίο ασχολείται με τα ευαίσθητα δεδομένα απαγορεύει πλήρως την

συλλογή και επεξεργασία τους. Όμως και τα δύο άρθρα προβλέπουν εξαιρέσεις υπέρ του Δημοσίου. Το άρθρο 4 επιτρέπει την επεξεργασία χωρίς τη συγκατάθεση εφόσον η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο. Όσο για το Άρθρο 7, επιτρέπει την επεξεργασία για θέματα υγείας από σχετικό πάροχο ενώ με μεταγενέστερη προσθήκη με τον ν. 3156/2003 επιτρέπεται η επεξεργασία ευαίσθητων προσωπικών δεδομένων από Δημόσια αρχή για την άσκηση δημόσιου φορολογικού ελέγχου ή **δημόσιου ελέγχου κοινωνικών παροχών.**

Ο νόμος δεν απαλλάσσει πάντως τους δημόσιους οργανισμούς γενικότερα από την υποχρέωση γνωστοποίησης της τήρησης αρχείου και την αίτηση άδειας σε περίπτωση που το αρχείο αυτό περιλαμβάνει προσωπικά δεδομένα. Ιδιαίτερη αδειοδότηση απαιτεί και η διασύνδεση αρχείων εφόσον κάποιο περιέχει ευαίσθητα δεδομένα. Ο νόμος πάντως έθεσε τις προϋποθέσεις για την διασύνδεση των αρχείων, διαδικασία που εξελίχθηκε αρκετά τα επόμενα χρόνια μέσω της διασύνδεσης μητρώων της ΗΔΙΚΑ με ασφαλιστικούς οργανισμούς και αργότερα με τις βάσεις δεδομένων της φορολογικής διοίκησης.

Ως προς το απόρρητο και ασφάλεια της επεξεργασίας που αναφέρονται στο άρθρο 10, ο νόμος ακολούθησε σχεδόν κατά γράμμα τις σχετικές προβλέψεις της Οδηγίας 1995/46/ΕΚ όπως αναφέρθηκαν νωρίτερα. Ανάθεσε δε στην νεοσυσταθείσα ΑΠΔΠΧ την υποχρέωση να παρέχει εκάστοτε οδηγίες για το βαθμό ασφάλειας των δεδομένων, καθώς και για τα μέτρα προστασίας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία δεδομένων, λαμβάνοντας υπ'όψη τις τεχνολογικές εξελίξεις.

2.4.4 Ευρωπαϊκός Κανονισμός 2016/679/ΕΕ - GDPR

Η σημαντικότερη νομοθετική εξέλιξη για την προστασία των προσωπικών δεδομένων των τελευταίων χρόνων είναι ο Ευρωπαϊκός Κανονισμός 2016/679/ΕΚ, ευρύτερα γνωστός με το λατικινό αρκτικόλεξο GDPR, αρχικά των λέξεων General Data Protection Rule (Γενικός Κανονισμός για την Προστασία Δεδομένων). Ο κανονισμός ψηφίστηκε τον Απρίλιο του 2016 και αντικαθιστά τόσο την Οδηγία 1996/46/ΕΚ όσο και τον Ν. 2472/97 και τις λοιπές εθνικές νομοθεσίες για την προστασία δεδομένων. Ο GDPR αφορά τις εταιρείες, τους οργανισμούς αλλά και τους δημόσιους φορείς που επεξεργάζονται δεδομένα πολιτών της Ευρωπαϊκής Ένωσης. Οι ευρωπαϊκές εταιρείες και οργανισμοί είχαν στη διάθεσή του συνολικά σχεδόν δύο χρόνια, από τον Απρίλιο

του 2016 μέχρι τον Μάιο του 2018, για να αλλάξουν τις πολιτικές τους σχετικά με τη διασφάλιση ιδιωτικότητας, να τροποποιήσουν κατάλληλα τα πληροφοριακά τους συστήματα, καθώς και τις επιχειρησιακές τους διαδικασίες, ώστε να συμμορφώνονται με τον νέο κανονισμό.

Ως προς το τι εστί δεδομένο προσωπικού χαρακτήρα**,** ο GDPR αναφέρει ρητά μια σειρά από δεδομένα όπως όνομα, αριθμό θέσεις αλλά και προεκτείνεται σε παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του φυσικού προσώπου. Προσθέτει δε δύο νέες ειδικές κατηγορίες προσωπικών δεδομένων, τα **γενετικά δεδομένα** που αφορούν τα γενετικά χαρακτηριστικά ενός φυσικού προσώπου και τα **βιομετρικά δεδομένα,** τα οποία προκύπτουν από ειδική τεχνική επεξεργασία φυσικών, βιολογικών ή συμπεριφορικών χαρακτηριστικών και τα οποία επιτρέπουν την ταυτοποίηση ενός φυσικού προσώπου. Τέτοια μπορεί να είναι τα δακτυλικά αποτυπώματα, εικόνες προσώπου κ.α.

Στο άρθρο 4 Ο GDPR παρέχει επίσης έναν ορισμό του **συστήματος αρχειοθέτησης**, το οποίο καθορίζει ως κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

Σε σχέση με τις αρχικές κατευθύνσεις του ΟΟΣΑ ο GDPR ως προς τις αρχές της θεμιτής επεξεργασίας προσωπικών δεδομένων προσέθεσε την αρχή του περιορισμού της περιόδου αποθήκευσης. Αναλυτικά, οι γενικές αρχές που καθορίζει για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι οι ακόλουθες:

Νομιμότητα, αντικειμενικότητα και διαφάνεια: Να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων,

Περιορισμός του σκοπού: Να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς, με ορισμένες εξαιρέσεις

Ελαχιστοποίηση των δεδομένων: Να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

Ακρίβεια: Να είναι ακριβή, να επικαιροποιούνται και να λαμβάνονται όλα τα

εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση ανακριβών δεδομένων

Περιορισμός της περιόδου αποθήκευσης: Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας, με ορισμένες εξαιρέσεις για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς,

Ακεραιότητα και εμπιστευτικότητα: υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων

Λογοδοσία: Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις παραπάνω αρχές.

Η αρχή της Λογοδοσίας αποτελεί νεωτερισμό του κανονισμού και διατρέχει πολλές διατάξεις του. Ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να είναι σε θέση να αποδείξει τη συγκατάθεση του υποκειμένου (Άρθρο 7 π. 1). Είναι επίσης υπεύθυνος για να παρέχει διαφανή ενημέρωση και ανακοινώσεις στα υποκείμενα των δεδομένων αναφορικά με τα δεδομένα που τηρεί και την επεξεργασία τους, με συγκεκριμένη μάλιστα προθεσμία ενός μήνα μετά από αίτημα παροχής πληροφοριών (Άρθρο 12).

Παρά τις νέες απαιτήσεις, ο GDPR προβλέπει και κάποιες διοικητικές ελαφρύνσεις για τους οργανισμούς όπως η κατάργηση της υποχρέωσης γνωστοποίησης της επεξεργασίας δεδομένων στις κατά τόπους εποπτικές αρχές. Αντίστοιχα όμως οι οργανισμοί υποχρεούνται να γνωστοποιήσουν τυχόν παραβίαση δεδομένων στην αρμόδια εποπτική αρχή εντός 72 ωρών. Επίσης, όταν η παραβίαση βάζει σε κίνδυνο τα δικαιώματα των υποκείμενων των δικαιωμάτων, πρέπει να γνωστοποιείται και σε αυτά.

Ο νέος κανονισμός έχει συγκεκριμενοποιήσει αρκετά τις απαιτήσεις από τους οργανισμούς αναφορικά με τις διαδικασίες. Το άρθρο 25 εισάγει στην ευρωπαϊκή νομοθεσία τις έννοιες της προστασίας των δεδομένων από τον σχεδιασμό (privacy by design) και εξ ορισμού (by default). Η προσέγγιση της προστασίας από τον σχεδιασμό βασίζεται σε επτά αρχές, η δεύτερη εκ των οποίων είναι η προστασία εξ ορισμού. Πρεσβεύει την ενσωμάτωση της προστασίας της ιδιωτικότητας στον αρχικό σχεδιασμό των πληροφοριακών συστημάτων, επιχειρηματικών πρακτικών και δικτυακών υποδομών και όχι την ενσωμάτωση της εκ των υστέρων. Ειδικά η προστασία εξ

ορισμού σημαίνει πως τα δεδομένα του υποκείμενου προστατεύονται αυτόματα, χωρίς να απαιτείται κάποια ενέργεια εκ μέρους του.

Οι τεχνικές απαιτήσεις για την **ασφάλεια της επεξεργασίας** των προσωπικών δεδομένων ορίζονται πολύ πιο εκτεταμένα στον GDPR σε σχέση με την οδηγία που αντικατέστησε. Το άρθρο 32 αναφέρει τα ακόλουθα τεχνικά και οργανωτικά μέτρα που πρέπει, κατά περίπτωση, να λαμβάνουν ο υπεύθυνος και ο εκτελών την επεργασία:

- Ψευδωνυμοποίηση και κρυπτογράφηση των δεδομένων
- διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση
- δυνατότητα αποκατάσταση της διαθεσιμότητας και της πρόσβασης στα δεδομένα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος
- διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας

Το άρθρο 35 εισάγει νομικά τη διαδικασία της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (Data Protection Impact Assessment, DPIA) για τους υπεύθυνους επεξεργασίας. Ο υπεύθυνος επεξεργασίας υποχρεούται ρητά σε διενέργεια DPIA, πριν από την κρίσιμη επεξεργασία, κάθε φορά που ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών, και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας αυτής, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Ανάμεσα στις περιπτώσεις που η διενέργεια DPIA κρίνεται απαραίτητη είναι σε περιπτώσεις συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο. Στην περίπτωση αυτή εμπίπτουν οι ΦΚΑ, ιδιαίτερα ο ΕΦΚΑ ο οποίος χειρίζεται και ευαίσθητα ιατρικά δεδομένα.

Εφόσον η εκτίμηση αντικτύπου υποδείξει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο λόγω έλειψης μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας, ο υπέυθυνος καλείται να ζητήσει την γνώμη της εποπτικής αρχής (αρ.

36). Η τελευταία του παρέχει γραπτές συμβουλές και δύναται να ασκήσει όλες τις εξουσίες που τις παρέχει ο GDPR. Ειδικά για Δημόσιους Φορείς που ασκούν επεξεργασία προς το δημόσιο συμφέρον περιλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία, όπως στην περίπτωση των ΦΚΑ, ο νόμος επιτρέπει στα κράτη να καταστήσουν υποχρεωτική την διαβούλευση και αδειοδότηση από την εποπτική αρχή. Είναι μια δυνατότητα η οποία δεν έχει εισαχθεί ακόμα στην ελληνική νομοθεσία, αφού εκκρεμεί η εισαγωγή προς ψήφιση του νόμου που θα εισάξει τον GDPR στην εσωτερική έννομη τάξη.

Μια σημαντική καινοτομία που εισάγει ο GDPR με το άρθρο 37 είναι το να καταστήσει υποχρεωτική τη θέση του **Υπεύθυνου Προστασίας Δεδομένων** (Data Protection Officer, DPO). Ο συγκεκριμένος ρόλος προβλέφθηκε για πρώτη φορά στην Οδηγία 1995/46/ΕΚ ενώ υπάρχει και στο άρθρο 36 του Ν. 3979/2011 «*για την ηλεκτρονική διακυβέρνηση*». Αποστολή του ΥΠΔ είναι να ενημερώνει και να συμβουλεύει τους υπεύθυνους επεξεργασίας αναφορικά με την τήρηση του GDPR. Πραγματοποιεί την εκτίμηση αντικτύπου, παρακολουθεί την εσωτερική συμμόρφωση, οργανώνει την εκπαίδευση και ευαισθητοποίηση του προσωπικού και αποτελεί το σημείο επαφής του οργανισμού με την ΑΠΔΠΧ. Έχοντας συμβουλευτικό ρόλο, δεν φέρει προσωπική νομική ευθύνη για τυχόν μη συμμόρφωση του οργανισμού, ενώ μπορεί να είναι εσωτερικός ή εξωτερικός συνεργάτης. Ο ορισμός DPO είναι υποχρέωση για τους δημόσιους φορείς, όπως οι ΦΚΑ, αν και, κατά περίπτωση, μπορεί ένας DPO να ορίζεται για περισσότερους από έναν φορείς.

Ο GDPR ενθαρρύνει επίσης τη σύνταξη **κώδικα δεοντολογίας** από κλαδικούς φορείς, χωρίς όμως αυτοί να αφορούν τις δημόσιες αρχές ή φορείς. Εθελοντική είναι επίσης και η **πιστοποίηση**, η οποία μπορεί να χρησιμοποιηθεί ως απόδειξη συμμόρφωσης του υπεύθυνου επεξεργασίας με τις υποχρεώσεις του, τον σχεδιασμό εξ ορισμού, των εκτελούντων που προσλαμβάνει ή με την ασφάλεια της επεξεργασίας.

Τα ανεπαρκή μέτρα προστασίας των δεδομένων μπορούν να οδηγήσουν σε πρόστιμα που ανέρχονται στις δύο εκατοστιαίες μονάδες του παγκόσμιου κύκλου εργασιών ή σε 10.000.000 €. Η Αρχή Προστασίας Δεδομένων μπορεί, επίσης, να αναστείλει τη λειτουργία μίας εταιρείας, έως ότου η εταιρεία αυτή συμμορφωθεί με τον νέο κανονισμό GDPR.

Όπως φαίνεται από τα παραπάνω, ο νέος κανονισμός για την προστασία δεδομένων επιβάλλει αυστηρότερες πολιτικές και κανόνες σε σχέση με την προηγουμένως ισχύουσα νομοθεσία. Επίσης, παρέχει πλέον στις Αρχές Προστασίας Δεδομένων τη δυνατότητα να επιβάλουν πολύ υψηλότερα πρόστιμα σε σχέση με παλαιότερα

3.Τήρηση και Ασφάλεια δεδομένων στην Κοινωνική Ασφάλιση

3.1 Κατηγορίες Δεδομένων στην Κοινωνική Ασφάλιση

Οι ΦΚΑ για να φέρουν σε πέρας την αποστολή τους συλλέγουν μια πληθώρα δεδομένων από Τα δεδομένα μπορούν να διακριθούν νομικά σε τρεις κατηγορίες: Σε *μη προσωπικά δεδομένα*, σε *προσωπικά δεδομένα* και σε *ευαίσθητα προσωπικά δεδομένα,* όπως αυτά καθορίζονται στον GDPR. Οι κύριες ομάδες δεδομένων είναι:

Δεδομένα ασφαλιστικών εισφορών: Περιλαμβάνονται δεδομένα που αφορούν τον υπολογισμό και την καταβολή των εργοδοτικών εισφορών και υποβάλλονται μέσω των ΑΠΔ, οι οποίες γίνονται πλέον αποκλειστικά ηλεκτρονικά.[2] Μέσα σε αυτά βρίσκονται προσωπικά δεδομένα των ασφαλισμένων και πιο συγκεκριμένα τα ΑΜΚΑ, ο ΑΦΜ, ονοματεπώνυμο, ονόματα γονέων του/της, καθώς και η ημερομηνία γέννησης και τόπος γέννησης. Στα προσωπικά δεδομένα περιλαμβάνονται επίσης το είδος της εργασίας και η αμοιβή των εργαζομένων.

Δεδομένα παροχών ασφαλισμένων: Πρόκειται για δεδομένα που αφορούν την απονομή συντάξεων καθώς και παροχές σε χρήμα όπως επιδόματα ασθένειας, μητρότητας, αναπηρίας, έξοδα κηδείας κ.α. Προσωπικά δεδομένα που περιλαμβάνονται σε αυτή την κατηγορία είναι τα ΑΜΚΑ, ο Αριθμός Μητρώου Ασφαλισμένου ΑΦΜ, ονοματεπώνυμο, ονόματα γονέων, καθώς και η ημερομηνία γέννησης και τόπος γέννησης. Επίσης προσωπικά οικονομικά δεδομένα όπως το ύψος της σύνταξης και ο αριθμός τραπεζικού λογαριασμού. Τέλος, στα στοιχεία αυτής της κατηγορίας περιλαμβάνονται ιατρικές γνωματεύσεις, οι οποίες κατατάσσονται στα ευαίσθητα προσωπικά δεδομένα.[3]

---

[2] Με κάποιες εξαιρέσεις για διαχειριστές κτιρίων (Πολυκατοικίες κλπ), όσους εκτελούν Δημόσια οικοδομοτεχνικά έργα με αυτεπιστασία ή με ανάθεση, μέχρι και τρεις εργαζόμενους και όσους εκτελούν Ιδιωτικά οικοδομικά και τεχνικά έργα με αυτεπιστασία

[3] Ο ΕΟΠΥΥ χρησιμοποιεί τα πληροφοριακά συστήματα του ΕΦΚΑ, και πιο συγκεκριμένα το ΟΠΣ ΙΚΑ/Υποσύστημα Υγείας στα πλαίσια της λειτουργίας του κατόπιν συμφωνίας. Ως αποτέλεσμα, τα υπολογιστικά συστήματα του ΕΦΚΑ καταχωρούν πληθώρα ευαίσθητων προσωπικών δεδομένων όπως ιατρικές εξετάσεις, επισκέψεις κλπ, καθώς και προσωπικά δεδομένα ιατρών. Επειδή όμως η φύλαξη αυτή

Οικονομικά και λογιστικά δεδομένα: Δεδομένα τα οποία περιλαμβάνουν στοιχεία των εργαζομένων του ΕΦΚΑ και τρίτους συναλασσόμενους με αυτό (προμηθευτές κ.α.), καθώς επίσης και στοιχεία ισολογισμών, απολογισμών και διαχείρισης του χαρτοφυλακίου του φορέα. Τα προσωπικά δεδομένα σε αυτή την κατηγορία αφορούν κυρίως τους εργαζόμενους και προμηθευτές και περιλαμβάνουν τον ΑΜΚΑ, ο Αριθμός Μητρώου Ασφαλισμένου, το ΑΦΜ, ονοματεπώνυμο, ονόματα γονέων, καθώς και την ημερομηνία και τόποςγέννησης.

