



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ
ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΠΡΟΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ
ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ



Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και Ασφάλειας Δεδομένων στην Ελλάδα

Στέφανος Χάμπας
13198, icsd13198@icsd.aegean.gr

Επιβλέπων: Χαραλαμπίδης Ιωάννης

ΣΕΠΤΕΜΒΡΙΟΣ 2021

Η Διπλωματική Εργασία παρουσιάστηκε ενώπιον
του Διδακτικού Προσωπικού του Πανεπιστημίου Αιγαίου
Σε Μερική Εκπλήρωση των απαιτήσεων για την απόκτηση του διπλώματος του
Μηχανικού Πληροφοριακών και Επικοινωνιακών Συστημάτων

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ
ΕΠΙΚΥΡΩΝΕΙ ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΟΥ
ΣΤΕΦΑΝΟΥ ΧΑΜΠΑ

Επιβλέπων: Χαραλαμπίδης Ιωάννης
Καθηγητής

Τμήμα Μηχανικών Πληροφοριακών
και Επικοινωνιακών Συστημάτων

Λουκής Ευριπίδης
Καθηγητής

Τμήμα Μηχανικών Πληροφοριακών
και Επικοινωνιακών Συστημάτων

Παπαδοπούλου Παναγιώτα
Επίκουρη Καθηγήτρια

Τμήμα Μηχανικών Πληροφοριακών
και Επικοινωνιακών Συστημάτων

© 2021

Με επιφύλαξη παντός δικαιώματος.

Στέφανος Χάμπας

Πανεπιστήμιο Αιγαίου

Πρόλογος

Με την ολοκλήρωση της διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλλαν στην εκπόνησή της.

Ευχαριστώ θερμά τον επιβλέπων καθηγητή μου, κύριο Ιωάννη Χαραλαμπίδη, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, τις υποδείξεις του, την επιμονή του, το αμείωτο ενδιαφέρον του, και τη συνεχή του υποστήριξη από την αρχή μέχρι το τέλος.

Επίσης, ευχαριστώ τον κύριο Δαβαλά Αθανάσιο, D.P.O του Δήμου Ζωγράφου, για τις απαντήσεις που μου έδωσε στο εργαλείο αξιολόγησης και με βοήθησαν στην υλοποίηση της διπλωματικής μου εργασίας.

Τέλος, θα ήθελα εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου για τη στήριξη, τη συμπαράσταση και την κατανόησή τους, καθ' όλη τη διάρκεια των σπουδών μου.

Περίληψη

Σε μια εποχή που η τεχνολογία και ο τομέας της πληροφορικής αναπτύσσεται ταχύτατα η Ηλεκτρονική Διακυβέρνηση του Ελληνικού κράτους πρέπει να ακολουθήσει την συγκεκριμένη ανάπτυξη. Η Ηλεκτρονική Διακυβέρνηση αφορά στον εκσυγχρονισμό του Κράτους και της Δημόσιας Διοίκησης, βασιζόμενο στις Τεχνολογίες Πληροφοριών και Επικοινωνιών. Οι υπηρεσίες που προσφέρονται απαιτούν την διαλειτουργικότητα μεταξύ των πληροφοριακών συστημάτων του δημόσιου τομέα, με σκοπό την αυτοματοποιημένη ανταλλαγή δεδομένων και πληροφοριών.

Προκειμένου να αξιοποιηθούν οι υπηρεσίες ηλεκτρονικής διακυβέρνησης, απαιτείται η συλλογή και επεξεργασία πολλών ειδών πληροφοριών, όπως τα προσωπικά δεδομένα, των οποίων η προστασία και η επεξεργασία τους είναι υποχρεωτικό να γίνονται με βάση τις νομοθεσίες που τα προστατεύουν.

Στην παρούσα εργασία αρχικά γίνεται αναφορά στον Νόμο « 4727/2020 Ψηφιακή Διακυβέρνηση» ο οποίος ρυθμίζει όλα τα θέματα της ψηφιακής διακυβέρνησης και των Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ) από τους φορείς του δημόσιου τομέα για τις ανάγκες της λειτουργίας τους, καθώς και την υποστήριξη της άσκησης των αρμοδιοτήτων και των συναλλαγών τους με φυσικά ή νομικά πρόσωπα ή νομικές οντότητες.

Στην συνέχεια αναλύεται ο Νόμος «4624/2019 : Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», ο οποίος αναφέρει ρητά όλα τα μέτρα που απαιτούνται, με στόχο τη διαφύλαξη της ασφάλειας των προσωπικών δεδομένων πολιτών, αναγνωρίζοντας σε αυτούς νέα δικαιώματα και αυξάνοντας την προστασία τους.

Τέλος προτείνεται και περιγράφεται το εργαλείο « Εργαλείο Αξιολόγησης Συμμόρφωσης με τις νομοθεσίες της Ηλεκτρονικής Διακυβέρνησης και την Ασφάλεια Προσωπικών Δεδομένων». Το συγκεκριμένο εργαλείο έχει ως στόχο να αξιολογεί κάθε δημόσιο φορέα, δίνοντας του ως αποτέλεσμα τον βαθμό συμμόρφωσης και το ποσοστό που υπολείπεται ως προς την πλήρη συμμόρφωση του με τους κανονισμούς.

Λέξεις - Κλειδιά: Ηλεκτρονική Διακυβέρνηση, Δεδομένα προσωπικού χαρακτήρα, Αξιολόγηση νομοθεσιών, ΤΠΕ, Δημόσια Διοίκηση, Νόμος 4727/2020, Νόμος 4624/2019

Abstract

Analysis of Digital Governance and Cyber Security Legal Framework in Greece

At a time when technology and the IT sector are rapidly developing, the e-Government of the Greek state must quickly follow this development. E-Government concerns the modernization of the State and Public Administration, based on Information and Communication Technologies. The services offered require the interoperability between the Information systems of the public sector, for the purpose of automated data exchange and information.

In order to utilize the e-government services, the collection and processing of many types of information is required, such as personal data, the protection and processing of which is mandatory to be made under the laws that protect them.

In the present work, reference is initially made to the Law “4727/2020 Digital Governance” which regulates all issues of digital governance and of Information and Communication Technologies (ICT) by its bodies of public sector for the needs of their operation, as well as support the exercise of their responsibilities and their transactions with natural or legal persons or legal entities.

Following, the Law “4624/2019: Data Protection Authority of private nature” is analyzed which explicitly states all the measures required, with a view to safeguarding the security of citizens’ personal data, recognizing to them new rights and increasing their protection.

Finally, the tool “Evaluation of Compliance Tool with the laws of e-Government and Personal Data Security” is proposed and described. This tool aims to evaluate each public body, giving it the grade of compliance and the percentage remaining in terms of full compliance with the regulations.

Keywords: *E-Government, State and Public Administration, Data Protection, Evaluation of Compliance Tool, Law “4727/2020”, Law “4624/2019”*