3.2 Διαδικασίες Διαχείρισης

Οι διαδικασίες διαχείρισης ποικίλουν ανάλογα με το είδος της υπηρεσίας και τον βαθμό ηλεκτρονικοποίησης της

Είσοδος δεδομένων σε χειρόγραφη μορφή και μετατροπή τους σε ηλεκτρονική μορφή: Σε πολλές περιπτώσεις αιτήσεων πχ για απόδοση παροχών, οι ασφαλισμένοι καταθέτουν χειρόγραφα την αίτηση τους, ενώ στη συνέχεια τα δεδομένα που περιέχει αυτή εισάγονται ηλεκτρονικά στο ΠΣ, μέσω του οποίου συνεχίζεται η συσχέτιση τους. Βέβαια παράλληλα με την ηλεκτρονική διαδικασία είναι πιθανόν να διακινούνται και παραστατικά σε έγχαρτη μορφή.

Είσοδος δεδομένων σε χειρόγραφη μορφή - ηλεκτρονική επεξεργασία - παραγωγή αποτελέσματος σε έγχαρτη μορφή: Στη συγκεκριμένη περίπτωση οι συναλλαγή ξεκινά με την κατάθεση εγγραφής αίτησης. Η επεξεργασία γίνεται με την αξιοποίηση ηλεκτρονικών δεδομένων και το τελικό αποτέλεσμα παραδίδεται στον συναλλασσόμενο σε έγχαρτη μορφή. Τέτοια περίπτωση είναι η χορήγηση βεβαίωσης ασφαλιστικής ενημερότητας για πολλούς τομείς του ΕΦΚΑ οι οποίοι δεν έχουν ενταχθεί στην ηλεκτρονική υπηρεσία. Επίσης σε αυτή την κατηγορία συγκαταλέγονται οι αιτήσεις απονομής σύνταξης και εφάπαξ σε κάποιους τομείς του ΕΤΕΑΕΠ.

*Ηλεκτρονική επεξεργασία δεδομένων - παραγωγή σε έγχαρτη μορφή***:** Πρόκειται για περιπτώσεις που η αίτηση γίνεται προφορικά σε υποκατάστημα, όπως πχ στην περίπτωση μιας αίτησης για βεβαίωση αποδοχών προς ασφαλισμένους, ενώ η επεξεργασία γίνεται στο ΠΣ.

δεν γίνεται στα πλαίσια παροχών κοινωνικής ασφάλισης αλλά υγείας δεν απασχολούν την συγκεκριμένη εργασία.

Πλήρως ηλεκτρονική διαχείριση δεδομένων: Πρόκειται για πλήρως ηλεκτρονικές υπηρεσίες οι οποίες παρέχονται είτε από τον ιστότοπο του ΕΦΚΑ είτε μέσω άλλου τρόπου ηλεκτρονικής ανταλλαγής δεδομένων. Η σχετική διαδικασία με την μεγαλύτερη χρήση είναι η ηλεκτρονική καταβολή της ΑΠΔ από τους εργοδότες, κατόπιν εγγραφής και αυθεντικοποίησης τους, είτε μέσω εφαρμογής προσβάσιμης από τον ιστότοπο του ΕΦΚΑ είτε μέσω ηλεκτρονικού αρχείου κατάλληλα διαμορφωμένου το οποίο μεταφορτώνεται. Αφού ελεγχθεί η υποβολή του εργοδότη στη συνέχεια είτε ζητείτε διόρθωση είτε τα δεδομένα καταχωρούνται στο ΠΣ του ΕΦΚΑ.

Επίσης, για ορισμένες λειτουργίες, τα συστήματα του ΕΦΚΑ ανταλάσσουν δεδομένα με άλλα εξωτερικά πληροφοριακά συστήματα. Τέτοια είναι η περίπτωση συγχρονισμού συστημάτων του ΕΦΚΑ με το μητρώο ΑΜΚΑ ή με το Taxis για αυθεντικοποίηση χρηστών. Η ανταλλαγή δεδομένων δεν γίνεται απαραίτητα μέσω δικτύου αλλά μπορεί να γίνεται και με την χρήση αποθηκευτικών μέσων (πχ USB).

3.3 Αποθήκευση δεδομένων

Ηλεκτρονικά δεδομένα: Τα ηλεκτρονικά δεδομένα τηρούνται στις βάσεις δεδομένων των ΠΣ του ΕΦΚΑ, οι οποίες βρίσκονται στα υπολογιστικά κέντρα τα οποία αναφέρθηκαν στο κεφάλαιο 1.2.3.3. Σε καθημερινή βάση δημιουργούνται αντίγραφα των δεδομένων, τα οποία τηρούνται σε δύο διαφορετικές τοποθεσίες. Τα ηλεκτρονικά δεδομένα δεν διαγράφονται μετά το πέρας κάποιου χρονικού διαστήματος

Δεδομένα σε χάρτινη μορφή: Ο όγκος των δεδομένων που εισέρχονται στον ΕΦΚΑ σε χάρτινη μορφή έχει μειωθεί μετά την θέσπιση της υποχρεωτικής ηλεκτρονικής υποβολής των ΑΠΔ και αφορούν κατά κύριο λόγο αιτήματα παροχών. Στην πλειοψηφία των περιπτώσεων μετά την ολοκλήρωση της παροχής της υπηρεσίας τα έγγραφα τηρούνται στο σχετικό υποκατάστημα του φορέα.

Για την αποθήκευση των δεδομένων που βρίσκονται σε χάρτινη μορφή χρησιμοποιούνται διάφορα μέσα που ποικίλουν ανά φορέα, τομέα ή ακόμα και υποκατάστημα. Μπορεί να είναι κούτες με σήμανση, κλασέρ, ντοσιέ, φάκελοι, φοριαμοί κλπ.

Ως προς τον χρόνο τήρησης των χάρτινων δεδομένων και τις διαδικασίες καταστροφής τους, θεωρητικά ορίζονται από τις διατάξεις των ΠΔ 768/1980 και 480/1985, χωρίς να τηρούνται πάντα οι προβλέψεις τους.

3.4 Ασφάλεια Δεδομένων στα Συστήματα Κοινωνικής Ασφάλισης

3.4.1 Το ζήτημα της ασφάλειας των Πληροφοριακών Συστημάτων

Στο κεφάλαιο 1.1.2 αναλύθηκε η σημασία του ΠΣ για τον συντονισμό των μονάδων ενός οργανισμού και τη νευραλγική του θέση για τη λήψη αποφάσεων. Τα ΠΣ των ΦΚΑ αποτελούν κρίσιμο στοιχείο της υποδομής τους και η αποτελεσματική και αδιάκοπη λειτουργία τους παραμένει άρρηκτα συνδεδεμένη με τη λειτουργία του οργανισμού. Η αναγκαιότητα διασφάλισης τους προκύπτει από:

- Την ποικιλία και ένταση των κινδύνων που αντιμετωπίζουν τα σύγχρονα ΠΣ
- Τις νομικές απαιτήσεις προστασίας προσωπικών δεδομένων
- Το κόστος που προκύπτει τόσο από τις εσκεμμένες παραβιάσεις της ασφάλειας όσο και από τυχαία ή φυσικά γεγονότα που μπορεί να διαταράξουν την λειτουργία ενός ΠΣ

Η ασφάλεια των ΠΣ επαφίεται σε έναν συνδυασμό παραγόντων, τόσο τεχνικούς όσο και διοικητικούς-οργανωτικούς. Η απόλυτη ασφάλεια δεν είναι κάτι το εφικτό. Επιπλέον, το κόστος βαίνει αυξανόμενο καθώς αυξάνει το επίπεδο της ασφάλειας και είναι πάντα ένας παράγοντας που προσμετράται κατά τη λήψη μέτρων ασφάλειας.

3.4.2 Απειλές

Τα ΠΣ αντιμετωπίζουν μια σειρά απειλών τα οποία μπορεί να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων που είναι καταχωρημένα σε αυτά. Κάποιες από αυτές τις απειλές αυτές είναι **φυσικές και περιβαλλοντικές** όπως οι κίνδυνοι από πλημμύρες και σεισμούς ή από αστοχία ηλεκτρολογικών συστημάτων ή ακόμα και από κλοπή. Υπάρχουν ακόμα **λογικές απειλές** όπως η πλαστοπροσωπία, οι ηλεκτρονικοί ιοί ή η υποκλοπή δεδομένων μέσω δικτύου. Τέλος, δύο ακόμα κατηγορίες απειλών αφορούν την **αστοχία εξοπλισμού** και

λογισμικού, οι οποίες επηρεάζουν συνήθως την διαθεσιμότητα των ΠΣ και των δεδομένων τους.

Η αξιολόγηση του μεγέθους του ρίσκου που επισύρει κάθε μορφή απειλής για ένα ΠΣ γίνεται με μεθόδους εκτίμησης επικινδυνότητας (risk assessments). Στον τομέα της Κοινωνικής Ασφάλισης έχουν γίνει περιορισμένες σχετικές μελέτες λόγω και του σχετικά μικρού αριθμού εκτεταμένων ΠΣ και της, επίσης σχετικής, σύντομης περιόδου λειτουργίας τους. Μια τέτοια εκτίμηση στο πλέον σημαντικό ΠΣ των ΦΚΑ, του ΟΠΣ ΙΚΑ, η οποία είχε γίνει από την εταιρία συμβούλων Planet (2012) με την μέθοδο CRAMM,[4] εκτιμούσε τιςς ακόλουθες ως τις σημαντικότερες περιπτώσεις υψηλής επικινδυνότητας για το σύστημα:

Πλαστογραφία από Παρόχους Υπηρεσιών/Τρίτους: Σε περίπτωση που κάποιος τρίτος αποκτήσει λογαριασμό και συνθηματικό εξουσιοδοτημένου χρήστη μπορεί να επιφέρει σημαντικές επιπτώσεις στο σύστημα

Μη εξουσιοδοτημένη χρήση εφαρμογών: Υψηλή επικινδυνότητα λόγω των σοβαρών επιπτώσεων σε περίπτωση που κάποιος υπάλληλος του Ιδρύματος ή τρίτος καταφέρει να χρησιμοποιήσει εφαρμογές του ΠΣ με μη εξουσιοδοτημένο τρόπο[5]

Διείσδυση μέσω δικτύου: Η απόκτηση μη εξουσιοδοτημένης πρόσβασης ενέχει τον κίνδυνο άρσης της εμπιστευτικότητας των δεδομένων, αλλά και βλάβης της ακεραιότητας τους

Κλοπή από τρίτους:Τυχόν κλοπή των μέσων αποθήκευσης όπου φυλάσσονται τα δεδομένα των πληροφοριακών συστημάτων θα μπορούσε να έχει ως συνέπεια την αποκάλυψη των δεδομένων τους και προσωρινή διακοπή της λειτουργίας του ΠΣ.

Πυρκαγιά και σεισμός: Μια φυσική καταστροφή στο κτίριο όπου στεγάζονται τα πληροφοριακά συστήματα του φορέα θα μπορούσε να έχει ως συνέπεια τη διακοπή της λειτουργίας του φορέα για μεγάλο χρονικό διάστημα λόγω έλλειψης εναλλακτικών

[4] Η μέθοδος CRAMM (CCTA Risk Analysis Management Methodology) προέρχεται από το Ηνωμένο Βασίλειο και αποτελεί πρότυπο για τους οργανισμούς του ευρύτερου δημοσίου τομέα της χώρας. Καλύπτει όλες τις συνιστώσες της ασφάλειας, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας κλπ

[5] Στις 25/5/2018 ανακοινώθηκε πως υπάλληλος του ΕΦΚΑ τέθηκε σε αναστολή άσκησης καθηκόντων κατηγορούμενος πως χρησιμοποιώντας παράνομα κωδικούς πρόσβασης παρενέβη για να αλλοιώσει το ποσοστό αναπηρίας του ασφαλισμένου. Δείγμα πως ο κίνδυνος της μη εξουσιοδοτημένης χρήσης εξακολουθεί να υπάρχει στον ΕΦΚΑ.

εγκαταστάσεων πληροφοριακών συστημάτων, με δυσμενείς συνέπειες για την διαθεσιμότητα των δεδομένων

3.4.3 Σχέδιο ασφάλειας

Στην ενότητα αυτή θα εξεταστεί το σχέδιο ασφάλειας του ΟΠΣ ΙΚΑ. Το συγκεκριμένο ΠΣ επελέγη γιατί αποτελεί το πλέον εκτενές και ολοκληρωμένο ΠΣ ΦΚΑ στην Ελλάδα και παράλληλα συνιστά το βασικό δομικό στοιχείο του πληροφοριακού συστήματος του μεγαλύτερο ΦΚΑ, του ΕΦΚΑ

3.4.3.1 Οργάνωση, διαχείριση και διοίκηση ασφάλειας:

Ο ν. 4387/2016 , όπως τροποποιήθηκε από τον ν. 4445/2016, προβλέπει τη διοικητική οργάνωση του ΕΦΚΑ μέχρι την έναρξη ισχύος του οργανισμού του νέου φορέα. Αρμόδια για τον σχεδιασμό, την ανάπτυξη και εφαρμογή της πολιτικής ασφάλειας στα συστήματα ΤΠΕ του φορέα καθίσταται η Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών, στην οποία έχει ιδρυθεί Τμήμα Ασφάλειας Συστημάτων και Εφαρμογών, στελεχωμένο από 5 εργαζόμενους, τρεις επιστήμονες πληροφορικής και δύο τεχνικούς. Στα καθήκοντα του τμήματος ανήκουν:

- Η παρακολούθηση και η διαρκής ενημέρωση της εξέλιξης των τεχνολογιών σε θέματα ασφάλειας των συστημάτων πληροφορικής και επικοινωνιών.
- Η εκπόνηση μελετών και η διατύπωση προτάσεων για τη διαμόρφωση της πολιτικής και του σχεδίου ασφάλειας που θα εφαρμόζεται από το ΕΦΚΑ
- Η παρακολούθηση της εφαρμογής του σχεδίου ασφάλειας και η αξιολόγηση της αποτελεσματικότητάς του.
- Η διενέργεια περιοδικών και εκτάκτων ελέγχων για τη διαπίστωση της τήρησης των κανόνων ασφάλειας.
- Ο σχεδιασμός και η εφαρμογή διαδικασιών εναρμόνισης των πληροφοριακών συστημάτων του ΕΦΚΑ με εθνικά και διεθνή πρότυπα ασφάλειας.
- Η σύνταξη περιοδικών αναφορών και εκθέσεων ασφάλειας, καθώς και ετήσιας απολογιστικής έκθεσης σχετικά με την αποτελεσματικότητα του σχεδίου ασφάλειας

- Η επιμέλεια για την ορθή εφαρμογή της νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα και γενικά των διαβαθμισμένων πληροφοριών.

Υπάρχουν και άλλες Διευθύνσεις και Τμήματα με αρμοδιότητες οι οποίες επηρεάζουν την τήρηση των προσωπικών δεδομένων και γενικότερα την ασφάλεια. Στη Διεύθυνση Υποδομών Πληροφορικής και Επικοινωνίας είναι δύο τα σχετικά τμήματα. Το Τμήμα Διαχείρισης Κεντρικών Υποδομών είναι υπεύθυνο, ανάμεσα σε άλλες αρμοδιότητες, για:

- Περιοδική λήψη και φύλαξη αντιγράφων ασφαλείας δεδομένων, καθώς και τη μέριμνα για την ανάκαμψη από καταστροφές.
- Εξασφάλιση της συνεχούς λειτουργίας και διαθεσιμότητας των συστημάτων πληροφορικής και υλοποίηση σχεδίων ταχείας ανάκαμψης αυτών από βλάβη ή καταστροφή.
- Εφαρμογή αρχών και προτύπων ασφαλείας από εσωτερικές και εξωτερικές απειλές και κινδύνους.

Επίσης, το τμήμα Διαχείρισης Δικτυακών Υποδομών έχει ευθύνη για:

- Εφαρμογή αρχών και προτύπων για την ασφάλεια των δικτύων από εσωτερικές και εξωτερικές απειλές και κινδύνους.
- εξασφάλιση της συνεχούς λειτουργίας και διαθεσιμότητας των δικτυακών υποδομών και υλοποίηση σχεδίων ταχείας ανάκαμψης αυτών από βλάβη ή καταστροφή.

Στη Διεύθυνση Εφαρμογών και Ανάπτυξης, το Τμήμα Ανάπτυξης και Συντήρησης Εφαρμογών Πληροφορικής έχει ευθύνη για την εφαρμογή αρχών και προτύπων ασφάλειας από εσωτερικούς και εξωτερικούς κινδύνους για τα δεδομένα. Το δε Τμήμα Παραγωγικής Λειτουργίας Κεντρικών Συστημάτων είναι αρμόδιο για:

- Περιοδικούς τακτικούς και έκτακτους ελέγχους για την ποιότητα και την ακεραιότητα των δεδομένων
- Καθορισμό των κανόνων ανταλλαγής των δεδομένων και προετοιμασία και ησύναψη συμφωνιών ανταλλαγής δεδομένων με άλλους φορείς.

- Προσδιορισμό των δικαιωμάτων πρόσβασης σε εφαρμογές και δεδομένα, καθώς και πιστοποίησης των χρηστών.
- Εφαρμογή αρχών και προτύπων για την ασφάλεια των δεδομένων από εσωτερικές και εξωτερικές απειλές και κινδύνους.

Στην, προσωρινή, διοικητική οργάνωση του φορέα παρατηρείται μια διάχυση της ευθύνης για την ασφάλεια των δεδομένων και των πληροφοριακών συστημάτων ευρύτερα. Αντίθετα με τις διεθνείς βέλτιστες πρακτικές και το ISO 27001, τα οποία συστήνουν την θέσπιση ανεξάρτητων τμημάτων ασφαλείας τα οποία αναφέρονται απευθείας στη διοίκηση, έχει επιλεγεί η ίδρυση ενός Τμήματος Ασφάλειας εντός μιας Γενικής Διεύθυνσης Πληροφορικής με τις συνεπαγόμενες συγκρούσεις συμφερόντων οι οποίες μπορεί να προκύψουν. Επιπλέον, το τμήμα αυτό, βάσει της περιγραφής των αρμοδιοτήτων του φαίνεται να έχει κυρίως συμβουλευτικό και ελεγκτικό ρόλο. Η ευθύνη για την υλοποίηση ανατίθεται στις επιμέρους διευθύνσεις, ενώ το σχετικό Τμήμα Ασφάλειας φαίνεται να μην έχει λέγειν σε κρίσιμες διαδικασίες για την ασφάλεια των πληροφοριακών συστημάτων όπως ο καθορισμός των κανόνων ανταλλαγής δεδομένων και ο προσδιορισμός των δικαιωμάτων πρόσβασης.

Η νομική αποτύπωση της δομής ενός οργανισμού δεν αντανακλάται βέβαια πάντα στην πραγματικότητα της λειτουργίας του. Υπάρχουν αρκετές αναφορές πως λόγω του σύντομου χρόνου ύπαρξης του και τη μη έκδοσης προβλεπόμενων προεδρικών διαταγμάτων και υπουργικών αποφάσεων που αφορούν την καθημερινή λειτουργία του ΕΦΚΑ, αυτή παραμένει στην πράξη οργανωμένη βάσει των προϋπάρχοντων ταμείων, νυν φορέων.

3.4.3.2 Υποδομή και Μηχανισμοί Ασφάλειας

Κεντρικές Υπολογιστικές Μονάδες

Όπως αναφέρθηκε στην Ενότητα 1.2.3.3, ο ΕΦΚΑ διαθέτει δύο Κέντρα Δεδομένων, στις οδούς Παπαδιαμαντοπούλου και Πατησίων 12. Κανένα από τα δύο δεν διαθέτει ολοκληρωμένο σύστημα ψύξης και διαχείρισης θερμοκρασίας ενώ μόνο αυτό της Παπαδιαμαντοπούλου διαθέτει προβλέψεις για περίπτωση διακοπής της παροχής ρεύματος από το κεντρικό δίκτυο. Ο εξοπλισμός πάντως στα κεντρικά και περιφερειακά συστήματα, ο οποίος βασίζεται σε αρχιτεκτονική πελάτη-εξυπηρετητή

(client-server) θεωρείται απαρχαιομένος και δεν υποστηρίζεται ή συντηρείται από κάποιον ανάδοχο.

Έλεγχος Πρόσβασης

Η πρόσβαση στα πληροφοριακά συστήματα γίνεται με τη χρήση συνδυασμού ονόματος και κωδικού χρήστη. Κάθε διακριτικό είναι μοναδικό και συνδέεται με συγκεκριμένο χρήστη. Ως προς την φυσική πρόσβαση στις εγκαταστάσεις, κανένα από τα δύο υπολογιστικά κέντρα δεν διαθέτει εν λειτουργία μηχανισμό ελέγχου πρόσβασης στον χώρο. Οι κτιριακές εγκαταστάσεις φυλάσσονται πάντως 24 ώρες το 24ωρο.

Φυσικός διαχωρισμός τοπικών δικτύων

Τα τοπικά δίκτυα εντός του ΕΦΚΑ είναι φυσικά διαχωρισμένα και δεν επικοινωνούν μεταξύ τους. Το δίκτυο του ΟΠΣ-ΙΚΑ πχ δεν επικοινωνεί με άλλα τοπικά δίκτυα

Περιορισμός πρόσβασης στο διαδίκτυο

Οι σταθμοί εργασίας που συνδέονται στο ΟΠΣ ΙΚΑ δεν διαθέτουν πρόσβαση στο διαδίκτυο. Επίσης οι χρήστες τους δεν έχουν εξουσιοδότηση για εγκατάσταση εφαρμογών λογισμικού σε αυτούς. Οι θύρες USB των υπολογιστών αυτών είναι απενεργοποιημένες. Οι σταθμοί εργασίας που διαθέτουν πρόσβαση με το διαδίκτυο στα υποκαταστήματα δεν συνδέονται με το τοπικό δίκτυο του υποκαταστήματος και συνδέονται με το διαδίκτυο μέσω ξεχωριστής σύνδεσης.

Προστασία από κακόβουλο λογισμικό

Ο ΕΦΚΑ διαθέτει λογισμικό ανίχνευσης κακόβουλου λογισμικού εγκατεστημένο σε όλους τους σταθμούς εργασίας των συστημάτων του. Διαθέτει πάντως αρκετούς σταθμούς εργασίας με παλαιές εκδόσεις λειτουργικών συστημάτων οι οποίες δεν υποστηρίζονται πλέον με ενημερώσεις ασφαλείας.

Firewalls

Τα τοπικά δίκτυα που έχουν πρόσβαση στο διαδίκτυο προστατεύονται από firewalls

Διαθεσιμότητα συστημάτων

Ο εξοπλισμός των βασικών πληροφοριακών συστημάτων του ΕΦΚΑ ακολουθεί αρχιτεκτονική υψηλής διαθεσιμότητας και αξιοποιούνται τεχνικές clustering, RAID κ.α. Επίσης οι εξυπηρετητές υποστηρίζονται από συστήματα UPS, τα οποία όμως χρήζουν αναβάθμισης.

Ασφάλεια δικτύων WAN / Extranet

Το VPN δίκτυο ΙΚΑΝΕΤ (βλέπε ενότητα 1.2.3.3) θεωρείται ένα έμπιστο και κλειστό δίκαιο

3.4.3.3 Διαδικασίες και Πολιτική Ασφάλειας

Πολιτική Ασφάλειας

Στα πλαίσια των συμβατικών της υποχρεώσεων ως ανάδοχος του έργου «Εκπόνηση Μελέτης Ασφάλειας Υποδομών Πληροφορικής και Επικοινωνιών και Σχέδιο Ανάκαμψης από Καταστροφή» την περίοδο 2011-2012 η εταιρεία Planet Consulting ανέλαβε την σύνταξη πολιτικής ασφάλειας καθώς και ενημέρωση των στελεχών του τότε ΙΚΑ. Η Πολιτική διαρθρώθηκε βάσει των προαναφερθέντων αξόνων του ISO 27001.

Η προτεινόμενη πολιτική ασφάλειας περιελάμβανε μια σειρά από λεπτομερώς διατυπωμένες διαδικασίες ασφάλειας για θέματα όπως η λήψη και ή φύλαξη αντιγράφων ασφάλειας, πρόληψη και αντιμετώπιση κακόβουλου λογισμικού κ.α. Ειδικά για την ασφαλή διαχείριση δεδομένων, περιλαμβανομένων των προσωπικών και ευαίσθητων, η πολιτική προέβλεπε:

- Τήρηση ενημερωμένου και κοστολογημένου καταλόγου πληροφοριακών πόρων
- Κατηγοριοποίηση των δεδομένων ανάλογα με τον βαθμό προστασίας που χρειάζονται βάσει ανάλυσης επικινδυνότητας και νομικών απαιτήσεων και χρήση της για εξουσιοδότηση των αποδεκτών της
- Καθορισμός των διαδικασιών χειρισμού της κάθε κατηγορίας δεδομένων από τον υπεύθυνο ασφάλειας

- Διασφάλιση της αρχής της μη αποποίησης - κάθε επεξεργασία θα πρέπει να μπορεί να μπορεί να αποδοθεί σε κάποιον

Σύμφωνα με προφορικές συζητήσεις με εργαζόμενους στη Γενική Διεύθυνση Πληροφοριακών Συστημάτων του ΕΦΚΑ, η πολιτική δεν τέθηκε σε γενική ισχύ και προσπάθειες που έχουν γίνει έκτοτε για την διαμόρφωση μιας νέας επίσημης πολιτικής δεν έχουν καρποφορήσει. Παρόλα αυτά, πολλές από τις προτάσεις που πρότεινε η πολιτική έχουν ενσωματωθεί στις πρακτικές του οργανισμού

Μελέτη ασφάλειας υποδομών

Η τελευταία μελέτη ασφάλειας υποδομών ΤΠΕ για τον οργανισμό έγινε το 2015 από την INTRASOFT στα πλαίσια της παροχής υπηρεσιών συμφωνημένου επιπέδου υποστήριξης της παραγωγικής λειτουργίας του ΟΠΣ-ΙΚΑ. Η μελέτη αφορούσε μόνο το συγκεκριμένο, σίγουρα κομβικής σημασίας για τον ΕΦΚΑ, ΠΣ.

Εγγραφή χρηστών - Απόδοση δικαιωμάτων

Οι χρήστες πληροφοριακών συστημάτων του ΕΦΚΑ αποκτούν πρόσβαση στα ΠΣ του φορέα με τη χρήση συνδυασμού ονόματος και κωδικού χρήστη. Τα διακριτικά εκδίδονται κεντρικά από τους διαχειριστές των συστημάτων, κατόπιν έγγραφης αίτησης που υπογράφεται από τον Διευθυντή του τμήματος όπου υπηρετεί ο χρήστης.

Λήψη αντιγράφων ασφαλείας (backups)

Οι διαχειριστές των πληροφοριακών συστημάτων του ΕΦΚΑ λαμβάνουν σε καθημερινή βάση αντίγραφα ασφαλείας των δεδομένων των συστημάτων. Τα αντίγραφα τηρούνται σε διαφορετική τοποθεσία από αυτή της εγκατάστασης

Συνέχιση της επιχειρησιακής λειτουργίας

Το ΙΚΑ είχε αναπτύξει εγχειρίδια όπου περιγράφονται οι διαδικασίες που πρέπει να ακολουθηθούν σε περίπτωση μη διαθεσιμότητας των συστημάτων του Ιδρύματος. Τα εγχειρίδια είναι προσαρμοσμένα στις κύριες επιχειρησιακές περιοχές λειτουργιών του ΟΠΣ-ΙΚΑ και επιτρέπουν τη συνέχιση της υπηρεσιακής λειτουργίας με χειρόγραφες διαδικασίες και μέσα.

Ο ΕΦΚΑ πάντως δεν διαθέτει απομακρυσμένο Disaster Recovery Site ώστε τα ΠΣ να μπορούν να επαναλειτουργήσουν άμεσα σε περίπτωση ολοκληρωτικής καταστροφής των υπολογιστικών του κέντρων.

Ασφάλεια Δεδομένων στις Ηλεκτρονικές Υπηρεσίες

Για την είσοδο στις ηλεκτρονικές υπηρεσίες του ΕΦΚΑ από τους ασφαλισμένους και τους συνταξιούχους χρησιμοποιείται η υπηρεσία αυθεντικοποίησης της ΓΓΠΣ, η οποία περιγράφηκε στην ενότητα 1.2.3.5. Ειδικά για τους εργοδότες απαιτείται ιδιαίτερη πιστοποίηση και σε κάθε έναν αποδίδεται ένας μοναδικός κωδικός χρήστη και συνθηματικό. Τα διακινούμενα στοιχεία προστατεύονται με κρυπτογράφηση. Ο ΕΦΚΑ διαθέτει firewall με δυνατότητες εντοπισμού IDS/IPS[6] για την ασφάλεια των ηλεκτρονικών του υπηρεσιών.

3.2.3.1 Ασφάλεια και Ανθρώπινο Δυναμικό

Ο ΕΦΚΑ διαθέτει ένα πολύ μεγάλο αριθμό εργαζομένων, προερχόμενων από διαφορετικά οργανωσιακά περιβάλλοντα. Τα κεντρικά του γραφεία βρίσκονται συγκεντρωμένα στον νομό Αττικής ενώ οι υπόλοιπες εγκαταστάσεις του είναι διάσπαρτες ανά την ελληνική επικράτεια. Οι γνώσεις της πλειοψηφίας του ανθρώπινου δυναμικού για θέματα ασφαλείας περιορίζονται στην χρήση των συνθηματικών και, παρά τις κατά καιρούς προτάσεις που έχουν γίνει από την Διεύθυνση Πληροφορικής για εκστρατείες ενημέρωσης δεν έχει γίνει κάποια εκτεταμένη προσπάθεια. Ως Δημόσιοι Υπάλληλοι πάντως δεσμεύονται από το άρθρο 26 του Δημοσιυπαλληλικού κώδικα αναφορικά με την υποχρέωση τήρησης εχεμύθειας.

Ειδικά τα στελέχη πληροφορικής του ΕΦΚΑ έχουν αποκτήσει γνώσεις ασφάλειας ΤΠΕ μέσα από εκπαιδευτικά σεμινάρια που έχουν γίνει ιδιαίτερα σε τεχνικά αντικείμενα, αλλά και επάνω στο θέμα της οργάνωσης ενός συστήματος διαχείρισης ασφάλειας δεδομένων.

[6] IDS/IPS (Intrusion Detection System / Intrusion Prevention System) είναι ηλεκτρονικά συστήματα που επιβλέπουν τα δίκτυα, καταγράφουν τυχών παραβιάσεις ασφάλειας, τις παρεμποδίζουν και τις αναφέρουν στους διαχειριστές

4. Προσαρμογή Φορέων Κοινωνικής Ασφάλισης στις απαιτήσεις του GDPR

Όπως αναφέρθηκε στο κεφάλαιο 2.4.4, η ψήφιση του GDPR έχει σημαντικές επιπτώσεις στη λειτουργία των οργανισμών του Δημοσίου Τομέα οι οποίοι επεξεργάζονται προσωπικά δεδομένα στα πλαίσια της λειτουργίας τους, όπως στην περίπτωση των ΦΚΑ.

4.1 Οργάνωση

Η σημαντικότερη οργανωτική αλλαγή που επιφέρει ο GDPR στον ΕΦΚΑ και τον ΕΤΕΑΕΠ είναι η υποχρέωση ορισμού Υπεύθυνων Προστασίας Δεδομένων (ΥΠΔ). Υπάρχουν πολλές επιλογές που μπορούν να μελετηθούν ως προς το ποια θα είναι η οργανωτική μορφή:

Εξωτερικός ΥΠΔ: Ως μια μεταβατική λύση μέχρι την οριστικοποίηση του Οργανισμού των δύο φορέων, θα μπορούσαν να ορίσουν ως ΥΠΔ έναν εξωτερικό σύμβουλο, ο οποίος θα μπορούσε να παράσχει τεχνογνωσία η οποία πιθανόν να απουσιάζει από τους δύο οργανισμούς. Ο προσωρινός εξωτερικός ΥΠΔ θα συνεργαζόταν με την διοίκηση ώστε να οριστικοποιηθεί το πλάνο για την προσαρμογή του οργανισμού στις απαιτήσεις του GDPR

Κοινός ΥΠΔ ΦΚΑ: Οι δύο φορείς θα μπορούσαν να επιλέξουν να έχουν έναν κοινό ΥΠΔ. Μια λύση η οποία, πέρα από τα όποια πλεονεκτήματα κόστους, συμβαδίζει με την υπάρχουσα κατάσταση, αφού το μεγαλύτερο ποσοστό των προσωπικών δεδομένων που διαχειρίζονται οι δύο φορείς είναι κοινό, χρησιμοποιούν και οι δύο μητρώα της ΗΔΙΚΑ ενώ προβλέπεται να εξυπηρετούνται από το ίδιο ΟΠΣ.[7] Θα μπορούσε να μελετηθεί η δυνατότητα ο κοινός *ΥΠΔ* να επιβλέπει και συνεπικουρεί και την ΗΔΙΚΑ, ώστε να συνεισφέρει στην ομογενοποίηση των πρακτικών προστασίας προσωπικών δεδομένων στον τομέα της Κοινωνικής Ασφάλισης.

[7] Σύμφωνα με το σχέδιο προκήρυξης για το ΟΠΣ ΕΦΚΑ

Εσωτερικός ΥΠΔ σε κάθε φορέα: η πιθανότερη λύση, η οποία έχει ήδη προταθεί, είναι ο ΥΠΟ να αποτελεί μέρος του οργανισμού του κάθε φορέα. Εφόσον επιλεχθεί αυτή η κατεύθυνση, ιδεατά η θέση του ΥΠΔ θα περιλαμβάνεται ανεξάρτητο Τμήμα Προστασίας Δεδομένων στην Κεντρική Υπηρεσία του κάθε φορέα το οποίο θα αναφέρεται κατευθείαν στη Διοίκηση. Η αυτονομία του ΥΠΔ από τις υπόλοιπες διευθύνσεις θα βοηθήσει στην αποφυγή σύγκρουσης συμφερόντων.

Λόγω του μεγέθους των ΦΚΑ, ο ΥΠΔ θα χρειαστεί να διαθέτει ομάδα ατόμων να τον συνεπικουρούν στο έργο του και πρόσβαση σε όλους τους αναγκαίους πόρους για την εκτέλεση της αποστολής του. Θα πρέπει επίσης να προβλεφθεί στον κανονισμό πως θα διαθέτει πρόσβαση σε κάθε είδους δεδομένα και πρόσκληση σε σχεδιαζόμενες πράξεις επεξεργασίας. Οι ΦΚΑ πρέπει να ανακοινώσουν στην ΑΠΔΠΧ τα στοιχεία του ΥΠΔ, ο οποίος και θα αποτελεί το σημείο επαφής ανάμεσα στις δύο οντότητες.

4.2 Διάγνωση

Η εναρμόνιση με τον GDPR απαιτεί μια καταγραφή της υπάρχουσας κατάστασης αναφορικά με τα είδη, τις διαδικασίες και την αποθήκευση των δεδομένων. Η καταγραφή έχει ξεχωριστή σημασία για τους ΦΚΑ αφού η πρόσφατη και χρονικά πεπιεσμένη σύσταση τους δεν έχει επιτρέψει μια συνολική χαρτογράφηση των στοιχείων αυτών. Συνοπτικά, η διάγνωση της υπάρχουσας κατάστασης θα πρέπει να περιλαμβάνει τα ακόλουθα:

- Ποια προσωπικά δεδομένα/ποιών προσώπων συλλέγονται
- Πότε συλλέγονται, με ποιον τρόπο, και βάσει ποιας διάταξης
- Που και πως μεταφέρονται
- Που αποθηκεύονται - λογισμικό και μέσα αποθήκευσης
- Ποιός είναι ο χρόνος διαγραφής
- Είδη επεξεργασίας
- Πόσο ασφαλή είναι τα δεδομένα
- Με ποιους άλλους φορείς μοιράζονται τα δεδομένα

- Ποια είναι η εναρμόνιση με τον GDPR των εταιρειών με τις οποίες συνεργάζεται ο φορέας για επεξεργασία δεδομένων

Τα αποτελέσματα της διάγνωσης θα επιτρέψουν την δημιουργία Διαγραμμάτων Ροής Δεδομένων[8], καθώς και την διεξαγωγή μιας Ανάλυσης Αποκλίσεων[9] προκειμένου να χαρτογραφηθούν τα σημεία βελτίωσης των οργανισμών.