Ενδεικτικός Πίνακας Περιεχομένων

1.	Εισαγωγή	8
1.1	Σκοπός Διπλωματικής Εργασίας	9
1.2	Δομή Διπλωματικής Εργασίας	9
2.	Το πλαίσιο της Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα	10
2.1	Ορισμός Ηλεκτρονικής Διακυβέρνησης	10
2.2	Τύποι Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης	10
2.3	Οφέλη της ηλεκτρονικής διακυβέρνησης	11
2.4	Ανασταλτικοί παράγοντες για την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης	12
2.5	Συμμετοχή πολιτών και Διαλειτουργικότητα συστημάτων	13
2.6	Πολιτικές ψηφιακής διακυβέρνησης και αρχές	15
2.7	Νόμος Ψηφιακής Διακυβέρνησης	15
2.8	Ιστορική Αναδρομή Νομοθεσιών Ηλεκτρονικής Διακυβέρνησης	16
2.9	Ιστορική Αναδρομή Νομοθεσιών για τα προσωπικά δεδομένα και τις ηλεκτρονικές επικοινωνίες	17
3.	Νόμος 4727/2020 Ψηφιακή Διακυβέρνηση	19
3.1	Εισαγωγή	19
3.2	Νομοθεσία	20
3.2.1	Προσωπικός Αριθμός και Γενικές διατάξεις για τα ηλεκτρονικά έγγραφα	20
3.2.2	Ενδοδιοικητική οργάνωση ψηφιακής διακυβέρνησης	20
3.2.3	Παροχή ψηφιακών δημόσιων υπηρεσιών - Ενιαία ψηφιακή πύλη της δημόσιας διοίκησης	21
3.2.4	Ψηφιακή προσβασιμότητα	23
3.2.5	Πιστοποιητικά υπηρεσιών εμπιστοσύνης	23
3.2.6	Ανοικτά δεδομένα και περαιτέρω χρήση πληροφοριών του δημόσιου τομέα	24
3.2.7	Ψηφιακή διαφάνεια - Πρόγραμμα Διαύγεια	25
3.2.8	Υποδομές	27
3.2.9	Μητρώα ψηφιακής διακυβέρνησης	29
3.2.10	Έκτακτα μέτρα λόγω της πανδημίας COVID-19	29
3.2.11	Ηλεκτρονικές Επικοινωνίες	29
4.	Γενικός Κανονισμός για την Προστασία Δεδομένων	31
4.1	Εισαγωγή	31
4.2	Γενικές Διατάξεις	31
4.3	Υπεύθυνος Προστασίας Δεδομένων (DPO) και διαδικασίες επεξεργασίας δεδομένων	31
4.4	Δικαιώματα του υποκειμένου των δεδομένων	33

4.5	Υποχρεώσεις εκτελούντος την επεξεργασία και υπεύθυνου επεξεργασίας.....	34
4.5.1	Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην Αρχή...	34
4.5.2	Προστασία δεδομένων από τον σχεδιασμό και εξ' ορισμού	35
4.6	Εκτίμηση Αντικτύπου- Data Protection Impact Assesment (ΕΑΠΔ - DPIA).....	36
5.	Εργαλείο Αξιολόγησης	37
5.1	Δημιουργία Ερωτήσεων Εργαλείου	37
5.2	Οδηγίες Συμπλήρωσης Εργαλείου Αξιολόγησης	40
6.	Εφαρμογή – Αξιολόγηση Δημόσιου Φορέα.....	45
6.1	Αποτελέσματα Αξιολόγησης	45
6.2	Συμπεράσματα από την αξιολόγηση του Φορέα.....	48
7.	Συμπεράσματα	49
7.1	Συμπεράσματα επί των αποτελεσμάτων	49
7.2	Συμπεράσματα επί των εργαλείων	49
7.3	Επόμενα βήματα-Μελλοντικοί στόχοι	50
8.	Λεξικό όρων.....	51
8.1	Λεξικό όρων Νόμου 4727/2020	51
8.2	Λεξικό όρων Νόμου 4624/2019	52
9.	Αναφορές	53

1. Εισαγωγή

Στη σύγχρονη κοινωνία οι τεράστιες αλλαγές που επιτελούνται στον τομέα της τεχνολογίας των τηλεπικοινωνιών και των δικτύων με κυριότερη από αυτές την ανάπτυξη του διαδικτύου, όπως είναι φυσικό επηρεάζουν καθοριστικά τις σχέσεις που αναπτύσσουν οι πολίτες με τις δημόσιες υπηρεσίες και το κράτος. Η δημόσια διοίκηση προκειμένου να προσαρμοστεί σ' αυτά τα νέα δεδομένα έχει προβεί στη χρησιμοποίηση των Τεχνολογιών των Πληροφοριών και Επικοινωνιών (ΤΠΕ) στο πλαίσιο τόσο των λειτουργιών της, όσο και της βελτίωσης της επικοινωνίας και των συναλλαγών με τους πολίτες και τις επιχειρήσεις. Οι τεχνολογίες αυτές αποτελούν το σημαντικότερο εργαλείο της δημόσιας διοίκησης για να εφαρμόσει σύγχρονα μοντέλα διοίκησης.

Συνοπτικά ως στόχοι τίθενται ο ριζικός μετασχηματισμός των διαδικασιών μέσω της αναβάθμισης των υπηρεσιών που θα εξασφαλίζουν την ικανοποίηση των αναγκών για τους πολίτες αλλά και την ενεργή συμμετοχή τους σε αυτήν. Εφόσον διαχειριστούν με σωστό τρόπο οι τεχνολογίες και το διαδίκτυο θα επιτευχθεί η αυτοματοποίηση των υπηρεσιών των δημοσίων φορέων. Έτσι ο πολίτης θα έχει τη δυνατότητα διεκπεραίωσης υποχρεώσεων και συναλλαγών ανά πάσα στιγμή χωρίς χρονοτριβές και γραφειοκρατία. Μέσω της αύξησης της διαφάνειας αλλά και της μείωσης της διαφθοράς θα δημιουργηθεί ένα ασφαλές περιβάλλον μέσω του οποίου θα είναι δυνατή κάθε συναλλαγή τόσο των πολιτών και των επιχειρήσεων όσο και των δημοσίων φορέων και του κράτους.

Η αξιοποίηση των υπηρεσιών ηλεκτρονικής διακυβέρνησης απαιτεί την συλλογή, αποθήκευση αλλά και την επεξεργασία πολλών ειδών πληροφοριών, όπως για παράδειγμα των προσωπικών δεδομένων, των οποίων η προστασία κατά την συλλογή και επεξεργασία τους, θεσμοθετείται από μία σειρά κανόνων σύμφωνα με την σχετική νομοθεσία. (Νόμος 4624/2019)

Η εν λόγω νομοθεσία επιχειρεί να βάλει τάξη στις διαδικασίες διακίνησης προσωπικών δεδομένων μέσω του διαδικτύου. Με βάση το νέο νομικό πλαίσιο όσοι διαχειρίζονται προσωπικά δεδομένα θα πρέπει να έχουν την συγκατάθεση των υποκειμένων επεξεργασίας δίνοντας του όλες τις πληροφορίες για τον σκοπό της επεξεργασίας και τα μέτρα που εξασφαλίζουν την ιδιωτικότητα τους. Με τον τρόπο αυτό προστατεύονται τα προσωπικά δεδομένα από κακόβουλες χρήσεις.

Δίνεται με αυτό τον τρόπο η δυνατότητα σε κάθε οντότητα να επιλέγει εάν συμφωνεί με την επεξεργασία των προσωπικών του δεδομένων. Ακόμα και στην περίπτωση που είναι θετικός στην διαδικασία αυτή έχει πάντοτε την δυνατότητα να ζητά πρόσβαση, διόρθωση, διαγραφή ή ακόμα και τον περιορισμό της επεξεργασίας.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να λαμβάνουν τα απαραίτητα μέτρα(τεχνικά και οργανωτικά) που εξασφαλίζουν το μέγιστο επίπεδο ασφαλείας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Σημαντικό ρόλο έχει η υποχρεωτική ύπαρξη, σε κάθε δημόσιο φορέα, Υπεύθυνου Προστασίας Δεδομένων (DPO). Ο ρόλος του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων είναι συμβουλευτικός και υποστηρικτικός, με σκοπό να ενημερώνει, συμβουλεύει και παρακολουθεί τον φορέα αναφορικά με τη συμμόρφωση αυτής με τον Κανονισμό, με σκοπό την ελαχιστοποίηση του κινδύνου παραβίασης.