4.3 Εκτίμηση Αντικτύπου Προστασίας Δεδομένων

Η νομική υποχρέωση των ΦΚΑ είναι αμφίβολη. Σύμφωνα με τον Συνήγορο του Πολίτη, όταν η επεξεργασία αφορά έννομη υποχρέωση του υπευθύνου επεξεργασίας (αρ. 6 στ. γ) ή εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημοσίας εξουσίας (αρ. 6 στ. 3), έχει νομική βάση στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το εν λόγω δίκαιο ρυθμίζει την εκάστοτε συγκεκριμένη πράξη επεξεργασίας ή σειρά πράξεων και έχει διενεργηθεί ήδη εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων στο πλαίσιο της έγκρισης της εν λόγω νομικής βάσης, δεν απαιτείται νέα εκτίμηση αντικτύπου (Σουγλέ, 2018). Για τους ΦΚΑ συντρέχουν οι προϋποθέσεις της έννομης υποχρέωσης, όμως υπάρχει και η προϋπόθεση της προηγούμενης Εκτίμησης Αντικτύπου, η οποία μένει να διευθετηθεί αν καλύπτεται από αυτήν που έχει κατά το παρελθόν το ΙΚΑ, στην περίπτωση του ΕΦΚΑ. Σε κάθε περίπτωση πάντως θα απαιτηθεί ΕΑΠΔ για τις επεξεργασίες του ΕΦΚΑ που αφορούν δεδομένα υγείας.

Πέρα από την νομική απαίτηση, η διενέργεια μιας ΕΑΠΔ μπορεί να συνεισφέρει θετικά στην προστασία των προσωπικών δεδομένων που τηρούν οι ΦΚΑ. Η προαναφερθείσα διαδικασία διάγνωσης αποτελεί ένα εκ των νομικά υποχρεωτικών τμημάτων μιας ΕΑΠΔ ενώ ο GDPR στο αρ. 15 π.7 προβλέπει επίσης εκτίμηση της αναγκαιότητας και αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς τους, εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων και τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων ώστε να διασφαλίζεται η προστασία των δεδομένων και η συμμόρφωση προς τον. Όλα στοιχεία απαραίτητα για την πολιτική προστασίας ενός οργανισμού.

[8] Διάγραμμα ροής δεδομένων (Data Flow Mapping)
[9] Ανάλυση Αποκλίσεων (Gap Analysis)

4.4 Αναδιοργάνωση εσωτερικών διαδικασιών

4.4.1 Ικανοποίηση δικαιωμάτων υποκείμενων δεδομένων

Ο GDPR επαναβεβαιώνει μια σειρά από δικαιώματα των υποκείμενων των προσωπικών δεδομένων, ενώ αποδίδει και κάποια νέα. Αυτά τα δικαιώματα όμως δημιουργούν και μια σειρά υποχρεώσεων στους Υπεύθυνους Επεξεργασίας Δεδομένων ώστε να εκπληρώσουν τις απαιτήσεις που θα προκύψουν.

Καταρχάς το **δικαίωμα στην πρόσβαση** στα δεδομένα χωρίς περαιτέρω αιτιολόγηση υποχρεώνει τους ΦΚΑ να δημιουργήσουν διαδικασία απόδοσης των δεδομένων του σε οποιονδήποτε υποκείμενο τους τα αιτηθεί και βέβαια την δημιουργία σχετικής φόρμας και επιλογή εύλογων και αναλογικών μέσων επαλήθευσης της ταυτότητας του αιτούντα. Η διαδικασία αναμένεται να είναι ιδιαίτερα απαιτητική για τους ΦΚΑ αφού προσωπικά δεδομένα περιέχονται και στην ασφαλιστική ιστορία των εργαζομένων, μέρος της οποίας βρίσκεται διάσπαρτη σε έγχαρτα αρχεία. Ο GDPR προβλέπει και την παροχή δυνατότητας ηλεκτρονικής υποβολής σχετικών αιτημάτων, οπότε πρέπει να γίνουν και οι σχετικές τροποποιήσεις στους δικτυακούς των φορέων.

Η εκπλήρωση του **δικαιώματος διόρθωσης,** δηλαδή της διόρθωσης ανακριβών δεδομένων και της συμπλήρωσης ελλιπών, αφού ανάλογες διαδικασίες προβλέπονται ήδη, ενώ ενδεικτικά στον ιστότοπο του ΕΦΚΑ λειτουργεί και ηλεκτρονική υπηρεσία η οποία επιτρέπει την μεταβολή των ατομικών στοιχείων του ασφαλισμένου.

4.4.2 Δικαιώματα εργαζομένων

Πέρα από τα δικαιώματα των εξωτερικών συναλασσόμενων με τους ΦΚΑ, οι τελευταίοι πρέπει να τηρούν τα δικαιώματα και των εργαζομένων τους αναφορικά με το απόρρητο των επικοινωνιών, των δεδομένων θέσης και της αλληλογραφίας που προβλέπει ο GDPR. Ωφείλουν να παράσχουν την σχετική ενημέρωση, να φροντίσουν να χρησιμοποιούν τα δεδομένα των εργαζομένων σύμφωνα με την αρχή της αναλογικότητας και να εφαρμόσουν τις αρχές αυτές και στις προδιαγραφές των ΠΣ τους.

4.4.3 Ασφάλεια δεδομένων

Οι ΦΚΑ πρέπει να σχεδιάσουν ή να επικαιροποιήσουν τις διαδικασίες που αφορούν (Παναγοπούλου, 2018):

Σχέδιο ανάκαμψης από καταστροφές: Συμπεριλαμβάνει τις βασικές διαδικασίες που ακολουθούνται για την προστασία των προσωπικών δεδομένων σε περιπτώσεις έκτακτων περιστατικών

Διαχείριση Χρηστών: Η διαδικασία πρέπει να εξασφαλίζει πως οι εκτελεστές της επεξεργασίας έχουν πρόσβαση μόνο στα δεδομένα που απαιτούνται για την εκτέλεση της εργασίας τους (πχ το τμήμα συντάξεων δεν πρέπει να έχει πρόσβαση σε ιατρικά δεδομένα που αφορούν τις παροχές)

Εκτελούντες την επεξεργασία: Οι συμβάσεις με τρίτους που εκτελούν την επεξεργασία, όπως συμβαίνει πχ με τις SLA για υποστήριξη πληροφοριακών συστημάτων πρέπει να συμπεριλαμβάνουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού. Επίσης θα πρέπει να λαμβάνεται σχετική άδεια από την ΑΠΔΠΧ. Να σημειωθεί πως σε τυχόν παραβίαση του κανονισμού από τον υπό σύμβαση εκτελούντα βαραίνει τους ΦΚΑ ως υπεύθυνους επεξεργασίας.

Διαχείριση φυσικού αρχείου: Οι ΦΚΑ οφείλουν να ορίσουν υπεύθυνους διαχείρισης των φυσικών αρχείων, τα οποία ακόμα αφθονούν σε αυτούς. Επίσης, πρέπει να οριστεί και να τηρείται κατάλληλη διαδικασία καταγραφής των προσβάσεων σε αυτά, ώστε να υπάρχει διαφάνεια στη διαχείριση.

Καταστροφή δεδομένων: Απαιτείται εφαρμογή κατ' ελάχιστο της Οδηγίας 1/2005 της ΑΠΔΠΧ ώστε να διασφαλίζεται η ασφαλής καταστροφή των δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας

Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων: Ο GDPR απαιτεί την καταγραφή όλων των περιστατικών παραβίασης της ιδιωτικότητας και την κοινοποίηση τους εντός 72 ωρών από την ανακάλυψη τους στην ΑΠΔΠΧ και στα υποκείμενα των δεδομενων εφόσον πρόκειται για περιστατικά υψηλού κινδύνου. Οι

ΦΚΑ καλούνται να αναπτύξουν διαδικασίες καταγραφής, αξιολόγησης και κοινοποίησης των περιστατικών.

Επίλογος

Η μελέτη της τήρησης των προσωπικών δεδομένων στα Πληροφοριακά Συστήματα των Φορέων Κοινωνικής Ασφάλισης χρησιμεύει για την εξαγωγή κάποιων συμπερασμάτων τα οποία πιθανόν να ξεφεύγουν από το πλαίσιο της παρούσας εργασίας.

Καταρχάς κατάδειξε την, σύνηθη, απόσταση ανάμεσα στο ρυθμιστικό πλαίσιο και την εργασιακή πρακτική στο Δημόσιο. Η Ελλάδα διαθέτει ένα σύγχρονο ρυθμιστικό πλαίσιο ύστερα από την ψήφιση του ν. 2472/97 και μια δραστήρια Ανεξάρτητη Αρχή η οποία επιβλέπει την εφαρμογή του. Η πρόσφατη επικύρωση του GDPR από το Ευρωπαϊκό Κοινοβούλιο δεν αποτελεί μια ανατροπή του ήδη ισχύοντα νόμου αλλά συμπλήρωση και επέκταση. Παρόλα αυτά και από το γεγονός πως από την ψήφιση του αρχικού νόμου έχουν παρέλθει περισσότερες δύο δεκαετίες, οι Φορείς Κοινωνικής Ασφάλισης, οι οποίοι πλέον έχουν συρρικνωθεί σε μόλις δύο, εμφανίζονται ανέτοιμοι να προσαρμοστούν στις απαιτήσεις της νομοθεσίας.

Τα αίτια αυτής της υστέρησης μπορούν να αναζητηθούν στις οργανωτικές δυσανεξίες των Φορέων Κοινωνικής Ασφάλισης. Η πολυδιάσπαση σε μικρούς φορείς δεν επέτρεψε οικονομίες κλίμακας οι οποίες θα καθιστούσαν ικανή την επένδυση σε ΤΠΕ και την δημιουργία μιας υλικής υποδομής αλλά και οργανωτικής κουλτούρας ασφάλειας των δεδομένων. Δεν είναι συμπτωματικό πως οι δύο μεγαλύτεροι ΦΚΑ προ της δημιουργίας του ΕΦΚΑ, το ΙΚΑ και ο ΟΓΑ, διέθεταν τα πληρέστερα Πληροφοριακά Συστήματα και το πρώτο είχε προβεί στις απαιτούμενες ενέργειες για συμμόρφωση με τον 2472/96. Επιπλέον, οι σχετικά συχνές αλλαγές της νομοθεσίας αναφορικά με την ανάπτυξη των ΤΠΕ στην Κοινωνική Ασφάλιση από τα τέλη της δεκαετίας του ‘70 και ύστερα, η διάχυση της ευθύνης ανάμεσα σε Υπουργείο, ΚΗΥΚΥ και Φορείς δημιούργησε αποτρεπτικά στην καθιέρωση κοινών πρακτικών αναφορικά με την τήρηση και επεξεργασία των προσωπικών δεδομένων.

Η πρόσφατη συγχώνευση των ΦΚΑ με τον ν. 4387/2016 δημιούργησε της προϋποθέσεις για την δημιουργία βιώσιμων ΦΚΑ οι οποίοι θα αξιοποιούν τις ΤΠΕ προκειμένου να παρέχουν ποιοτικές υπηρεσίες στα ενδιαφερόμενα μέρη με χαμηλότερο

κόστος. Η ευσπευσμένη όμως δημιουργία των δύο Φορέων σε συνδυασμό με τις ελλείψεις ανθρωπίνου δυναμικού έχει ως αποτέλεσμα οι περιορισμένοι ανθρώπινοι πόροι στα τμήματα Πληροφορικής να έχουν επικεντρωθεί στην κάλυψη πιο επειγουσών αναγκών προκειμένου να εκτελούνται οι πιο βασικές υπηρεσίες όπως η απόδοση συντάξεων. Παρά την ενημερότητα αναφορικά με τον GDPR, η σχετική προετοιμασία δεν έχει ολοκληρωθεί.

Οι απαιτήσεις του GDPR αποτελούν όμως μια ευκαιρία για τους νεοσύστατους ΦΚΑ. Ευκαιρία να εφαρμόσουν τις αρχές της προστασίας των δεδομένων από τον σχεδιασμό (*privacy by design*) καθώς αναπτύσσονται οι νέες διαδικασίες τους και οι προδιαγραφές του ΟΠΣ-ΕΦΚΑ. Μια τέτοια επιλογή θα επιτρέψει στους νέους ΦΚΑ να προσφέρουν όχι μόνο καλύτερες υπηρεσίες αλλά να συνεισφέρουν με επιπλέον τρόπους στην προστασία των πολιτών από κινδύνους, την ουσία δηλαδή του σκοπού τους.

Βιβλιογραφία

Ξενόγλωσση

Council, OECD (2014). OECD Recommendation on Digital Government Strategies.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). *Privacy and Data Protection by Design-from policy to engineering*. Διαθέσιμο στο: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design [Προσπελάστηκε στις 10/12/2018]

DeCew, Judith, (2018).Privacy. στο Edward N. Zalta (ed.) *The Stanford Encyclopedia of Philosophy*. Διαθέσιμο στο: https://plato.stanford.edu/archives/spr2018/entries/privacy [Πρόσβαση 10/12/2018]

Gellman, R. (2017). *Fair information practices: A basic history*. Διαθέσιμο στο: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf [Προσπελάστηκε στις 8/12/2018]

Grönlund, Å. & Horan, T. (2005). Introducing e-Gov: History, Definitions, and Issues. *Communications of the Association for Information Systems*, 15(1), pp. 713 - 729.

Laudon, K. C., & Laudon, J. P. (2011). *Essentials of management information systems*. Upper Saddle River: Pearson.

Rosenberg, R. (1992). *The Social Impact of Computers*. San Diego: Academic Press.

Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. L. Rev.,* 154, 477.

Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. (1973). *Records, Computers, and the Rights of Citizens: Report*. Mit Press.

Virilio, P. (2007). *The Original Accident*, Cambridge: Polity, 2007

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Ελληνική

Αλεξανδροπούλου-Αιγυπτιάδου Ε. (2002). *Ζητήματα από το δίκαιο της πληροφορικής*. Αθήνα: Σάκκουλας

Αριστοτέλης. *Ηθικά Νικομάχεια*

Γκρίτζαλης, Δ. (2004). *Ασφάλεια Πληροφοριακών Συστημάτων σε Περιβάλλοντα Υψηλής Ευπάθειας*. Σάμος: Πανεπιστήμιο Αιγαίου.

Ευρωπαϊκή Ένωση:Ευρωπαϊκή Επιτροπή, *Ανακοίνωση της Επιτροπής προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών - Ο ρόλος της ηλεκτρονικής διακυβέρνησης για το μέλλον της Ευρώπης*, COM(2003) 0567 τελική, διαθέσιμη στο https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0567:FIN:EN:PDF

ΗΔΙΚΑ (2012). Εθνικό Μητρώο ΑΜΚΑ. Διαθέσιμο στο: http://www.idika.gr/etaireia/erga/amka [Προσπελάστηκε στις 2 Δεκεμβρίου 2018]

Συμβούλιο της Ευρώπης, (1950). *Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (4 Νοεμβρίου 1950)*.
Διαθέσιμη στο: http://www.echr.coe.int/Documents/Convention_ELL.pdf
[Προσπελάστηκε
στις 20 Νοεμβρίου 2018]

Καλλονιάτης, Χ. (2011). *Ασφάλεια Δεδομένων στην Κοινωνία της Πληροφορίας - Ιδιωτικότητα*, Μυτιλήνη: Πανεπιστήμιο Αιγαίου.

Κοινωνία της Πληροφορίας, (2008). *Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας*, Αθήνα: Κοινωνία της Πληροφορίας.

Ηνωμένα Έθνη, Γενική Συνέλευση, (1948). *Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου (10 Δεκεμβρίου 1948)*. Διαθέσιμη στο: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=grk [Προσπελάστηκε στις 20 Νοεμβρίου 2018]

Κιουντούζης, Ε. (2009). *Μεθοδολογίες ανάλυσης και σχεδιασμού πληροφοριακών συστημάτων*. Αθήνα: Εκδόσεις Μπένου .

Κοκκολάκης, Σ., Γκρίτζαλης, Σ., Καρύδα, Μ., Λάμπρου, Κ. (2002). *Μελέτη Ασφάλειας Ολοκληρωμένου Πληροφοριακού Συστήματος ΟΠΣ-ΙΚΑ*

Μήτρου, Λ. (2010). Η Προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες. Η νομική διάσταση. Σε: Λαμπρινουδάκης, Κ (Επιμ.) *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών*. Αθήνα: Παπασωτηρίου, σελ. 505 - 552.

Μήτρου, Λ. (2006). *Προστασία Προσωπικών Δεδομένων*. Σάμος: Πανεπιστήμιο Αιγαίου.

Παναγοπούλου, Γ. (2018). *Γενικός Κανονισμός Προστασίας Δεδομένων Οι υποχρεώσεις της Δημόσιας Διοίκησης*. Ημερίδα ΕΚΔΔΑ

Παπακωνσταντίνου, Ε. (2006). *Νομικά Θέματα Πληροφορικής.* Αθήνα: Σάκκουλας

Planet Consulting. (2011). *ΙΚΑ - Εκπόνηση Μελέτης Ασφάλειας Υποδομών Πληροφορικής και Επικοινωνιών και Σχέδιο Ανάκαμψης από Καταστροφή*. Αθήνα: Planet Consulting

Σαγκριώτου, Φ. (2000). *Η Πληροφορική στην Κοινωνική Ασφάλιση*. Αθήνα: Γενική Γραμματεία Κοινωνικών Ασφαλίσεων, Δ/νση Μηχανογραφικών Εφαρμογών

Σιουγλέ, Ευφ. (2018). *Γενικός Κανονισμός Προστασίας Δεδομένων: Οι υποχρεώσεις της δημόσιας διοίκησης*. Ημερίδα ΕΚΔΔΑ

Τράμπας, Ν. (2010). *Το πληροφοριακό σύστημα ΟΠΣ-ΙΚΑ, ανάλυση περιεχομένου σελίδας, προτάσεις βελτίωσης ηλεκτρονικού management*. Κοζάνη: ΤΕΙ Δυτικής Μακεδονίας

Παράρτημα

Παράρτημα ΙΙ Διακήρυξης 1658635/22-12-17

2. ΥΦΙΣΤΑΜΕΝΗ ΚΑΤΑΣΤΑΣΗ

Η Πληροφοριακή Υποδομή του Ενιαίου Φορέα Κοινωνικής Ασφάλισης, αποτελείται από τα διαφορετικά πληροφοριακά συστήματα των συγχωνευθέντων Φορέων Κοινωνικής Ασφάλισης (ΦΚΑ) και τις Ηλεκτρονικές Υπηρεσίες που παρέχονται μέσω διαδικτύου σε πολίτες, επιχειρήσεις και φορείς.