Τέλος στην περίπτωση που διαπιστωθεί παραβίαση δεδομένων προσωπικού χαρακτήρα ο υπεύθυνος πρέπει να ενημερώνει την Αρχή άμεσα και να γνωστοποιεί την φύση της παραβίασης, το στοιχείο επικοινωνίας του υπεύθυνου επεξεργασίας, τις συνέπειες της παραβίασης και τα μέτρα που έχουν ληφθεί για την αντιμετώπιση της παραβίασης

1.1 Σκοπός Διπλωματικής Εργασίας

Σκοπός της παρούσας διπλωματικής εργασίας είναι να αναλυθεί το θεσμικό πλαίσιο των δύο νομοθεσιών που απαιτούνται για την σωστή λειτουργία των υπηρεσιών τη Ηλεκτρονικής Διακυβέρνησης. Του νόμου 4727/2020 που αναρτήθηκε με ΦΕΚ στις 23-09-2020 με τίτλο «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.» και του νόμου που αναρτήθηκε με ΦΕΚ στις 29-8-2019 με τίτλο «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.»

Κατά την διάρκεια της εργασίας γίνεται όσο το δυνατό καλύτερη αναφορά στα επιμέρους άρθρα των δύο νομοθεσιών που έχουν πλήρη συσχέτιση με την Ηλεκτρονική Διακυβέρνηση και τους τρόπους που θα εξασφαλιστεί πλήρως η προστασία των προσωπικών δεδομένων και η ιδιωτικότητα των οντοτήτων.

Προκειμένου να είναι εφικτός ο έλεγχος συμμόρφωσης του δημόσιου τομέα είναι αναγκαία η ύπαρξη ενός εργαλείου που θα ελέγχει και θα αξιολογεί των εκάστοτε φορέα ως προς την συμμόρφωση του με τις δύο νομοθεσίες που αναφέραμε. Για τον σκοπό αυτό δημιουργήθηκε το «Εργαλείο Αξιολόγησης Συμμόρφωσης με τις νομοθεσίες της Ηλεκτρονικής Διακυβέρνησης και την Ασφάλεια Προσωπικών Δεδομένων». Ο αρχικός στόχος του συγκεκριμένου εργαλείου είναι η αυτό-αξιολόγηση του κάθε φορέα με σκοπό την βελτίωση της συμμόρφωσης του. Έτσι κάθε φορέας θα μπορεί να γνωρίζει τον βαθμό αξιολόγησης του ανά πάσα στιγμή και θα έχει την δυνατότητα να προχωράει στις αναγκαίες αλλαγές-βελτιώσεις.

1.2 Δομή Διπλωματικής Εργασίας

Η διπλωματική εργασία, μετά τα εισαγωγικά της στοιχεία στο 1^ο κεφάλαιο, προχωράει στο 2^ο κεφάλαιο όπου γίνεται μια αναφορά στο γενικότερο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης. Αναλύει τους τύπους Ηλεκτρονικής Διακυβέρνησης που είναι διαθέσιμοι στις μέρες μας και παρουσιάζει τα οφέλη που υπάρχουν από την χρήση της. Από την άλλη δίνονται και οι ανασταλτικοί παράγοντες που υπάρχουν και “εμποδίζουν” σε κάποιες περιπτώσεις την εφαρμογή της. Στο τέλος του 2^{ου} κεφαλαίου γίνεται ιστορική αναδρομή τόσο για τις νομοθεσίες που αφορούν την Ηλεκτρονική Διακυβέρνηση όσο και τις νομοθεσίες περί προστασίας των προσωπικών δεδομένων.

Προχωρώντας στο 3^ο κεφάλαιο αναλύει το θεσμικό πλαίσιο του ισχύοντος νόμου που αφορά την Ηλεκτρονική Διακυβέρνηση και συγκεκριμένα του Νόμου 4727/2020 ο οποίος αναρτήθηκε με ΦΕΚ στις 23-9-2020. Αναλύονται τα σημαντικότερα άρθρα αυτού και κάποιες σημαντικές διατάξεις που αποσκοπούν στην εφαρμογή της Ηλεκτρονικής Διακυβέρνησης στο Ελληνικό Κράτος.

Στο 4^ο κεφάλαιο γίνεται αντίστοιχα ανάλυση του θεσμικού πλαισίου του τελευταίου νόμου 4624/2019 που αφορά την προστασία προσωπικών δεδομένων ο οποίος αναρτήθηκε με ΦΕΚ στις 29-8-2019.

Στα επόμενα δύο κεφάλαια (5^ο και 6^ο) παρουσιάζεται το Εργαλείο Αξιολόγησης Συμμόρφωσης με τις νομοθεσίες της Ηλεκτρονικής Διακυβέρνησης και την Ασφάλεια Προσωπικών Δεδομένων το οποίο δημιουργήθηκε στα πλαίσια της διπλωματικής εργασίας. Επίσης αναλύονται τα στοιχεία τα οποία λάβαμε από δημόσιο φορέα ο οποίος έκανε χρήση και αξιολογήθηκε από το συγκεκριμένο εργαλείο.

Κλείνοντας αναφέρονται όλα τα συμπεράσματα που εξάγαμε κατά την υλοποίηση της διπλωματικής εργασίας, τα προβλήματα που κληθήκαμε να αντιμετωπίσουμε, τους περιορισμούς που προέκυψαν κατά την διάρκεια υλοποίησης και τα μελλοντικά σχέδια-στόχους τους οποίους έχουμε θέσει.

2. Το πλαίσιο της Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα

2.1 Ορισμός Ηλεκτρονικής Διακυβέρνησης

Η Ηλεκτρονική Διακυβέρνηση (eGovernment) αφορά στον εκσυγχρονισμό του Κράτους και της Δημόσιας Διοίκησης, με όχημα τις Τεχνολογίες Πληροφοριών και Επικοινωνιών (ΤΠΕ), με στόχο το ριζικό μετασχηματισμό των υφιστάμενων διαδικασιών και την αναβάθμιση των παρεχόμενων υπηρεσιών, σε υπηρεσίες προστιθέμενης αξίας, προκειμένου η Διοίκηση να καταστεί αποτελεσματικότερη και αποδοτικότερη, εξασφαλίζοντας την ικανοποίηση των αναγκών του κοινωνικού συνόλου και προάγοντας την ενεργή συμμετοχή των πολιτών.

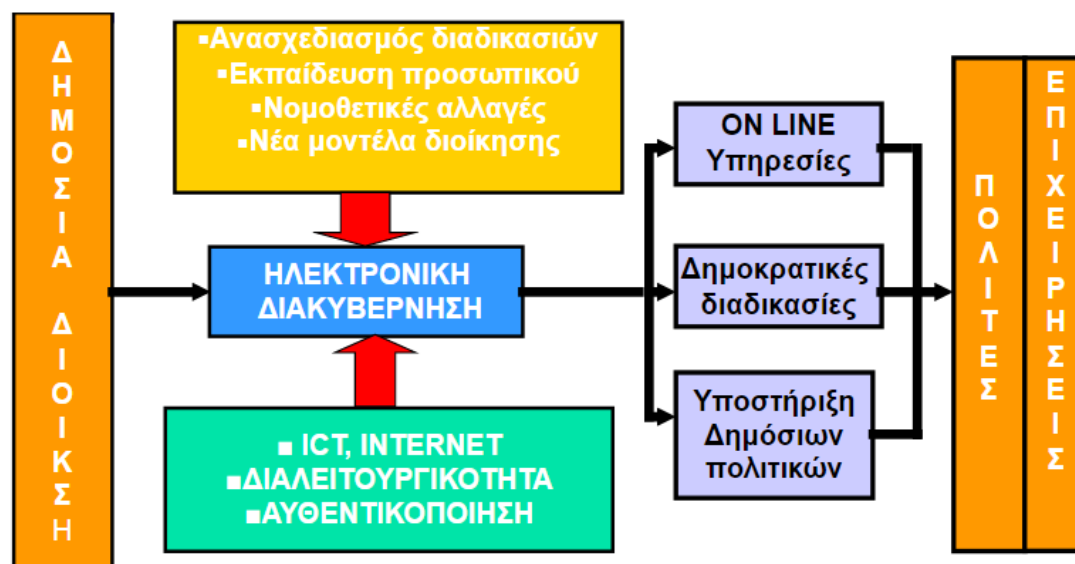
Σύμφωνα με την Ευρωπαϊκή Ένωση: Ηλεκτρονική διακυβέρνηση είναι «η χρήση των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ) στις δημόσιες διοικήσεις, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού. Σκοπός είναι η βελτίωση των δημόσιων υπηρεσιών, καθώς και η ενίσχυση των δημοκρατικών διαδικασιών και των διαδικασιών στήριξης των δημόσιων πολιτικών». [1]

Ενώ ο Οργανισμός Οικονομικής Συνεργασίας & Ανάπτυξης (Ο.Ο.Σ.Α.) αναφέρει

α) «η ηλεκτρονική διακυβέρνηση ορίζεται ως η παροχή υπηρεσιών μέσω του Internet και άλλων δραστηριοτήτων που σχετίζονται με το Internet, όπως είναι οι ηλεκτρονικές διαβουλεύσεις»

β) «η ηλεκτρονική διακυβέρνηση είναι η χρήση των ΤΠΕ στη δημόσια διοίκηση. Αν και η έμφαση της χρήσης των ΤΠΕ είναι γενικά στην παροχή υπηρεσιών, ο ευρύτερος ορισμός περιλαμβάνει την υποστήριξη όλων των διαστάσεων της δραστηριότητας της δημόσιας διοίκησης»,

γ) «η ηλεκτρονική διακυβέρνηση ορίζεται ως η δυνατότητα μετασχηματισμού της δημόσιας διοίκησης μέσω της χρήσης των ΤΠΕ ή ακόμη ο όρος αυτός μπορεί να χρησιμοποιηθεί για να περιγράψει τις νέες μορφές της δημόσιας διοίκησης που μπορούν να αναπτυχθούν βάσει των ΤΠΕ. Η διάσταση αυτή συνήθως συνδέεται με τη χρήση Internet». [2]



Εικόνα 2.1: Αναπαράσταση Ηλεκτρονικής Διακυβέρνησης [3]

2.2 Τύποι Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Οι υπηρεσίες Ηλεκτρονικής Διακυβέρνησης χωρίζονται σε τρεις κατηγορίες ανάλογα με το ποιος τις παρέχει και σε ποιους απευθύνονται. Οι υπηρεσίες αυτές παρέχονται από τη Δημόσια Διοίκηση προς

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

πολίτες, επιχειρήσεις ή εργαζομένους ή ανάμεσα σε φορείς της Διοίκησης. Από τη Δημόσια Διοίκηση προς άλλα μέρη:

- **G2C (Government to Citizen):**

Διαδικασίες που αφορούν στις σχέσεις αλληλεπίδρασης μεταξύ των δημόσιων οργανισμών και των πολιτών. Αποτελεί μια σημαντική κατηγορία της Ηλεκτρονικής διακυβέρνησης καθώς ο στόχος της είναι να εξυπηρετήσει με τον καλύτερο δυνατό τρόπο τους πολίτες στις συναλλαγές τους με το κράτος. Κύριος στόχος είναι η μείωση του χρόνου διεκπεραίωσης συναλλαγής και του βαθμού δυσκολίας, μέσω της μείωσης της γραφειοκρατίας. Είναι γνωστό άλλωστε ότι οι συναλλαγές των πολιτών με κρατικούς φορείς είναι καθημερινοί.

- **G2B (Government to Business) :**

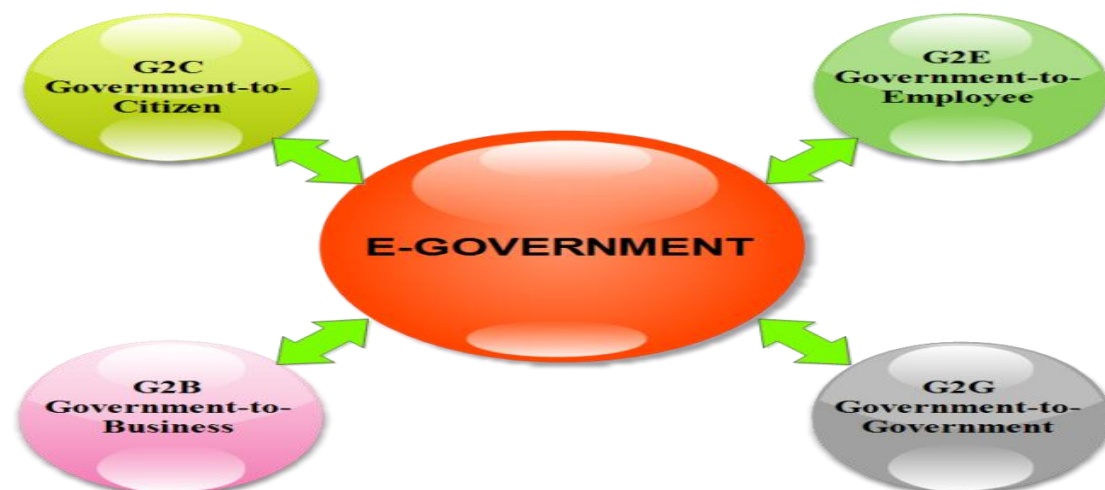
Διαδικασίες που αφορούν στις σχέσεις αλληλεπίδρασης μεταξύ των επιχειρήσεων με το κράτος. Πρόκειται για ένα ιδιαίτερο σύμμαχο που έχουν οι επιχειρήσεις με στόχο την άμεση διευθέτηση διαδικασιών μεταξύ πελατών(επιχειρήσεις) και κρατικών οργανισμών. Ο τρόπος λειτουργίας μιας επιχείρησης αρκετές φορές είναι δομημένος με σύνθετο τρόπο και απαιτεί διαρκή επαφής με οργανισμούς όσο αφορά στην έκδοση εγγράφων και πληρωμές προς το κράτος.

- **G2E (Government to Employee):**

Πρόκειται για παρόμοιο τύπο με το G2C. Αναφέρεται και πάλι σε πολίτες αλλά με την ιδιότητα των υπαλλήλων. π.χ για την συναλλαγή ενός εργαζομένου με τον ΟΑΕΔ ή το ασφαλιστικό του ταμείο.

- **G2G (Government to Government-national):**

Η κατηγορία αυτή αναφέρεται στα διάφορα είδη υπηρεσιών που πραγματοποιούνται μεταξύ των φορέων της Δημόσιας Διοίκησης σε εθνικό επίπεδο.



Εικόνα 2.2: Τύποι Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

2.3 Οφέλη της ηλεκτρονικής διακυβέρνησης

i. Τα οφέλη της ηλεκτρονικής διακυβέρνησης στον δημόσιο τομέα.

Χάρη στην ανάπτυξη εφαρμογών-υπηρεσιών e-government είναι πλέον εφικτή η αλληλεπίδραση μεταξύ υπηρεσιών του δημόσιου τομέα και των πολιτών, με την βοήθεια αυτοματοποιημένων διαδικασιών που λειτουργού με αποδοτικό τρόπο και με τον ελάχιστο δυνατό χρόνο.

Η εφαρμογή των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στον δημόσιο τομέα βοηθάει στην μείωση των κρατικών δαπανών-εξόδων, εάν συγκρίνουμε τον τρόπο με τον οποίο λειτουργούσε το δημόσιο μέχρι πριν μερικά χρόνια. Επιπλέον μειώνεται και ο χρόνος διεκπεραίωσης για μια συναλλαγή πολίτη-δημοσίου καθώς δίνεται η δυνατότητα η συναλλαγή αυτή να γίνει ανεξαρτήτως της απόστασης μεταξύ πελάτη και υπηρεσίας.