Ειδικότερα, το πληροφοριακό σύστημα του ΕΦΚΑ Μισθωτών αποτελείται από τις παρακάτω υποδομές - πλατφόρμες:

1. Ολοκληρωμένο Πληροφοριακό Σύστημα Μισθωτών (ΟΠΣ - ΕΦΚΑ Μισθωτών)
2. Δίκτυο ευρείας περιοχής (WAN) του ΕΦΚΑ Μισθωτών - ΙΚΑΝΕΤ
3. Διαδικτυακός τόπος του πρώην ΙΚΑ – ΕΤΑΜ και Ηλεκτρονικές Υπηρεσίες προς μισθωτούς, εργοδότες, οφειλέτες και φορείς.
4. Ενιαίο Μητρώο Ασφαλισμένων ΕΦΚΑ
5. Σύστημα Εισφορών Μη Μισθωτών
6. Σύστημα Ηλεκτρονικών Κατασχέσεων εις χείρας Πιστωτικών Ιδρυμάτων

2.1 ΟΛΟΚΛΗΡΩΜΕΝΟ ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ ΜΙΣΘΩΤΩΝ (ΟΠΣ - ΕΦΚΑ ΜΙΣΘΩΤΩΝ)

Το ΟΠΣ-τ.ΙΚΑ είχε εγκατασταθεί αρχικά σε περίπου 300 σημεία εγκατάστασης (μεταξύ των οποίων 164 Υποκ/τα και 127 Παρ/τα), με περίπου 9.000 χρήστες, οι οποίοι εκτελούσαν περίπου 120.000 συναλλαγές ημερησίως. Σήμερα το ΟΠΣ- ΕΦΚΑ Μισθωτών (πρώην ΟΠΣ – ΙΚΑ) λειτουργεί πλέον των 200 σημείων εγκατάστασης με 6.000 χρήστες.

Το ΟΠΣ - ΕΦΚΑ Μισθωτών είναι **ένα ιδιαίτερα πολύπλοκο έργο πληροφορικής**. Για την υλοποίηση του λογισμικού του ΕΦΚΑ Μισθωτών, έχουν δημιουργηθεί περίπου 15.000 προγραμματιστικά αντικείμενα (πίνακες της βάσης δεδομένων, όψεις της βάσης δεδομένων, συναρτήσεις και triggers). Το **μέγεθος των Βάσεων Δεδομένων του ΕΦΚΑ Μισθωτών,** είναι σήμερα της τάξεως των **7 TB** και αυξάνεται σε καθημερινή βάση.

2.1.1 Επιχειρησιακές Λειτουργίες ανά Υποσύστημα

Στον πίνακα που ακολουθεί παρατίθενται οι λειτουργίες των επιχειρησιακών περιοχών που υποστηρίζονται από το ΟΠΣ ΕΦΚΑ Μισθωτών:

ΠΑΡΟΧΕΣ
Επιχειρησιακές Λειτουργίες
Έξοδα Κηδείας

Επίδομα Ασθενείας
Επίδομα Μητρότητας
Δώρου Επιδόματος
Ατύχημα - Επαγγελματική Ασθένεια
Αναδρομικά
Καταλογισμός
WORKFLOW ΣΥΝΤΑΞΕΩΝ
Επιχειρησιακές Λειτουργίες
Πρωτόκολλο Ροής Εργασιών Συντάξεων
Εισερχόμενο Πρωτόκολλο
Εξερχόμενο Πρωτόκολλο
Διαχείριση Εργασιών
ΑΝΑΓΚΑΣΤΙΚΑ ΜΕΤΡΑ
Επιχειρησιακές Λειτουργίες
Υποθήκη
Παραγγελίες Κατασχέσεων
Κατάσχεσης Ακινήτων
Κατάσχεσης Κινητών
Κατάσχεσης εις χείρας τρίτου
Πλειστηριασμός
Πτώχευση
ΕΙΣΦΟΡΕΣ
Επιχειρησιακές Λειτουργίες
Μητρώο Εργοδοτών Κοινών Επιχειρήσεων
Μητρώο Οικοδομοτεχνικών Έργων
Μητρώο Ειδικών Κατηγοριών Ασφάλισης
ΑΠΔ
Έλεγχος Δηλωθέντων Καταβληθέντων
Ουσιαστικός Έλεγχος Εργοδοτών
Ασφαλιστική Ενημερότητα
Καταγγελία Ασφαλισμένου
Πράξεις Επιβολής
Έντυπα Εισφορών ΕΕ
Οικονομικές Κινήσεις Εργοδοτών
Διαχείριση ασφαλιστικής Ιστορίας

Διαχείριση Αποφάσεων Εισφορών
Ασφάλιση Ειδικών Κατηγοριών
Εργόσημο
Είσπραξη Τρεχουσών Εισφορών
Προαιρετική Ασφάλιση
Αναγνώριση Χρόνου Ασφάλισης
Εκθέσεις Επιτόπιων Ελέγχων
ΚΑΘΥΣΤΕΡΟΥΜΕΝΕΣ ΕΙΣΦΟΡΕΣ – ΟΦΕΙΛΕΣ – Κ.Ε.Α.Ο.
Επιχειρησιακές Λειτουργίες
Μητρώο Οφειλετών
Οικονομικές Κινήσεις Οφειλέτη
Ρυθμίσεις Οφειλών
Παραγραφόμενες – Παραγραμμένες Οφειλές
Είσπραξη Καθυστερούμενων Οφειλών
Εισπράξεις μέσω Ηλεκτρονικών Κατασχέσεων
Είσπραξη Δόσεων Ρύθμισης
Βεβαίωση Οφειλών
Ατομικές Ειδοποιήσεις
Μηνύσεις
Ένδικα Μέσα
ΜΗΤΡΩΟ ΑΣΦΑΛΙΣΜΕΝΩΝ
Επιχειρησιακές Λειτουργίες
Εμφάνιση Στοιχείων Ασφαλισμένου
Έντυπα Μητρώου Ασφαλισμένων Ε.Ε.
Ασφαλιστική Ικανότητα
Ασφαλιστική Ικανότητα Ανέργων ΟΑΕΔ
Βεβαιώσεις Μητρώου Ασφαλισμένων
ΔΙΑΧΕΙΡΙΣΗ ΑΠΟΘΕΜΑΤΩΝ
Επιχειρησιακές Λειτουργίες
Χορηγήσεις - Συμβάσεις - Εγγυητικές
Διαχείριση Μητρώου Ειδών
Αιτήσεις Προμήθειας
Κινήσεις Αποθήκης
Φυσική Απογραφή
Διαχείριση Παγίων Στοιχείων

ΒΟΗΘΗΤΙΚΗ ΛΟΓΙΣΤΙΚΗ
Επιχειρησιακές Λειτουργίες
Διαχείριση Συναλλασσομένων
Διαχείριση Φορολογικών Παραστατικών
Βεβαιωτικά Σημειώματα Εσόδων
Αποφάσεις Ανάληψης Υποχρέωσης
Μητρώο Δεσμεύσεων
Φύλλα Εκκαθάρισης
Εντάλματα – Γραμμάτια Είσπραξης
Ταμειακές Κινήσεις
ΓΕΝΙΚΗ ΛΟΓΙΣΤΙΚΗ
Επιχειρησιακές Λειτουργίες
Διαχείριση Λογιστικών Πράξεων
Οικονομικές Αναφορές
Λογιστικοποίηση Συναλλαγών
ΠΡΟΥΠΟΛΟΓΙΣΤΙΚΗ ΛΟΓΙΣΤΙΚΗ
Επιχειρησιακές Λειτουργίες
Διαχείριση Προϋπολογισμού
Μεταφορές Πιστώσεων
Παρακολούθηση εκτέλεσης Προϋπολογισμού
ΣΥΝΤΑΞΕΙΣ
Επιχειρησιακές Λειτουργίες
Αιτήσεις Απονομών / Μεταβολών
Θεμελίωση Δικαιώματος
Διαχείριση Χρόνων Ανακεφαλαίωσης
Αποφάσεις Συνταξιοδότησης
Πληρωμές Συντάξεων
Προσωρινές Συντάξεις
Παραμετροποίηση Διατάξεων
ΚΕ.Π.Α.
Επιχειρησιακές Λειτουργίες
Διαχείριση Μητρώου Αιτούντων Πιστοποίησης
Υγειονομικές Επιτροπές

Μητρώο Ιατρών
Πλάνο Εργασιών ΚΕΠΑ
Αιτήσεις Πιστοποίησης Αναπηρίας
Αποφάσεις Πιστοποίησης Αναπηρίας
Διαχείριση Ενστάσεων
ΚΑΤ' ΟΙΚΟΝ ΦΡΟΝΤΙΔΑ ΣΥΝΤΑΞΙΟΥΧΩΝ
Επιχειρησιακές Λειτουργίες
Αίτηση συμμετοχής Παρόχου
Έλεγχος δικαιολογητικών-κριτηρίων
Συμβάσεις
Αίτηση Συμμετοχής Ωφελούμενου
Έλεγχος Κριτηρίων Ωφελούμενου
Δήλωση Παροχής Υπηρεσιών
Εκκαθάριση Δήλωσης

2.1.2 Εξοπλισμός Ολοκληρωμένου Πληροφοριακού Συστήματος

ΚΕΝΤΡΙΚΗ ΥΠΟΛΟΓΙΣΤΙΚΗ ΥΠΟΔΟΜΗ

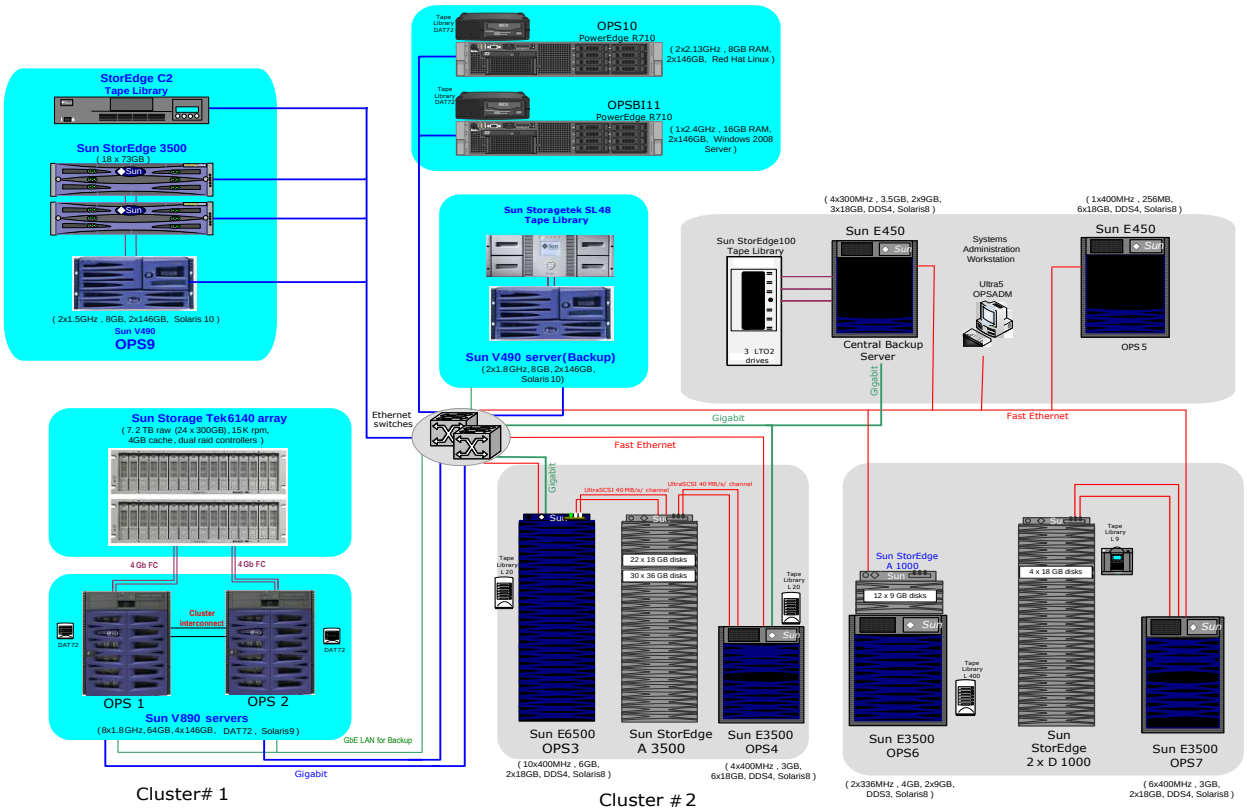
Η κεντρική υπολογιστική υποδομή αποτελείται από Unix-based και Windows-based εξυπηρετητές καθώς και ενεργό δικτυακό εξοπλισμό, όπως φαίνεται στον πίνακα που ακολουθεί :

Hardware	Λογισμικό / Λειτουργικότητα	Ποσότητα
Servers SUN V890	SUN Solaris / Υποστήριξη εφαρμογών του ΟΠΣ-ΕΦΚΑ Μισθωτών (OPS1, OPS2)	2
Servers SUN 6500	SUN Solaris / Υποστήριξη εφαρμογών του ΟΠΣ-ΕΦΚΑ Μισθωτών (OPS3)	1
Servers SUN 3500	SUN Solaris / Υποστήριξη Παραγωγής Στατιστικών (OPS4)	1
Server SUN V490	SUN Solaris / Backup Server	1
Server SUN V490	SUN Solaris / Υποστήριξη διασυνδέσεων ΟΠΣ- ΕΦΚΑ Μισθωτών με Διακτυακό Τόπο (OPS9)	1
SUN Storage Tek 6140	Storage Area Network	1
Sun StorageTek SL48	Σύστημα τήρησης αντιγράφων ασφαλείας	1
Server DELL R710	Red Hat Linux / DB Server για χρήση από το Datawarehouse του Συστήματος Ανάλυσης Επικινδυνότητας (OPS 10)	1
Server DELL R710	Windows 2008 R2 Server / Υποστήριξη Συστήματος	1

	Ανάλυσης Επικινδυνότητας (OPS BI 11)	
Intel Based Domain Servers	Windows 2000 Server / Active Directory – Microsoft Domain Servers, Διαχείριση του συστήματος και του δικτύου	12
Εκτυπωτές Line		13
Routers		28
Switches		30

Πίνακας 1: Κεντρική Υπολογιστική Υποδομή

Στο Σχήμα που ακολουθεί, παρουσιάζεται η αρχιτεκτονική της Κεντρικής Υπολογιστικής Υποδομής ΟΠΣ-ΕΦΚΑ Μισθωτών, όπως έχει διαμορφωθεί σήμερα:



Εικόνα 2: Αρχιτεκτονική της Κεντρικής Υπολογιστικής Υποδομής ΟΠΣ-ΕΦΚΑ Μισθωτών

ΠΕΡΙΦΕΡΕΙΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ

Στα Υποκαταστήματα έχουν εγκατασταθεί τοπικοί Windows Servers, σταθμοί εργασίας και λοιπός εξοπλισμός, σύμφωνα με τον παρακάτω πίνακα:

ΕΙΔΟΣ	ΛΟΓΙΣΜΙΚΟ	ΠΟΣΟΤΗΤΑ

LAN Servers (HP)	Windows 2000 Server	70
LAN Servers (IBM)	Windows 2000 Server	180
LAN Servers (Fujitsu Siemens)	Windows 2000 Server	140
UPS (Liebert)		70
UPS (Meta Systems ALLY)		320
Σταθμοί Εργασίας (HP)	Windows 2000 Professional Greek	2.620
Σταθμοί Εργασίας (IBM)	Windows 2000 Professional Greek	3.900
Σταθμοί Εργασίας (Fujitsu Siemens)	Windows XP Professional Greek	2.712
Εκτυπωτές DOT-MATRIX 80 Στηλών (OKI)		6.051
Εκτυπωτές DOT-MATRIX 132 Στηλών Network (Compuprint)		500
Εκτυπωτές DOT-MATRIX 132 Στηλών Network (OKI)		1.130
Εκτυπωτές LASER (HP 2200 Network)		250
Εκτυπωτές LASER (OKI B6200 Network)		1.660
Εκτυπωτές LASER (OKI B4400)		712

Πίνακας 2: Περιφερειακός Εξοπλισμός

ΛΟΙΠΟΣ ΕΞΟΠΛΙΣΜΟΣ

1. Ενοποιημένο Περιβάλλον Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών *(Πατησίων 12)*

Στον Server του Ενοποιημένου Περιβάλλοντος τηρούνται επί μέρους αντίγραφα των δεδομένων της Κεντρικής Υπολογιστικής Υποδομής και εγκαθίστανται τα αντικείμενα Λογισμικού, τα οποία είναι σε φάση ελέγχου από τα στελέχη του ΕΦΚΑ, πριν την τελική εγκατάσταση αυτών στο περιβάλλον παραγωγής.