Παρατηρούμε πως λόγω των υπηρεσιών e-government στον δημόσιο τομέα επιτυγχάνεται αποδοτικότητα, αποτελεσματικότητα και σημαντική μείωση των δαπανών.

ii. Τα οφέλη της ηλεκτρονικής διακυβέρνησης στον ιδιωτικό τομέα

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

Όπως στον δημόσιο έτσι και στον ιδιωτικό τομέα (π.χ επιχειρήσεις) προκύπτουν σημαντικά οφέλη από την εφαρμογή υπηρεσιών e-government. Το κόστος και ο χρόνος που απαιτείται για την διαδικασία της συναλλαγής μειώνεται στο ελάχιστο δυνατό. Οι ιδιοκτήτες επιχειρήσεων μπορούν να κάνουν συναλλαγές τόσο με υπηρεσίες του δημόσιου τομέα όσο και με πολίτες. Ειδικότερα όσο αφορά τις καθημερινές συναλλαγές με κρατικούς φορείς για την λήψη πιστοποιητικών εγγράφων ή για την υποβολή δηλώσεων (Φ.Π.Α) ή για πληρωμές.

iii. Τα οφέλη της ηλεκτρονικής διακυβέρνησης στον πολίτη

Το σημαντικότερο όφελος που έχουν οι πολίτες από την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης αφορά στην μείωση της γραφειοκρατίας που συνεπάγεται και μείωση του χρόνου αναμονής- διεκπεραίωσης και την βελτίωση της ποιότητας των υπηρεσιών που το παρέχονται. Τα οφέλη που αποκομίζουν οι πολίτες είναι τα εξής:

- Αδιάλειπτη χρήση των υπηρεσιών, 365 μέρες τον χρόνο.
- Πρόσβαση στις υπηρεσίες από το σπίτι.
- Άμεση εξυπηρέτηση και γρήγορη διεκπεραίωση συναλλαγών.
- Έλεγχος της διαδικασίας ηλεκτρονικά.
- Όλες του οι πληροφορίες βρίσκονται σε ηλεκτρονική μορφή και έτσι δεν απαιτείται η πληθώρα εγγράφων σε χαρτί που ελλοχεύει πάντα ο κίνδυνος να χαθεί το οτιδήποτε. Σε αυτή την περίπτωση ο πολίτης θα έπρεπε να μεταβεί εκ νέου στην υπηρεσία ώστε να του παραδώσει ξανά το απολεσθέν έγγραφο.
- Και το σημαντικότερο ότι ο πολίτης εξοικονομεί χρόνο διότι δεν χρειάζεται να μεταβαίνει στην εκάστοτε υπηρεσία για τις συναλλαγές του και επιπλέον διότι κάθε υπηρεσία θα μπορεί να επικοινωνεί ηλεκτρονικά με την άλλη για την λήψη των απαιτούμενων στοιχείων.

2.4 Ανασταλτικοί παράγοντες για την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης.

Η εφαρμογή της Ηλεκτρονικής Διακυβέρνησης σίγουρα αποτελεί ένα θετικό βήμα στην οργάνωση ενός κράτους. Από την άλλη όμως υπάρχει και μια σειρά παραγόντων που λειτουργούν ανασταλτικά στον εκσυγχρονισμό αυτό.

A. Οικονομικοί παράγοντες:

Προκειμένου να αναπτυχθεί κατάλληλα η λειτουργία της Ηλεκτρονικής Διακυβέρνησης απαιτούνται μια σειρά πόρων. Οι ήδη υπάρχουσες υποδομές δεν επαρκούν για την εξασφάλιση της εύρυθμης λειτουργίας. Είναι φανερό ότι είναι αναγκαίος ο εκσυγχρονισμός όλου του τεχνολογικού εξοπλισμού των κρατικών φορέων ώστε να ανταποκριθούν με επιτυχία στο ιδιαίτερο όγκο δεδομένων. Εκτός αυτού οικονομικοί πόροι θα δαπανηθούν και για την εκπαίδευση των υπαλλήλων που θα ασχοληθούν με την λειτουργία του εξοπλισμού. Γίνεται κατανοητό ότι χρειάζεται να δαπανηθεί ένα μεγάλο ποσό του κρατικού προϋπολογισμού προκειμένου η Ηλεκτρονική Διακυβέρνηση να είναι ικανή να λειτουργήσει εποικοδομητικά για όλες τις λειτουργίες ενός κράτους.

B. Έλλειψη τεχνολογικής παιδείας:

Εάν αναλογιστούμε την γεωμορφολογία της Ελλάδας θα διακρίνουμε ότι υπάρχουν αρκετά σημεία που η γεωγραφική τους θέση δεν επιτρέπει την χρήση τεχνολογικών μέσων. Επίσης σύμφωνα με την Απογραφή Πληθυσμού-Κατοικιών 2011 από την “Ελληνική Στατιστική Αρχή” βλέπουμε ότι ένα μεγάλο ποσοστό κατοίκων στην Ελλάδα είναι σε ηλικία που είναι αποδεδειγμένα δύσκολη η συμμετοχή στην τεχνολογική ανάπτυξη και η χρήση ψηφιακών μέσων.

Ομάδες ηλικιών	Σύνολο
0-14	1.569.268
15-19	553.276
20-29	1.350.868
30-39	1.635.304
40-49	1.581.095
50-59	1.391.854
60-69	1.134.045
70-79	1.017.242
80+	583.334
Σύνολο	10.816.286

25.8%

Εικόνα 2.3: Απογραφή Πληθυσμού 2011

Με βάση το σχήμα το ποσοστό των ανθρώπων στην Ελλάδα που είναι μεγαλύτερο των 60 ετών είναι 25.8%. Πρόκειται για το ¼ του συνολικού πληθυσμού της χώρας.

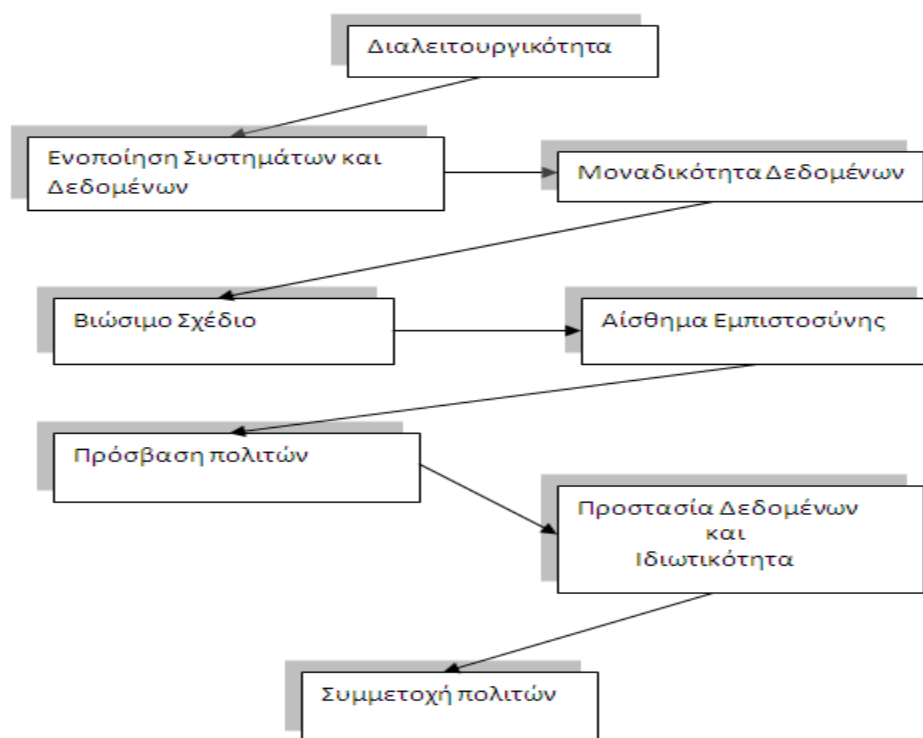
Υπάρχουν αρκετοί πολίτες στις μέρες μας οι οποίοι βιώνουν τον ψηφιακό αποκλεισμό καθώς δεν διαθέτουν πρόσβαση στο διαδίκτυο είτε λόγω προχωρημένης ηλικίας είτε λόγω ότι μένουν σε απομακρυσμένες περιοχές. Ένα ποσοστό επίσης δεν έχει την απαραίτητη εξοικείωση με τους υπολογιστές και την τεχνολογία. Με την εφαρμογή της ηλεκτρονικής διακυβέρνησης το ψηφιακό χάσμα σε συγκεκριμένες ομάδες πολιτών θα μεγαλώσει.