Ο **εξοπλισμός του ενοποιημένου περιβάλλοντος,** έχει ως ο **ΠΙΝΑΚΑΣ** που ακολουθεί:

ΕΞΟΠΛΙΣΜΟΣ ΕΝΟΠΟΙΗΜΕΝΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΣΥΝΕΡΓΑΣΙΑΣ ΟΜΑΔΩΝ ΕΡΓΟΥ		
ΕΙΔΟΣ	**ΛΟΓΙΣΜΙΚΟ**	**ΠΟΣΟΤΗΤΑ**
Κεντρικοί Servers (SUN)	Sun Solaris	1
LAN Servers (HP)	Windows 2000 Server	4
Σταθμοί Εργασίας (HP)	Windows 98	100

Εκτυπωτές DOT-MATRIX 80 Στηλών (OKI)		80
UPS (Liebert)		2
Router (Cisco)		1
Switch (Cisco)		8

Πίνακας 3: Εξοπλισμός του ενοποιημένου περιβάλλοντος

2. Περιβάλλον Ανάπτυξης και Ελέγχου Λογισμικού Εφαρμογών από τον Ανάδοχο (Πλατφόρμα Ανάπτυξης) (Πατησίων 12)

Ο **Εξοπλισμός της Πλατφόρμας Ανάπτυξης,** έχει ως ο **ΠΙΝΑΚΑΣ** που ακολουθεί:

ΕΞΟΠΛΙΣΜΟΣ ΠΛΑΤΦΟΡΜΑΣ ΑΝΑΠΤΥΞΗΣ		
ΕΙΔΟΣ	**ΛΟΓΙΣΜΙΚΟ**	**ΠΟΣΟΤΗΤΑ**
Κεντρικοί Servers (SUN)	Sun Solaris	2
LAN Servers (HP)	Windows 2000 Server	4
Σταθμοί Εργασίας (HP)	Windows 2000 Professional Greek	100
Εκτυπωτές Line (Tally)		1
Εκτυπωτές DOT-MATRIX 132 Στηλών (Compuprint SIGNUM)		5
Εκτυπωτές DOT-MATRIX 80 Στηλών (OKI)		7
Εκτυπωτές LASER (HP)		16
UPS (Liebert)		2
Router (Cisco)		4
Switch (Cisco)		39

Πίνακας 4: Εξοπλισμός της Πλατφόρμας Ανάπτυξης

3. Περιβάλλον Εκπαίδευσης τελικών χρηστών (Παπαδιαμαντοπούλου 87)

Το **Περιβάλλον Εκπαίδευσης Τελικών Χρηστών,** έχει ως ο **ΠΙΝΑΚΑΣ** που ακολουθεί:

ΕΙΔΟΣ	**ΛΟΓΙΣΜΙΚΟ**	**ΠΟΣΟΤΗΤΑ**
Κεντρικοί Servers (SUN)	Sun Solaris	1
LAN Servers (HP)	Windows 2000 Server	4
UPS (Meta Systems ALLY)		4
Σταθμοί Εργασίας (HP)	Windows 2000 Professional Greek	300
Εκτυπωτές DOT-MATRIX 80 Στηλών (OKI)		167
Εκτυπωτές DOT-MATRIX 132 Στηλών Network		31

(OKI)		
Εκτυπωτές LASER (HP)		44

Πίνακας 5: Εξοπλισμός Περιβάλλοντος Εκπαίδευσης Τελικών Χρηστών

4. Περιβάλλον συλλειτουργίας λογισμικού Εφαρμογών Συντάξεων ΟΠΣ-ΕΦΚΑ Μισθωτών με Η.ΔΙ.ΚΑ. (Παπαδιαμαντοπούλου 87)

Το **Περιβάλλον Συλλειτουργίας Λογισμικού Εφαρμογών Συντάξεων ΟΠΣ- ΕΦΚΑ Μισθωτών με Η.ΔΙ.ΚΑ.,** έχει ως ο **ΠΙΝΑΚΑΣ** που ακολουθεί:

ΕΙΔΟΣ	ΛΟΓΙΣΜΙΚΟ	ΠΟΣΟΤΗΤΑ
Κεντρικοί Servers (SUN)	Sun Solaris	1
Firewalls (Cisco PIX)		2

5. ΣΥΣΤΗΜΑ ΑΜΕΣΗΣ ΒΟΗΘΕΙΑΣ (HELP DESK) (Πατησίων 12)

Η Υποστήριξη Λειτουργίας του Γραφείου Άμεσης Βοήθειας (Help Desk) έχει ως ακολούθως:

- **Υποστήριξη Γραφείου Άμεσης Βοήθειας πρώτου επιπέδου**
  - Καταγραφή του προβλήματος στο σύστημα υποστήριξης του Γραφείου Άμεσης Βοήθειας (REMEDY).
  - Αναγνώριση προβλήματος και προώθηση στο αρμόδιο προσωπικό του ΕΦΚΑ ή του Αναδόχου ανάλογα με την κατηγορία του προβλήματος.
  - Επίλυση του προβλήματος από το αρμόδιο προσωπικό του Αναδόχου ή του ΕΦΚΑ.
  - Κλείσιμο της αναφοράς του προβλήματος στο σύστημα υποστήριξης του Γραφείου Άμεσης Βοήθειας.
- **Υποστήριξη Γραφείου Άμεσης Βοήθειας δευτέρου επιπέδου**
  - Αναφορά σε διόρθωση στοιχείων των Βάσεων Δεδομένων του ΕΦΚΑ.
  - Αναφορά σε υλικοτεχνική Υποδομή.
  - Αναφορά στο Λογισμικό Εφαρμογών (bugs).
  - Αναφορά για την οποία απαιτείται τροποποίηση ή βελτίωση του λογισμικού εφαρμογών (ενημερώνεται ο Διευθυντής Έργου εκ μέρους του Αναδόχου και η Γενική Διεύθυνση Πληροφορικής & Επικοινωνιών του ΕΦΚΑ, και στην συνέχεια αποφασίζεται από κοινού ο τρόπος αντιμετώπισής του).

Ο εξοπλισμός του Help Desk φαίνεται στον Πίνακα που ακολουθεί:

ΕΞΟΠΛΙΣΜΟΣ HELP - DESK		
ΕΙΔΟΣ	ΛΟΓΙΣΜΙΚΟ	ΠΟΣΟΤΗΤΑ

Κεντρικοί Servers (SUN)	Sun Solaris	1
LAN Servers (HP)	Windows 2000 Server	2
Σταθμοί Εργασίας (HP)	Windows 2000 Professional Greek	20
Εκτυπωτές DOT-MATRIX 80 Στηλών (OKI)		2
Εκτυπωτές LASER (HP)		2
Τηλεφωνικά Κέντρα		1
UPS (Liebert)		1
Switch (Cisco)		2

Πίνακας 6: Εξοπλισμός του Help Desk

6. Ενοποιημένο Περιβάλλον τοπικού δικτύου (domain) της Κεντρικής Υπηρεσίας Κ.Ε.Α.Ο. (Πειραιώς 28)

Στο Ενοποιημένο Περιβάλλον του τοπικού δικτύου της Κεντρικής Υπηρεσίας Κ.Ε.Α.Ο. συνδέονται σταθμοί εργασίας, με σκοπό την κοινή χρήση των μέσων (εκτυπωτών) και την ανταλλαγή πληροφοριών (κοινή χρήση αρχείων και φακέλων μέσω του δικτύου). Ο Server παρέχει τους κοινόχρηστους πόρους στο τοπικό δίκτυο.

Ο εξοπλισμός του ενοποιημένου περιβάλλοντος, φαίνεται στον πίνακα που ακολουθεί:

ΕΞΟΠΛΙΣΜΟΣ ΕΝΟΠΟΙΗΜΕΝΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΤΟΥ ΚΕΑΟ		
ΕΙΔΟΣ	**ΛΟΓΙΣΜΙΚΟ**	**ΠΟΣΟΤΗΤΑ**
LAN Server (Dell)	Windows Server 2008 R2	1
Σταθμοί Εργασίας (HP)	Windows 7 Pro	40
Σταθμοί Εργασίας (Lenovo)	Windows 7 Pro	1
Σταθμοί Εργασίας (QUEST X)	Windows 7 Pro	1
Σταθμοί Εργασίας (LAMTECH)	Windows 7 Pro	1
Εκτυπωτές LASER (lexmark)		6
Τείχος Ασφαλείας Firewall (Fortinet Fortigate)		1
Πολυμηχάνημα (Lexmark)		1
Router (OTE-Speedport Entry 2i)		1
UPS (APC)		1
Συσκευή αντιγράφων ασφαλείας backup (Dell)	SYMC BACKUP EXEC 2014 SERVER	1

Πίνακας 7: Εξοπλισμός του ενοποιημένου περιβάλλοντος τοπικού δικτύου του ΚΕΑΟ

7. Ασφαλής Διάταξη Δημιουργίας Υπογραφής / Κεντρικό ΑΔΔΥ (Πατησίων 12)

Πρόκειται για την ασφαλή διάταξη ARX Cosign Central FIPS v 7.1, η οποία έχει πιστοποιηθεί κατά ETSI TS 14167-5/Common Criteria EAL4+ καθώς και από την ΕΕΤΤ ότι καλύπτει τις απαιτήσεις των ασφαλών διατάξεων δημιουργίας υπογραφής.

Η εν λόγω διάταξη έχει τα εξής ελάχιστα χαρακτηριστικά απόδοσης & ασφάλειας:

- Υποστήριξη μέχρι 270 ψηφιακών υπογραφών/sec με κλειδιά 1024 bit
- Εξυπηρέτηση 10.000 χρηστών / Ασφαλή Διάταξη
- Υποστήριξη κλειδιών μήκους 4096 bit
- Υποστήριξη ψηφιακής υπογραφής εγγράφων χωρίς να απαιτείται χρήση άλλων εφαρμογών
- Υποστήριξη της δυνατότητα απομακρυσμένης διασύνδεσης με την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ-ΕΡΜΗΣ).

Το κεντρικό ΑΔΔΥ παρέχει μία προγραμματιστική διεπαφή CoSign Signature API (SAPI) που παρέχει υπηρεσίες ψηφιακής υπογραφής και λειτουργικότητα διασύνδεσης με εξωτερικά συστήματα και εφαρμογές. Οι προγραμματιστές μπορούν να χρησιμοποιήσουν το SAPI για να ολοκληρώσουν την υποστήριξη ψηφιακών υπογραφών σε προσαρμοσμένες διαδικασίες, εσωτερικά ανεπτυγμένες εφαρμογές, και την ενσωμάτωση του CoSign με τρίτες εφαρμογές, συστήματα και υπηρεσίες καταλόγου. Το SAPI παρέχει την λειτουργικότητά του σε τρεις τύπους διεπαφών προγραμματισμού:

- C/C++ βιβλιοθήκες για εφαρμογές Microsoft Windows
- COM Objects για προγραμματισμό σε περιβάλλον Microsoft
- Web Services

Στο κεντρικό ΑΔΔΥ βρίσκονται αποθηκευμένα αναγνωρισμένα ψηφιακά πιστοποιητικά για τους υπαλλήλους του ΕΦΚΑ, τα οποία έχουν εκδοθεί από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ-ΕΡΜΗΣ). Η διαχείριση χρηστών στο κεντρικό ΑΔΔΥ έχει ολοκληρωθεί με τη διαχείριση χρηστών του ΕΦΚΑ (χρήστες εφαρμογής ΟΠΣ Μισθωτών και χρήστες της εφαρμογής ηλεκτρονικών καταθέσεων εις χείρας πιστωτικών ιδρυμάτων).

Πλατφόρμα αυθεντικοποίησης με κωδικό πρόσβασης μιας χρήσης (OTP)

Πρόκειται για την πλατφόρμα LinOTP v2.8, η οποία επικοινωνεί με το Κεντρικό ΑΔΔΥ μέσω του τυποποιημένου πρωτόκολλου RADIUS, παρέχοντας τη δυνατότητα επέκτασης της πιστοποίησης χρηστών του Cosign με χρήση Two Factor Authentication – One Time Passwords (OTP) - Κωδικός Πρόσβασης Μιας Χρήσης.

Για το CoSign Central-FIPS που είναι μια πλατφόρμα κεντρικού εξυπηρετητή ψηφιακών υπογραφών, ο υψηλού επιπέδου έλεγχος ταυτότητας του υπογράφοντος είναι ένας βασικός παράγοντας για την ασφάλεια του όλου συστήματος. Για το λόγο αυτό ο μηχανισμός ταυτοποίησης βασίζεται σε δυο παράγοντες :

1. ένα κωδικό Πρόσβασης μιας χρήσης που παράγεται από μια συσκευή που έχει στην κατοχή του ο χρήστης, π.χ. μια συσκευή παραγωγής κωδικών (OTP hardware token) ή μια εφαρμογή στο κινητό του τηλέφωνο
2. κάποια πληροφορία που γνωρίζει ο χρήστης όπως π.χ. τα στοιχεία πρόσβασης (credentials) σε ένα πληροφοριακό σύστημα.

Μόνο η επιτυχής επικύρωση των δύο στοιχείων παρέχει επαρκείς εγγυήσεις για την ταυτότητα του τελικού χρήστη.

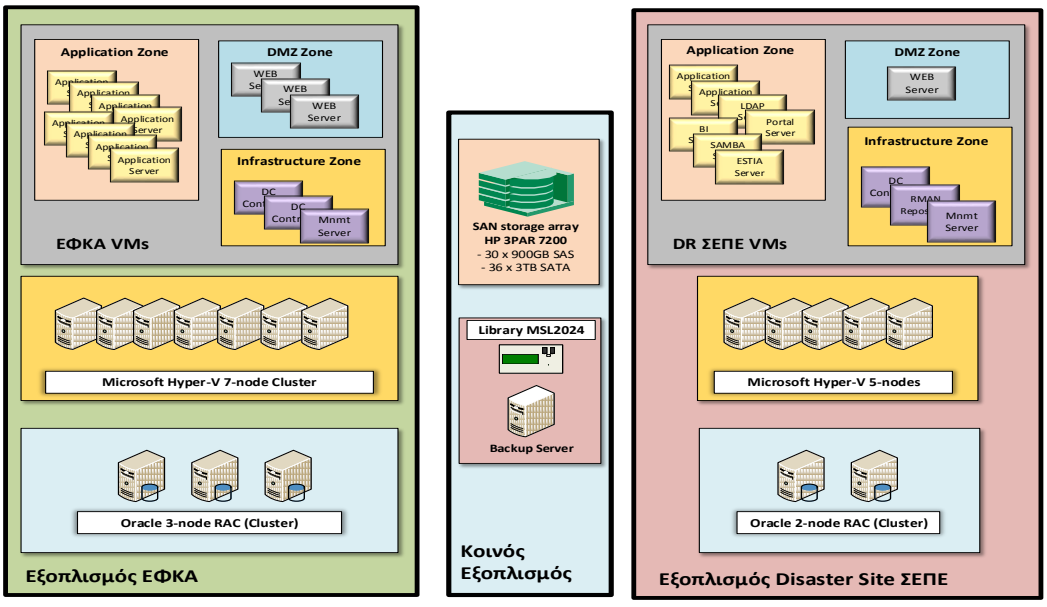
8. Μηχανογραφικός εξοπλισμός προερχόμενος από το ΣΕΠΕ (Παπαδιαμαντοπούλου 87)

Στο κεντρικό Computer Room του ΕΦΚΑ προστέθηκε εξοπλισμός προερχόμενος από τον εξοπλισμό πληροφορικής του Σ.ΕΠ.Ε. Ο εξοπλισμός αυτός έχει διπλό ρόλο:

1. καλύπτει τις ανάγκες του Σ.ΕΠ.Ε έχοντας τον ρόλο του Disaster Site.
2. μέρος του εξοπλισμού, αφού επαυξήθηκε σε πόρους (CPUs, MEMORY, Network Interfaces, κλπ) και μετά από την ανάλογη παραμετροποίηση, η υποδομή καλύπτει τις ανάγκες των ΣΥΝΤΑΞΕΩΝ του ΕΦΚΑ.

Οι υπηρεσίες παρέχονται προς το σύνολο των σημείων εγκατάστασης του ΟΠΣ-ΕΦΚΑ Μισθωτών (Client/Server Interface). Επίσης υπάρχει και διασύνδεση προς το ΣΥΖΕΥΞΙΣ και το INTERNET (Web Interface).

Ακολουθεί η αρχιτεκτονική της υφιστάμενης Υποδομής :



Εικόνα 3: Συστημική Αναπαράσταση εξοπλισμού πληροφορικής προερχόμενος από το Σ.ΕΠ.Ε.

Ο ανωτέρω εξοπλισμός έχει ως ακολούθως:

Υποδομή Βάσης Δεδομένων

Για την υποστήριξη της κεντρικής βάσης δεδομένων έχει υλοποιηθεί ένα Oracle Real Application Cluster (RAC) με τρείς (3) κόμβους με τον παρακάτω εξοπλισμό:

Database Servers (κοινός εξοπλισμός και για τους 3 κόμβους)	
Operating System	Oracle Linux v5 U10
RDBMS Software	Oracle Enterprise 10.2.0.5
Server Model	HP DL385p G8
CPU Info	2 x AMD 6344
RAM	64 GB
Internal Storage	3 x 300GB SAS 15k

Υποδομή Virtualization

Για την υλοποίηση του Virtualization έχει εγκατασταθεί και παραμετροποιηθεί ένα Microsoft Hyper-V Cluster , από επτά (7) κόμβους με τον παρακάτω εξοπλισμό:

Hyper-V Servers x 7	
Operating System	Microsoft 2012 R2 Server
Server Model	HP DL385p G8
CPU Info	1 ή 2 x AMD CPUs
RAM	128 ή 144 GB
Internal Storage	3 x 300GB SAS 15k

Virtual Machines

Για την υποστήριξη των εφαρμογών του Πληροφοριακού Συστήματος του ΕΦΚΑ έχουν εγκατασταθεί και παραμετροποιηθεί οι παρακάτω Ιδεατοί εξυπηρετητές (Virtual Machines):

WEB Servers x 3	
Operating System	Microsoft 2008 R2 Server
Application	Oracle HTTP Server 11g
vCPU Info	2 x vCPUs
RAM	32 GB
Virtual Disk Size	320GB

APPLICATION Servers x 8	
Operating System	Microsoft 2008 R2 Server
Application	Oracle Forms & Reports 11g & Oracle Weblogic 12c
vCPU Info	2 x vCPUs
RAM	32 GB
Virtual Disk Size	320GB

Λοιποί Servers

Για την υποστήριξη της παραπάνω υποδομής έχουν εγκατασταθεί και οι ακόλουθοι Servers, με τους εξής ρόλους:

Λοιποί Servers	
Domain Controller x 2	Microsoft 2012 R2 Server
File Servers x 2	Microsoft 2012 R2 Server
Management Server	Microsoft 2012 R2 Server
AntiVirus Server	Microsoft 2012 R2 Server
Backup Server	Microsoft 2012 R2 Server
Rules Engine Server	Microsoft 2008 R2 Server

9. Επιπρόσθετος Μηχανογραφικός εξοπλισμός πληροφορικής

Στα κεντρικά Computer Rooms του ΕΦΚΑ, Παπαδιαμαντοπούλου 87 & Πατησίων 12, έχει προστεθεί και λειτουργεί εξοπλισμός προερχόμενος από διάφορες προμήθειες, σύμφωνα με τον Πίνακα που ακολουθεί:

ΛΟΙΠΟΣ ΕΞΟΠΛΙΣΜΟΣ – ΔΙΑΦΟΡΕΣ ΠΡΟΜΗΘΕΙΕΣ		
ΕΙΔΟΣ	**ΡΟΛΟΣ**	**ΠΟΣΟΤΗΤΑ**
Server (Dell)	Microsoft HyperV Server	2
Storage DELL PowerVault	Αποθηκευτικό Σύστημα Δεδομένων	1
Server (Dell)	DB & Application Server	1
Firewall Fortinet Fortigate	Τείχος Ασφαλείας Firewall	1
Load Balancers (KEMP)	Load Balancers	2
COSign Appliance	Εξοπλισμός Ψηφιακών Υπογραφών	1

Πίνακας 8: Λοιπός Εξοπλισμός

2.1.3 Λογισμικό Ολοκληρωμένου Πληροφοριακού Συστήματος

1. **Λειτουργικά Συστήματα**
   - **SUN SOLARIS 8**

     Είναι εγκατεστημένο στους κεντρικούς Database Servers του ΟΠΣ- ΕΦΚΑ Μισθωτών, στους δύο (2) Servers της Πλατφόρμας Ανάπτυξης, στον Server του Ενοποιημένου Περιβάλλοντος, στον Server του Περιβάλλοντος Εκπαίδευσης τελικών χρηστών, στον Server περιβάλλοντος συλλειτουργίας Λογισμικού Εφαρμογών Συντάξεων ΟΠΣ- ΕΦΚΑ Μισθωτών με Η.ΔΙ.ΚΑ, καθώς και στον Server του Help Desk.
   - **SUN SOLARIS 9**

     Είναι εγκατεστημένο στους Κεντρικούς Database Servers του ΟΠΣ- ΕΦΚΑ Μισθωτών
   - **Windows 2008 Server R2**

     Είναι εγκατεστημένο σε Servers του Συστήματος Ηλεκτρονικών Υπηρεσιών.
   - **Windows 2012 Server R2**

     Είναι εγκατεστημένο σε Servers του Συστήματος Ηλεκτρονικών Υπηρεσιών.
2. **Σύστημα Διαχείρισης Βάσεων Δεδομένων**
   - **RDBMS Oracle Έκδοση 8.1.7 Enterprise Edition**
   - **RDBMS Oracle Έκδοση 10g Enterprise Edition**
   - **RDBMS Oracle Έκδοση 11g Enterprise Edition**
   - **SQL Svr 2000 Standard Edition**

     Είναι εγκατεστημένο στο Σύστημα Ηλεκτρονικών Υπηρεσιών
3. **Σύστημα Εξυπηρετητή Εφαρμογών Διαδικτύου**
   - **Oracle Internet Application Server**
   - **Oracle Web Logic Suite**
   - **MS Internet Information Services (IIS) for Windows Server**

Ακολουθεί Πίνακας Αδειών Χρήσης Oracle για τα (2) και (3) ανωτέρω:

ΑΔΕΙΕΣ ΧΡΗΣΗΣ ORACLE	
1. Oracle DB	7500 named users + 4 per CPU
2. Oracle Internet Application Server	70 named users
3. Oracle Web Logic Suite	130 per CPU
3. Oracle tunning Pack	72 per CPU
4. Oracle diagnostics Pack	72 per CPU
5. Oracle partitioning	72 per CPU

Πίνακας 9: Αδειών Χρήσης Oracle

4. Εργαλεία Ανάπτυξης
   - Oracle Developer 6i *(άδειες 42 named users)*

     Με το Oracle Developer 6i έχουν αναπτυχτεί οι εφαρμογές του ΟΠΣ- ΕΦΚΑ Μισθωτών
   - Oracle Discoverer/2000 *(άδειες 42 named users)*

     Με το Oracle Discoverer/2000 έχουν αναπτυχτεί οι εφαρμογές του ΟΠΣ- ΕΦΚΑ Μισθωτών
   - Macromedia COLDFUSION Server 4.5 Enterprise for Windows

     Με το Macromedia COLDFUSION έχουν αναπτυχθεί οι εφαρμογές του Συστήματος Ηλεκτρονικών Υπηρεσιών.
   - Oracle Web Logic Suite

     Με το Oracle Web Logic Suite έχουν αναπτυχθεί και εξακολουθούν να αναπτύσσονται οι εφαρμογές του Συστήματος Ηλεκτρονικών Υπηρεσιών που συμπεριλαμβάνει μεταξύ άλλων:
     - τον Oracle WebLogic Server 11g & 12c Enterprise Edition
     - το WebLogic Operations Control
     - το WebLogic RealTime (JRockit Real Time JRRT)
     - το Coherence Enterprise Edition
     - το Oracle Application Server Enterprise Edition με δυνατότητες OC4J, Oracle Portal, WebCache, Oracle Forms/Reports, Oracle Internet Directory, κλπ.
     - το Diagnostics Pack for Oracle Middleware

5. Λογισμικό Ανάλυσης Επικινδυνότητας

Έχει υλοποιηθεί υποδομή Risk Analysis, Business Intelligence και Datawarehouse η οποία αποτελείται από τα ακόλουθα δομικά συστατικά:

- RDBMS Oracle Έκδοση 11g Enterprise Edition
- Oracle Web Logic Suite
- Oracle Business Intelligence Suite
- ESKORT RISK Analysis Engine (υποσύστημα του ESKORT Selection Module)

6. Λογισμικό Αυτοματισμού Γραφείου
   - MS Office

     Είναι εγκατεστημένο στο μεγαλύτερο ποσοστό των θέσεων εργασίας του ΟΠΣ-ΕΦΚΑ Μισθωτών (7890 άδειες χρήσης)

7. Λογισμικό Ανίχνευσης Ιομορφών

- **FSecure Antivirus**

  Είναι εγκατεστημένο σε θέσεις εργασίας (PC).

- **TrustPort Antivirus**

  Είναι εγκατεστημένο σε θέσεις εργασίας (PC).

8. **Λογισμικό Firewall**

   - **VPN-1 Enterprise Center**

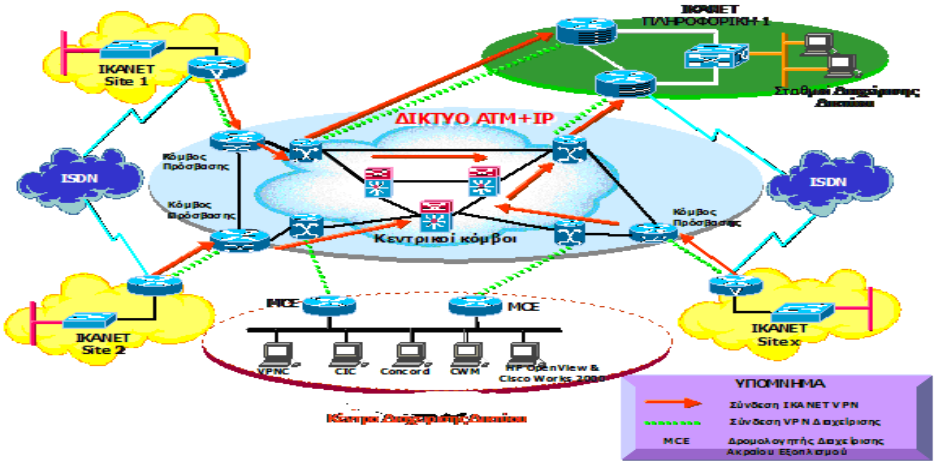
   Είναι εγκατεστημένο στο Σύστημα Ηλεκτρονικών Υπηρεσιών.

2.2 ΔΙΚΤΥΟ ΕΥΡΕΙΑΣ ΠΕΡΙΟΧΗΣ (WAN) ΤΟΥ ΕΦΚΑ ΜΙΣΘΩΤΩΝ - ΙΚΑΝΕΤ

Το Έργο εκτελείται με την μορφή Σύμβασης Παροχής Υπηρεσιών Συμφωνημένου επιπέδου (S.L.A), με αντικείμενο την Υλοποίηση ενός VPN δικτύου πολλαπλών υπηρεσιών (διακίνηση δεδομένων, φωνής και εικόνας) σε 362 Σημεία Εγκατάστασης, την Λειτουργία, Συντήρηση και Διαχείριση αυτού.

Το δίκτυο συνδέει όλες τις Διοικητικές Μονάδες του ΕΦΚΑ Μισθωτών (Περιφερειακές, Τοπικές, Παραρτήματα) με τις Κεντρικές Υπηρεσίες του ΕΦΚΑ. Το δίκτυο είναι τεχνολογίας IP-VPN. Η Αρχιτεκτονική του δικτύου, έχει ως εξής:

- Επίπεδο κορμού (Backbone).
- Επίπεδο Διανομής (Distribution).
- Επίπεδο Πρόσβασης (Access).



Εικόνα 4: Σχηματική απεικόνιση του δικτύου

Αναλυτικά η υλοποίηση του δικτύου πρόσβασης του ΕΦΚΑ έχει επιτευχθεί με τη δημιουργία δικτυακής υποδομής στα Υποκ/τα του ΕΦΚΑ Μισθωτών, μέσω της εγκατάστασης και διαμόρφωσης δρομολογητών και Ethernet switches, με την διασύνδεσή τους στο δίκτυο κορμού του υπάρχοντος αναδόχου μέσω των κυκλωμάτων πρόσβασης και στη συνέχεια με την οργάνωσή τους στο Ιδεατό Ιδιωτικό Δίκτυο ΙΚΑΝΕΤ.

Τα Υποκ/τα του ΕΦΚΑ Μισθωτών συνδέονται φυσικά σε ATM switches που βρίσκονται στα PoPs του δικτύου κορμού του υπάρχοντος παρόχου με κατάλληλες διεπαφές (ATM STM-1, ATM nxE1 IMA και Frame Relay E1/X.21), ανάλογα με το εύρος ζώνης που απαιτείται σε κάθε υποκατάστημα για την ικανοποιητική εξυπηρέτηση των αναγκών του.

Στο δίκτυο πρόσβασης έχει γίνει χρήση των παρακάτω τεχνολογιών κυκλωμάτων πρόσβασης:

- Σταθερή ασύρματη πρόσβαση στα 26Ghz.
- DSL με χρήση της υπηρεσίας ULL
- Ψηφιακού δικτύου HellasCom του ΟΤΕ
- Οπτική ίνα για την διασύνδεση του κεντρικού σημείου της ΠΛΗΡΟΦΟΡΙΚΗΣ
- ISDN δίκτυο του ΟΤΕ έτσι ώστε να εξασφαλίζεται η απρόσκοπτη συνέχιση της μετάδοσης της πληροφορίας μέσω του εν λόγω δικτύου σε περίπτωση που για οποιοδήποτε λόγω η πληροφορία δεν μπορεί να διοδεύσει μέσω του σταθερού κυκλώματος διασύνδεσης.

Η σχεδίαση και υλοποίηση του δικτύου έχει γίνει με τον κανόνα παροχής υπηρεσιών μεταγωγής δεδομένων υψηλού επιπέδου (SLA) έτσι ώστε σε κάθε περίπτωση να εξασφαλίζονται υψηλά ποιοτικά χαρακτηριστικά λειτουργίας (MRTD, Packet Delivery) και η διαθεσιμότητα του δικτύου να είναι τουλάχιστον 99,9% .

2.3 ΔΙΑΔΙΚΤΥΑΚΟΣ ΤΟΠΟΣ ΤΟΥ ΕΦΚΑ ΜΙΣΘΩΤΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

Η αρχική Υποδομή Internet (στο κτίριο επί της οδού Πατησίων 12) δημιουργήθηκε (Υπογραφή Σύμβασης 2001) για την κάλυψη του πρώτου κύματος ηλεκτρονικών υπηρεσιών, που παρείχε το ΙΚΑ προς τους συναλλασσόμενους. Ειδικότερα οι υπηρεσίες αυτές ήταν:

- Παροχή Υπηρεσιών πληροφόρησης
- Ηλεκτρονική υποβολή Α.Π.Δ
- Χορήγηση Ασφαλιστικής Ενημερότητας μέσω Διαδικτύου

Οι Ηλεκτρονικές Υπηρεσίες, οι οποίες εξυπηρετούνται από την Υποδομή Internet είχαν χρησιμοποιήσει το Σύστημα Διαχείρισης Βάσεων Δεδομένων (RDBMS) SQL Server Standard SP1 (version 2000) της εταιρείας Microsoft ενώ το σχετικό Λογισμικό Εφαρμογών έχει αναπτυχθεί με χρήση του περιβάλλοντος Coldfusion version 5 Enterprise της εταιρείας Macromedia.

Οι ηλεκτρονικές υπηρεσίες παρέχονται επί 24ώρου βάσεως προς τους πολίτες μέσω διαδικτύου και ειδικότερα στους Ασφαλισμένους, Εργοδότες, Συνταξιούχους και λοιπούς πιστοποιημένους φορείς, οι οποίοι συναλλάσσονται με το Φορέα. Επισημαίνεται ότι οι νέες Ηλεκτρονικές Υπηρεσίες, οι οποίες είτε έχουν υλοποιηθεί και είναι σε περιβάλλον παραγωγικής λειτουργίας είτε υλοποιούνται, εξακολουθούν να εξυπηρετούνται από την υπάρχουσα Υποδομή Internet. Χρησιμοποιούν το Σύστημα Διαχείρισης Βάσεων Δεδομένων (R.D.B.M.S) Oracle, έκδοση 11g, ενώ το σχετικό Λογισμικό Εφαρμογών έχει αναπτυχθεί με χρήση του Περιβάλλοντος Oracle Web Logic Suite.

Στον πίνακα που ακολουθεί παρουσιάζονται οι λειτουργίες των επιχειρησιακών περιοχών που υποστηρίζονται από τις Ηλεκτρονικές Υπηρεσίες:

WEB APPLICATIONS
ΥΠΟΒΟΛΗ ΑΙΤΗΣΗΣ ΣΥΝΤΑΞΙΟΔΟΤΗΣΗΣ
Αίτηση Σύνταξη Γήρατος
Αίτηση Σύνταξη Αναπηρίας
Αίτηση Σύνταξη Γήρατος, Αναπηρίας Επικουρικού
Στοιχεία Επικοινωνίας
ΑΣΦΑΛΙΣΤΙΚΗ ΕΝΗΜΕΡΟΤΗΤΑ
Πιστοποίηση Φορέων (Νομικά – Φυσικά Πρόσωπα)
Αίτηση Ασφαλιστικής Ενημερότητας (Πιστοποιημένος Εργοδότης)
Αίτηση Βεβαίωσης Ιδιωτικού Οικοδομοτεχνικού Έργου (Πιστοποιημένος Εργοδότης)
Αίτηση Βεβαίωσης Δημοσίου Έργου (Πιστοποιημένος Εργοδότης)
Αίτηση Ασφαλιστικής Ενημερότητας (Πιστοποιημένος Φορέας)
Αίτηση Βεβαίωσης Ιδιωτικού Οικοδομοτεχνικού Έργου (Πιστοποιημένος Φορέας)
Αίτηση Βεβαίωσης Δημοσίου Έργου (Πιστοποιημένος Φορέας)
Επιβεβαίωση Εγκυρότητας Ασφαλιστικής Ενημερότητας
ΑΠΔ
Πιστοποίηση για υποβολή ΑΠΔ κοινών επιχειρήσεων
Πιστοποίηση για υποβολή ΑΠΔ οικοδομοτεχνικών έργων
On-Line έλεγχος υποβολής ΑΠΔ
Μαζική Ταυτοποίηση Ασφαλισμένων
Υποβολή ΑΠΔ Κοινών Επιχειρήσεων ΚΑΝΟΝΙΚΗ
Υποβολή ΑΠΔ Κοινών Επιχειρήσεων ΚΑΝΟΝΙΚΗ μέσω αρχείου
Υποβολή ΑΠΔ Κοινών Επιχειρήσεων ΣΥΜΠΛΗΡΩΜΑΤΙΚΗ