Με τον όρο ψηφιακό χάσμα εννοείται το κενό που παράγεται ανάμεσα σε άτομα ή και ομάδες που ωφελούνται από τις νέες τεχνολογίες και σε εκείνα που δεν ωφελούνται εξαιτίας κοινωνικών και οικονομικών παραγόντων. Θεωρείται ζήτημα μείζονος σημασίας εξαιτίας σοβαρής επιπτώσεις του στην ικανότητα του ανθρώπου να αποκτά γνώση.

2.5 Συμμετοχή πολιτών και Διαλειτουργικότητα συστημάτων

Διαλειτουργικότητα (Interoperability) ορίζεται η ικανότητα ενός πληροφοριακού συστήματος να επικοινωνεί με το εξωτερικό περιβάλλον του, προκειμένου αρχικά να ανταλλάξει και στη συνέχεια να επεξεργαστεί πληροφορίες που γίνονται με τον ίδιο τρόπο κατανοητές από όλα τα μέρη, τόσο από το πληροφοριακό σύστημα, όσο και από τα εξωτερικά πληροφοριακά συστήματα. [4]

Η ροή των απαραίτητων ενεργειών ώστε να επιτύχει η ενεργή συμμετοχή των πολιτών σε εφαρμογές Ηλεκτρονικής Διακυβέρνησης δίνεται στο παρακάτω σχήμα και θα αναλυθεί.



Εικόνα 2.4:Ροή ενεργειών για επιτυχή συμμετοχή πολιτών

Όπως είναι κατανοητό κάθε φορέας χρησιμοποιεί ένα δικό του πληροφοριακό σύστημα διαχείρισης μιας και επεξεργάζονται διαφορετικού είδους δεδομένα. Ωστόσο κάποια από τα δεδομένα είναι κοινά και αφορούν συνήθως τα αμετάβλητα στοιχεία ενός άλλου φορέα ή ενός πολίτη. Σε αυτή την περίπτωση είναι δυνατή η ανταλλαγή καταχωρημένων στοιχείων που εξυπηρετεί στην γρηγορότερη εξυπηρέτηση.

Προκειμένου να επιτευχθεί μεγαλύτερος βαθμός διαλειτουργικότητας ένα σημαντικό βήμα είναι η ενοποίηση των συστημάτων και των δεδομένων. Με άλλα λόγια η δημιουργία μίας κοινής βάσης δεδομένων η οποία θα αφορά όλα εκείνα τα στοιχεία ενός ατόμου ή ενός φορέα τα οποία δεν υπόκειται σε αλλαγές και θα μπορούν να χρησιμοποιούνται από όλους. Βασικό χαρακτηριστικό αυτής της ενοποίησης θα είναι η μοναδικότητα των δεδομένων. Κάθε φορέας θα μπορεί να εισάγει στοιχεία τα οποία θα είναι επιβεβαιωμένα με κάθε δυνατό τρόπο ώστε ο καθένας που θα τα χρησιμοποιεί στην συνέχεια να είναι σίγουρος για την εγκυρότητα αυτών χωρίς να προβαίνει σε περαιτέρω έλεγχο. Είναι κατανοητό ότι με αυτό τον τρόπο η εξυπηρέτηση θα είναι ταχύτερη και οι χρήστες αποφεύγουν την περιττή ταλαιπωρία.

Οι παραπάνω ενέργειες εξασφαλίζουν την βιωσιμότητα του σχεδίου καθώς από τη μία πλευρά μειώνονται οι πόροι και από την άλλη αυξάνεται η αποτελεσματικότητα. Ο συνδυασμός αυτών των δύο οδηγεί σε ένα σχέδιο με όραμα.

Ο σημαντικότερος παράγοντας σε αυτές τις διαδικασίες είναι ο χρήστης-πολίτης. Ένα από τα δυσκολότερα πράγματα είναι το να νιώσει αίσθημα εμπιστοσύνης. Πώς είναι δυνατόν να επιτευχθεί αυτό; Οι φορείς της δημόσιας διοίκησης πρέπει να επενδύσουν στην εμπιστοσύνη των πολιτών. ο χρήστης πρέπει να κατανοήσει ότι όλες αυτές οι ενέργειες πραγματοποιούνται με σκοπό να διευκολύνουν την καθημερινότητά του. Ο καλύτερος τρόπος είναι να του φέρουν σε αντιπαράθεση τα παλαιότερα συστήματα τα οποία τον εξυπηρετούσαν σε σχέση με τα παρόντα που βασίζονται σε μεγάλο βαθμό σε αυτοματοποιημένα συστήματα.

Η πρόσβαση και η συμμετοχή των πολιτών σε τέτοιου είδους διαδικασίες θέτει ως προαπαιτούμενο την διασφάλιση της ιδιωτικότητας και την προστασία των προσωπικών δεδομένων. Προκειμένου να εξασφαλιστούν αυτά είναι αναγκαία η πλήρης εναρμόνιση με νομοθεσίες και κανόνες οι οποίοι θεσμοθετήθηκαν για αυτόν το σκοπό. Το νομοθετικό πλαίσιο το οποίο αφορά την ιδιωτικότητα και την προστασία των προσωπικών δεδομένων θα αναλυθεί σε επόμενο κεφάλαιο.

2.6 Πολιτικές ψηφιακής διακυβέρνησης και αρχές

Προκειμένου να γίνει σωστή εφαρμογή των πολιτικών της ψηφιακής διακυβέρνησης πρέπει να ακολουθήσουμε κάποιες αρχές, οι οποίες είναι οι ακόλουθες:

Αρχικά η τήρηση της νομιμότητας και όλο το διατάξεων που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα. Όλες οι ενέργειες σε εφαρμογές ηλεκτρονικής διακυβέρνησης πρέπει να στηρίζονται στην αρχή της διαφάνειας ώστε να μην υπάρχει παραμικρή υπόνοια για λανθασμένες ή κακόβουλες ενέργειες.

Επίσης σημαντική είναι η αρχή της ισότητας και ιδίως προσβασιμότητας με την έννοια του ότι όλοι οι πολίτες-χρήστες έχουν τη δυνατότητα για είσοδο και χρήση σε εφαρμογές, για το λόγο αυτό πρέπει να δίνεται ιδιαίτερη έμφαση σε απομακρυσμένες περιοχές.

Η έννοια της διαλειτουργικότητας έχει εξηγηθεί πλήρως σε προηγούμενο κεφάλαιο, και αφορά τη δυνατότητα ενός συστήματος να έχει επαφές με τα υπόλοιπα συστήματα που χρησιμοποιούνται από φορείς. Τα δεδομένα που εισάγονται είναι πάντοτε τεκμηριωμένα από τον εκάστοτε φορέα ανάλογα με την αρμοδιότητα του.

Τέλος η αρχή της ακεραιότητας της ασφάλειας και της εμπιστευτικότητας που αφορά όλα τα δεδομένα που επεξεργάζονται οι φορείς με τέτοιο τρόπο που να προστατεύει τα ατομικά δικαιώματα την προστασία των προσωπικών δεδομένων και να ενισχύει την ασφάλεια δικαίου.