Υποβολή ΑΠΔ Κοινών Επιχειρήσεων ΣΥΜΠΛΗΡΩΜΑΤΙΚΗ μέσω αρχείου
Υποβολή ΑΠΔ Κοινών Επιχειρήσεων ΔΙΟΡΘΩΣΗ ΑΠΔ
Υποβολή ΑΠΔ Κοινών Επιχειρήσεων ΕΠΑΝΥΠΟΒΟΛΗ μέσω αρχείου
Υποβολή ΑΠΔ Οικοδομοτεχνικών έργων ΚΑΝΟΝΙΚΗ
Υποβολή ΑΠΔ Οικοδομοτεχνικών έργων ΚΑΝΟΝΙΚΗ μέσω αρχείου
Υποβολή ΑΠΔ Οικοδομοτεχνικών έργων ΣΥΜΠΛΗΡΩΜΑΤΙΚΗ
Υποβολή ΑΠΔ Οικοδομοτεχνικών έργων ΣΥΜΠΛΗΡΩΜΑΤΙΚΗ μέσω αρχείου
Υποβολή ΑΠΔ Οικοδομοτεχνικών έργων ΕΠΑΝΥΠΟΒΟΛΗ μέσω αρχείου
Πιστοποίηση Ασφαλισμένου
Ατομικός Λογαριασμός Ασφάλισης
ΚΕΑΟ
Πίνακας χρεών οφειλέτη
Ηλεκτρονική Καρτέλα Οφειλέτη
Πληρωμές Οφειλέτη
Ταυτότητα οφειλέτη
Υπολογισμός ρύθμισης
Δημιουργία νέας ρύθμισης
Ασφαλιστική ενημερότητα Οφειλέτη – Υπευθύνων Οφειλέτη
Ηλεκτρονική ενημέρωση Οφειλέτη
Υπηρεσία Υποβολής Αρχείου Οφειλών και Παραλαβής Αρχείου Πιστώσεων
Ηλεκτρονικές Κατασχέσεις εις χείρας Πιστωτικών Ιδρυμάτων
ΛΟΙΠΕΣ ΥΠΗΡΕΣΙΕΣ
Αναζήτηση Αριθμού Μητρώου Ασφαλισμένου (ΑΜΑ) για τους ασφαλισμένους του τ. Ο.Π.Α.Δ.-Τ.Υ.Δ.Κ.Υ.
Απογραφή & Απόδοση Ασφαλιστικής Ικανότητας Εμμέσων Ασφαλισμένων
Εξέλιξη Αιτήματος Απογραφής και Απόδοσης Ασφαλιστικής Ικανότητας
Ατομικός Λογαριασμός Ασφάλισης Απασχολουμένων Εργοδότη
Ατομικός Λογαριασμός Ασφάλισης
Διαχείριση Ευρημάτων Επιτόπιων Ελέγχων Σ.ΕΠ.Ε.
Πληροφόρηση Συνταξιούχων για ΑΜΚΑ-ΑΦΜ
Πληροφόρηση Συνταξιούχων Εξωτερικού
Πιστοποίηση Οφειλετών ΚΕΑΟ άλλων Φορέων
Υπηρεσία Πιστοποίησης Ασφαλιστικών Οργανισμών
Πιστοποίηση Ασφαλισμένου

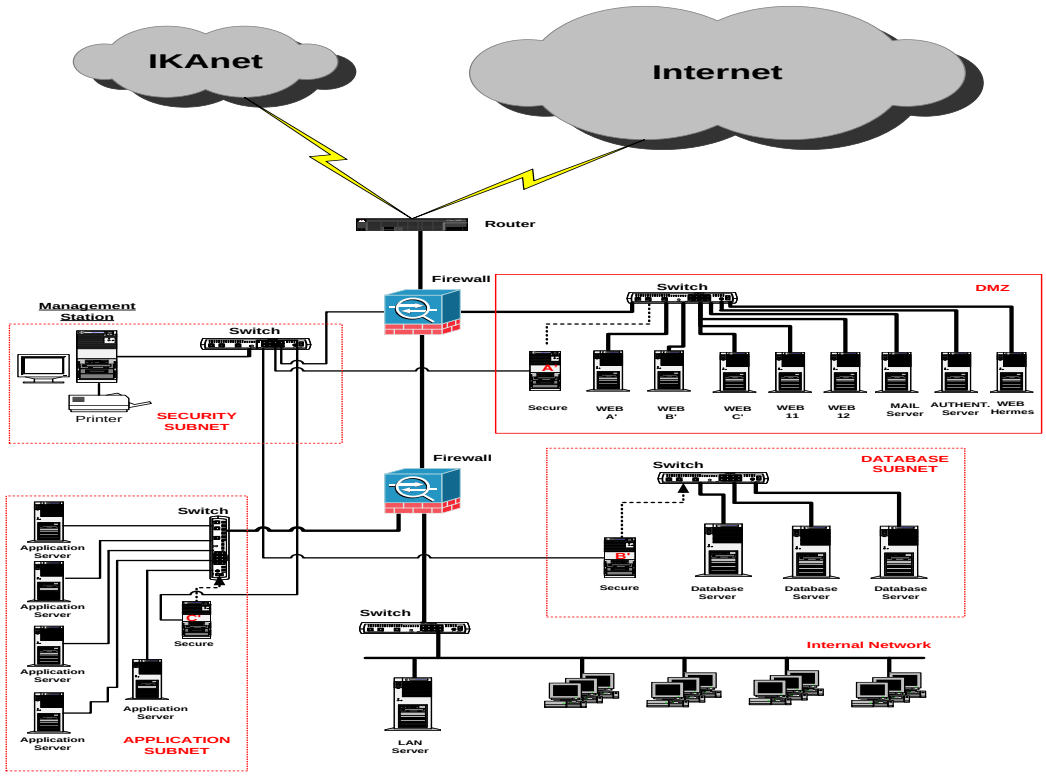
Γνωστοποίηση Αποτελέσματος Πιστοποίησης Αναπηρίας (ΚΕΠΑ)
Καρτέλα Κινήσεων Εργοδότη
Συγκέντρωση Στοιχείων Διεύθυνσης Ασφαλισμένου
Παρακολούθηση της Πορείας Αίτησης Συνταξιοδότησης ή Προσδιορισμού Χρόνου Ασφάλισης
Ενημερωτικό Σημείωμα Συντάξεων
Ενημερωτικό Σημείωμα Συντάξεων ΚΕΠ
Βεβαίωση Συντάξεων (Για Φορολογική Χρήση)
Βεβαίωση Συντάξεων (Για Φορολογική Χρήση) μεσω ΚΕΠ
Συμμετοχή σε Υγειονομικές Επιτροπές
ΚΑΤ' ΟΙΚΟΝ ΦΡΟΝΤΙΔΑ ΣΥΝΤΑΞΙΟΥΧΩΝ
Αίτηση Συμμετοχής Υποψηφίου Παρόχου
Πιστοποίηση Παρόχων
Διαχείριση Σύμβασης Ωφελούμενου
Διαχείριση Σύμβασης Απασχολούμενου
Ανανέωση Σύμβασης
Καταγγελία Σύμβασης
Υποβολή Μηνιαίας Δήλωσης Παροχής Υπηρεσιών

WEB SERVICES
Αίτηση Βεβαίωσης Ασφαλιστικής Ενημερότητας
Αίτηση Βεβαίωσης Οικοδομοτεχνικού Έργου.
Λήψη Αποτελέσματος Αιτήματος Βεβαίωσης Ασφαλιστικής Ενημερότητας.
Λήψη Αποτελέσματος Αιτήματος Βεβαίωσης Οικοδομοτεχνικού Έργου.
Επιβεβαίωση Εγκυρότητας Βεβαίωσης Ασφαλιστικής Ενημερότητας.
Web Service για την παροχή στοιχείων του εργοδότη.(ΣΕΠΕ)
Web Service για την παροχή authentication. (ΣΕΠΕ)
Web Service για τα στοιχεία των παραρτημάτων ενός εργοδότη. (ΣΕΠΕ)
Web Service για τα στοιχεία των υπευθύνων ενός εργοδότη. (ΣΕΠΕ)
Web Service για τα στοιχεία των παραμετρικών πινάκων της διασύνδεσης. (ΣΕΠΕ).
Web Service Ατομικού Λογαριασμού Ασφάλισης.
Web Service Client για εύρεση ΑΜΚΑ από ΗΔΙΚΑ.
Web Service Client για εύρεση ΑΦΜ από ΓΓΠΣ.
Web Service για Πιστοποίηση μέσω ΓΓΠΣ
Web Service Client για στοιχείων ταυτότητας από ΕΛΑΣ

Web Service Client για άντληση στοιχείων Υπηκόων Τρίτων Χωρών από ΥΠΕΣ
Web Service “Εν δυνάμει” Ασφαλιστικής Ικανότητας Υπηκόων Τρίτων χωρών σε ΥΠΕΣ
Ηλεκτρονική Καρτέλα Οφειλέτη (Κινήσεις Οφειλέτη-Transactions)
Ασφαλιστική ενημερότητα Οφειλέτη – Υπευθύνων Οφειλέτη (Status)
Αναγγελία εισπράξεων καθυστερούμενων οφειλών (Changes)
Υποβολή οφειλών σε ΚΕΑΟ(Submissions)
Εξωδικαστικός Συμβιβασμός – Ποσά οφειλών συγκεκριμένου ΑΦΜ
Εξωδικαστικός Συμβιβασμός – Αναλυτικές Οφειλές συγκεκριμένου ΑΦΜ
Εξωδικαστικός Συμβιβασμός – Απάντηση για ΑΦΜ με οφειλή
Εξωδικαστικός Συμβιβασμός – Εικόνα ρύθμισης συγκεκριμένου ΑΦΜ

Εξοπλισμός Υποδομής Παροχής Ηλεκτρονικών Υπηρεσιών μέσω Διαδικτύου

Ακολουθεί η **αρχιτεκτονική** της υφιστάμενης Υποδομής :



Ο **Εξοπλισμός της ανωτέρω Υποδομής,** έχει ως ο **ΠΙΝΑΚΑΣ** που ακολουθεί και είναι εγκατεστημένος στο κτίριο της οδού Πατησίων 12 :

ΕΞΟΠΛΙΣΜΟΣ ΥΠΟΔΟΜΗΣ INTERNET		
ΕΙΔΟΣ	**ΛΟΓΙΣΜΙΚΟ**	**ΠΟΣΟΤΗΤΑ**
LAN Servers (HP)	Windows 2000 Server	13
LAN Servers (DELL)	Windows 2008 Server R2	11
Σταθμοί Εργασίας (HP)	Windows 2000 Professional Greek	5
Εκτυπωτές LASER		3
Τηλεφωνικά Κέντρα		1
UPS (Liebert)		2
Firewall(Cisco) ASA 5550		2
Router (Cisco)		2
Switch (Cisco) Catalyst 6500		2
Switch (Cisco) Catalyst 2900 XL		4

Πίνακας 10: Εξοπλισμός υποδομής Internet

2.4 ΑΣΦΑΛΕΙΑ ΥΠΟΔΟΜΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΣΧΕΔΙΟ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΗ

Το Έργο έχει ολοκληρωθεί (ΦΠΥ5/09/04-01-2011 Σύμβαση) και έχει παραληφθεί στις 08/11/2011

ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ

Η εκπόνηση "Μελέτης Ασφάλειας Υποδομών Πληροφορικής και Επικοινωνιών και Σχέδιο Ανάκαμψης από Καταστροφή", αφορούσε κατ' ελάχιστο τα ακόλουθα:

Καταγραφή της υπάρχουσας κατάστασης. [Πληροφοριακών Συστημάτων, Υποδομών και Δεδομένων (προσδιορισμός της κρισιμότητας αυτών)]

Ανάλυση και Διαχείριση Επικινδυνότητας (Αποτίμηση Επικινδυνότητας στις ακόλουθες περιοχές: Υπολογιστικά Συστήματα, Δικτυακές υποδομές,, λογισμικό εφαρμογών και πληροφορίες που διαχειρίζονται τα υπολογιστικά συστήματα)

Ανάλυση Επίδρασης των απειλών ασφάλειας στην Επιχειρησιακή Λειτουργία του πρώην ΙΚΑ (Ειδική Μελέτη), η οποία υποστηρίζεται από την υπολογιστική και δικτυακή υποδομή.

Αποτίμηση Ευπαθειών [Μελέτη Αποτίμησης Ευπαθειών των Υπολογιστικών κόμβων του δικτυακού εξοπλισμού και Υποδομών του ΙΚΑ (αποτελεί μέρος της Ανάλυσης της Επικινδυνότητας)]

Πολιτική Ασφάλειας

Εκπόνηση Πολιτικής Ασφάλειας: Η Πολιτική Ασφάλειας, περιγράφει ένα **σύνολο κανόνων και διαδικασιών** που καθορίζουν τον τρόπο με τον οποίο πρέπει να διαχειρίζονται και προστατεύονται οι πληροφορίες, έτσι ώστε να επιτυγχάνονται συγκεκριμένοι στόχοι ασφάλειας. Οι κανόνες αυτοί προσδιορίζουν τον ρόλο κάθε εμπλεκομένου, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του. Τα συγκεκριμένα μέτρα τα οποία περιλαμβάνει μία πολιτική ασφάλειας είναι άμεσα σχετιζόμενα με τα αποτελέσματα της "Ανάλυσης Επικινδυνότητας". **"Το τεύχος Πολιτικής Ασφάλειας",** απευθύνεται σε Στρατηγικό Επίπεδο και χαράσσει τις κατευθυντήριες γραμμές, οι οποίες θα πρέπει να ακολουθούνται. Εμπεριέχει τα πρότυπα πολιτικής ασφάλειας, τις διαδικασίες ασφάλειας, τεχνικές οδηγίες και το πλάνο συμμόρφωσης.

Υλοποίηση Πολιτικής Ασφάλειας: Μετά τον σχεδιασμό του μοντέλου ενός αποδεκτού επιπέδου ασφάλειας, θα πρέπει να υλοποιηθεί και τεθεί σε λειτουργία το **Οργανωτικό και Λειτουργικό πλαίσιο,** το οποίο θα είναι σε θέση – εφόσον εφαρμόζεται – να διατηρείται στο επιθυμητό επίπεδο ασφάλειας.

Επιχειρησιακό Σχέδιο Ασφάλειας

Το Επιχειρησιακό Σχέδιο Ασφάλειας καθορίζει τις λειτουργικές, τεχνικές, οικονομικές και χρονικές παραμέτρους υλοποίησης των μέτρων ασφάλειας. Καλύπτει κατ' ελάχιστον τα ακόλουθα:

- Τεχνική και Λειτουργική Περιγραφή της υλοποίησης κάθε μέτρου ασφάλειας
- Οικονομική Αποτίμηση της Υλοποίησης κάθε μέτρου ασφάλειας
- Χρονοδιάγραμμα Υλοποίησης - Παραδοτέα

Σχέδιο Ανάκαμψης από καταστροφή (Disaster Recovery Plan). Το Disaster Recovery Plan καθορίζει τις τεχνικές, οικονομικές και χρονικές παραμέτρους υλοποίησης και λειτουργίας του Disaster Recovery Site.

ΠΑΡΑΔΟΤΕΑ / ΧΑΡΑΚΤΗΡΙΣΜΟΣ

Τα **Παραδοτέα του έργου,** είναι τα ακόλουθα:

1. **Τεύχος αποτύπωσης υπάρχουσας κατάστασης (Εμπιστευτικό έγγραφο)**
2. **Διαγράμματα ροής κρίσιμης πληροφορίας (Εμπιστευτικό έγγραφο)**

3. **Τεύχος Ανάλυσης Επικινδυνότητας** (Risk Analysis) **(Εμπιστευτικό έγγραφο)**
4. **Τεύχος Ανάλυσης Επίδρασης** (Business Impact Analysis) **(Εμπιστευτικό έγγραφο)**
5. **Τεύχος Αποτίμησης Ευπαθειών** (Vulnerability assessment) **(Άκρως Εμπιστευτικό έγγραφο)**
6. **Τεύχος Ανάπτυξης Πολιτικής Ασφάλειας** (Τεύχος Πολιτικής Ασφάλειας, Πρότυπα Πολιτικής Ασφάλειας, Διαδικασίες Ασφάλειας, Τεχνικές οδηγίες, Πλάνο Συμμόρφωσης κ.λ.π) **(Εμπιστευτικό έγγραφο)**
7. **Επιχειρησιακό Σχέδιο Ασφάλειας** (Περιγραφή προτεινόμενης Αρχιτεκτονικής Ασφάλειας, Λειτουργικές και Τεχνικές προδιαγραφές κάθε μέτρου ασφάλειας, κόστος υλοποίησης κάθε αντιμέτρου, χρονοδιάγραμμα υλοποίησης κ.λ.π) **(Εμπιστευτικό έγγραφο)**
8. **Σχέδιο Ανάκαμψης από καταστροφή** (Disaster Recovery Plan συμπεριλαμβανομένου του Disaster Recovery Site) **(Εμπιστευτικό έγγραφο)**
9. **Σχέδιο Τευχών Δημοπράτησης Δημόσιου Ανοικτού Διαγωνισμού,** με αντικείμενο, την παροχή υπηρεσιών και προϊόντων Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων (ΙΚΑSEC), εμπεριεχομένου και του Disaster Recovery Site, καθώς και Παροχή Υπηρεσιών Υποστήριξης Παραγωγικής Λειτουργίας χρονικής διάρκειας τριών (3) ετών.
10. **Μηνιαίες Αναφορές Προόδου**
11. **Πλάνο Εκπαίδευσης / Ενημέρωσης Στελεχών**
12. **Υπηρεσίες Εκπαίδευσης / Ενημέρωσης Στελεχών**
13. **Αναφορά Αποτελεσμάτων Εκπαίδευσης**
14. **Τελική Έκθεση Έργου**

<u>ΥΙΟΘΕΤΗΣΗ ΤΩΝ ΠΡΟΤΑΣΕΩΝ ΤΗΣ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ</u>

Αναφέρεται σε **δραστηριότητες οι οποίες είναι διαρκώς ενεργές** διότι πρέπει να παρακολουθούνται οι αλλαγές στο Οργανωτικό Επιχειρησιακό και Τεχνολογικό Περιβάλλον του ΕΦΚΑ. **Απαιτείται ετησίως Συντήρηση και Επικαιροποίηση αυτών.**

Επισημαίνεται ότι η ανωτέρω μελέτη, ολοκληρώθηκε το 2011 και αφορούσε **αποκλειστικά** το ΠΣ του πρώην ΙΚΑ-ΕΤΑΜ. Η επικαιροποίηση και συντήρηση αυτής, έπαυσε το 2016, με την ενσωμάτωση του ΙΚΑ-ΕΤΑΜ, στον ΕΦΚΑ. Στην παρούσα φάση ο ΕΦΚΑ είναι σε διαδικασία ενσωμάτωσης στη πολιτική ασφάλειας των αλλαγών που έχει επιφέρει η ίδρυσή του στο Οργανωτικό, Επιχειρησιακό και Τεχνολογικό Περιβάλλον. **Σημειώνεται ότι η εν λόγω δράση ενδέχεται να μην έχει ολοκληρωθεί μέχρι την υπογραφή της παρούσας σύμβασης**.

Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης (ΕΣΔΔΑ)
Πειραιώς 211, ΤΚ 177 78, Ταύρος
τηλ: 2131306349 , fax: 2131306479
www.ekdd.gr