Οι φορείς σχεδιάζουν και υλοποιούν υπηρεσίες και εφαρμογές με βασικό μέλημα την ευχρηστία και την ευκολία στην πρόσβαση. Πρέπει να λαμβάνονται υπόψη άτομα με δυσκολίες και αναπηρίες για τους οποίους θα πρέπει να παρέχεται η ίδια δυνατότητα πρόσβασης. Επίσης οι φορείς υλοποίησης θα πρέπει να μεριμνούν για την ασφάλεια των προσωπικών δεδομένων καθώς και για την ασφάλεια των Πληροφοριακών Συστημάτων. Θα πρέπει να υπάρχει πάντα ένα σχέδιο αντιμετώπισης και σχέδιο ασφαλείας σε περίπτωση κάποιου σφάλματος ή κακόβουλης ενέργειας. Σημαντική παράμετρος στην ασφάλεια αποτελούν οι τρέχουσες τεχνολογικές εξελίξεις. Είναι κατανοητό ότι με την πάροδο του χρόνου πρέπει να γίνονται συνεχώς βελτιώσεις στον τομέα αυτόν.

2.7 Νόμος Ψηφιακής Διακυβέρνησης

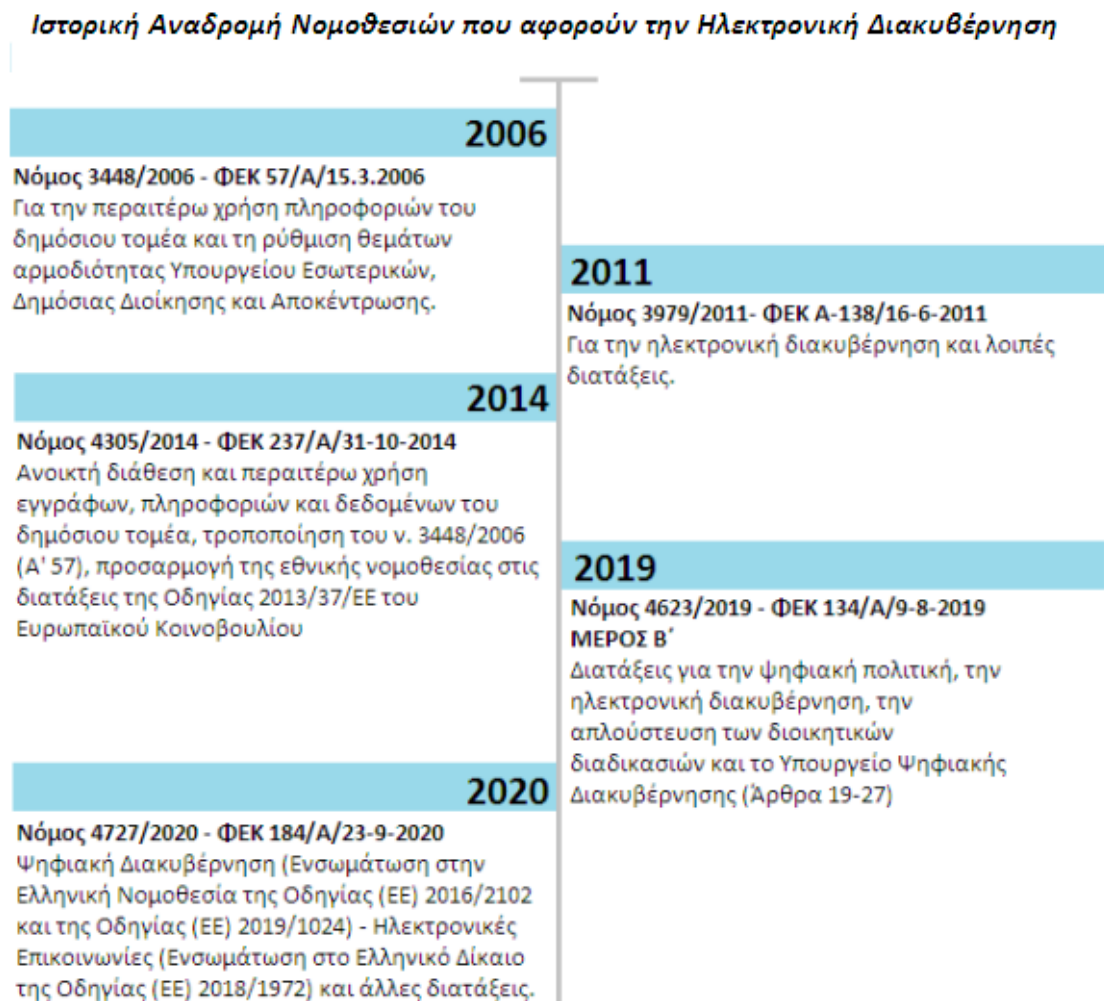
Το Υπουργείο Ψηφιακής Διακυβέρνησης κατέθεσε στην Ελληνική Βουλή σχέδιο νόμου με το τίτλο: "Νόμος Ψηφιακής Διακυβέρνησης - Ηλεκτρονικών Επικοινωνιών".

Σκοπός του παρόντος Κώδικα είναι η ολοκληρωμένη ρύθμιση όλων των θεμάτων που αφορούν την ψηφιακή διακυβέρνηση και κυρίως εκείνων που έχουν σχέση με τη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ) από τους φορείς του δημόσιου τομέα για τις ανάγκες της λειτουργίας τους

Επίσης αφορά την υποστήριξη της άσκησης των αρμοδιοτήτων και των συναλλαγών τους με φυσικά ή νομικά πρόσωπα.

Θεσπίζει την υποχρέωση της χρήσης ΤΠΕ από τους φορείς του δημόσιου τομέα στο πλαίσιο των αρμοδιοτήτων τους, όσο αφορά τις ανάγκες της λειτουργίας τους και την υποστήριξή τους στην παροχή υπηρεσιών με κάθε είδους οντότητες, καθώς και το δικαίωμα των τελευταίων να συναλλάσσονται με τους φορείς του δημόσιου τομέα μέσα από ΤΠΕ. [5]

2.8 Ιστορική Αναδρομή Νομοθεσιών Ηλεκτρονικής Διακυβέρνησης



Εικόνα 2.5: Ιστορική Αναδρομή Νομοθεσιών Ηλεκτρονικής Διακυβέρνησης

- Το 2006 ψηφίστηκε ο Νόμος 3448/2006 (ΦΕΚ 57/Α/15.3.2006) που ρυθμίζει την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα και τη ρύθμιση θεμάτων αρμοδιότητας Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης. Σκοπός αυτού του νόμου είναι ο καθορισμός (Οδηγία 2003/98/ΕΚ (L 345/90/31.12.2003)) , των όρων, των προϋποθέσεων, καθώς και των τρόπων διευκόλυνσης της περαιτέρω χρήσης εγγράφων, που βρίσκονται στην κατοχή φορέων του δημόσιου τομέα. Ήταν η πρώτη νομοθεσία που αφορούσε την περαιτέρω χρήση εγγράφων που διαχειρίζονται δημόσιοι φορείς.
- Το 2011 ψηφίζεται ο Νόμος 3979/2011 (ΦΕΚ Α-138/16-6-2011) για την ηλεκτρονική διακυβέρνηση. Σκοπός του νόμου αυτού είναι η επικοινωνία και συναλλαγή φυσικών προσώπων με τους φορείς του δημόσιου τομέα με χρήση τεχνολογιών πληροφορικής και επικοινωνιών και η της χρήση των ΤΠΕ από τους φορείς του δημόσιου τομέα.
- Το 2014 έρχεται η ψήφιση του Νόμου 4305/2014 (ΦΕΚ 237/Α/31-10-2014) με σκοπό την Ανοικτή διάθεση και περαιτέρω χρήση εγγράφων, πληροφοριών και δεδομένων του δημόσιου τομέα, τροποποίηση του ν. 3448/2006 (Α' 57), προσαρμογή της εθνικής νομοθεσίας στις διατάξεις της Οδηγίας 2013/37/ΕΕ του Ευρωπαϊκού Κοινοβουλίου.
- Το 2019 ψηφίζεται ο Νόμος 4623/2019 (ΦΕΚ 134/Α/9-8-2019). Στο Β' Μέρος του νόμου αναφέρεται στη Διάρθρωση Γενικής Γραμματείας Ψηφιακής Διακυβέρνησης και Απλούστευσης Διαδικασιών.

- Τέλος το 2020 ψηφίστηκε ο Νόμος 4727/2020 (ΦΕΚ 184/Α/23-9-2020) που αναφέρεται στην Ψηφιακή Διακυβέρνηση και προχωράει στην ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) .

2.9 Ιστορική Αναδρομή Νομοθεσιών για τα προσωπικά δεδομένα και τις ηλεκτρονικές επικοινωνίες

Ιστορική Αναδρομή Νομοθεσιών που αφορούν τα δεδομένα προσωπικού χαρακτήρα και τις ηλεκτρονικές επικοινωνίες



Εικόνα 2.6: Ιστορική Αναδρομή Νομοθεσιών για τα προσωπικά δεδομένα και τις ηλεκτρονικές επικοινωνίες

- Το 1997 ψηφίστηκε για πρώτη φορά νομοθεσία που διασφαλίζει την προστασία των προσωπικών δεδομένων. Συγκεκριμένα ο Νόμος 2472/1997 (ΦΕΚ Α-50/10-4-1997). Αντικείμενο του παρόντος νόμου 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.
- Το 2006 ψηφίστηκε ο Νόμος 3471/2006(ΦΕΚ 133/Α/28-6-2006) : Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.
- Το 2016 το Ευρωπαϊκό Κοινοβούλιο νομοθετεί τον Κανονισμό (ΕΕ) 2016/679 του συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

δεδομένων αυτών. Είναι ο κανονισμός ο οποίος κλήθηκαν όλες οι Ευρωπαϊκές χώρες να ακολουθήσουν.

- Η Ελλάδα σε συνέχεια του προηγούμενου κανονισμού ψηφίζει τον 2019 τον Νόμο 4624/2019 (ΦΕΚ 137/Α/29-8-2019) : Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις. Σκοπός του παρόντος νόμου είναι η αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και η εναρμόνιση με τις Ευρωπαϊκές οδηγίες.

3. Νόμος 4727/2020 Ψηφιακή Διακυβέρνηση

3.1 Εισαγωγή

Ο Ν. 4727/2020 (ΦΕΚ 184/23.09.2020) στοχεύει στην κωδικοποίηση και επικαιροποίηση της νομοθεσίας για την ψηφιακή διακυβέρνηση στο δημόσιο τομέα.

Με τον Νόμο Ψηφιακής Διακυβέρνησης, επιδιώκεται η δημιουργία των θεσμικών προϋποθέσεων για την επικοινωνία και συναλλαγή των πολιτών και των επιχειρήσεων με τους φορείς του δημόσιου τομέα με χρήση των τεχνολογιών πληροφορικής και επικοινωνιών.

Ο νέος Κώδικας εκσυγχρονίζει το πλαίσιο το οποίο ίσχυε μέχρι τώρα, προχωρώντας στην θέσπιση ενιαίων κανόνων για την διοίκηση, τη διαφάνεια, την αρχή της ισότητας και της προσβασιμότητας για όλους τους πολίτες, μέσα από σύγχρονες διαδικασίες που περιορίζουν σημαντικά φαινόμενα γραφειοκρατίας

Όπως αναφέρεται στην αιτιολογική έκθεση(Αιτιολογική Έκθεση στο σχέδιο νόμου «Κώδικας Ψηφιακής Διακυβέρνησης(Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) Κώδικας Ηλεκτρονικών Επικοινωνιών (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ)2018/1972) και άλλες διατάξεις») η νέα νομοθεσία επιδιώκει να εξοπλίσει το Κράτος, προκειμένου αυτό να είναι σε θέση να προσαρμόζεται στις ταχέως εξελισσόμενες τεχνολογικές και κοινωνικές εξελίξεις και να αποτελέσει επιταχυντή των εξελίξεων αυτών τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, με στόχο την προστασία του δημόσιου συμφέροντος.

Το κανονιστικό πλαίσιο της ψηφιακής διακυβέρνησης θα επιταχύνει και θα επεκτείνει τη χρήση Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ) τόσο στο πλαίσιο των φορέων του δημόσιου τομέα βελτιώνοντας τη λειτουργία τους από την πλευρά των πολιτών και των επιχειρήσεων. Το σχέδιο νόμου προβλέπει και ρυθμίζει, επίσης, την ηλεκτρονική επικοινωνία και συναλλαγή μεταξύ των φορέων του δημόσιου τομέα. Η άμεση ηλεκτρονική επικοινωνία μεταξύ των χειριστών μιας διοικητικής διαδικασίας μειώνει τον χρόνο που απαιτείται για την ολοκλήρωση της διαδικασίας, απελευθερώνοντας πόρους για τη δημόσια διοίκηση και χρόνο τόσο για τους πολίτες όσο και για τους φορείς.

Το πεδίο εφαρμογής του ρυθμιστικού πλαισίου για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών περιλαμβάνει τέσσερις Οδηγίες του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002 (L 108):

- (α) 2002/19/EK σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους.
- (β) 2002/20/EK για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.
- (γ) 2002/21/EK σχετικά με το κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών.
- (δ) 2002/22/EK για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, καθώς και την Οδηγία 2002/58/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (L 201). [6]

3.2 Νομοθεσία

3.2.1 Προσωπικός Αριθμός και Γενικές διατάξεις για τα ηλεκτρονικά έγγραφα

Προσωπικός αριθμός (Π.Α)

Κάθε φυσικό πρόσωπο διαθέτει ένα προσωπικό αριθμό ο οποίος πρόκειται για τον αριθμό υποχρεωτικής επαλήθευσης της ταυτότητάς του. Ο συγκεκριμένος αριθμός χορηγείται υποχρεωτικά σε κάθε φυσικό πρόσωπο ο οποίος διαθέτει ΑΦΜ ή ΑΜΚΑ. Ο προσωπικός αυτός ο αριθμός σε συνδυασμό με τα στοιχεία φυσικής ηλεκτρονικής ταυτοποίησης βοηθάει στην επαλήθευση της ταυτότητας των φυσικών προσώπων. Ο Π.Α αποτελεί στοιχείο αναγκαίο αλλά όχι επαρκές για την επαλήθευση ταυτότητας. Ο λόγος χρήσης του είναι η διευκόλυνση της διαλειτουργικότητας των ψηφιακών συστημάτων του δημόσιου τομέα.

Έκδοση Ηλεκτρονικών Δημοσίων Εγγράφων

Για τα ηλεκτρονικά ιδιωτικά έγγραφα προβλέπεται ότι σε περίπτωση που εκδίδονται από φυσικά ή νομικά πρόσωπα με χρήση εγκεκριμένης ηλεκτρονικής υπογραφής ή εγκεκριμένης ηλεκτρονικής σφραγίδας, γίνονται υποχρεωτικά αποδεκτά από τους φορείς του δημόσιου τομέα, και από φυσικά ή νομικά πρόσωπα ή νομικές οντότητες κατά την ηλεκτρονική διακίνησή τους. Κάθε ηλεκτρονικό έγγραφο ανάλογα με την μορφή του, πρέπει να ακολουθεί συγκεκριμένους κανόνες διαχείρισης και πρέπει να εμφανίζουν:

α) εγκεκριμένη ηλεκτρονική χρονοσφραγίδα
β) την εγκεκριμένη ηλεκτρονική σφραγίδα του φορέα ή την εγκεκριμένη ηλεκτρονική υπογραφή του αρμόδιου οργάνου.

Η ψηφιακή υπογραφή πρέπει φέρει ασφαλή χρονοσήμανση (secure timestamp), δηλαδή η ημερομηνία και η ώρα της υπογραφής να προέρχεται από κάποιο πιστοποιημένο server και όχι π.χ από το ρολόι του υπολογιστή του χρήστη.

Στην περίπτωση που η υπογραφή παίρνει την ώρα από το ρολόι του υπολογιστή ΔΕΝ ΕΙΝΑΙ ΕΓΚΥΡΗ!

γ) την ένδειξη «ακριβές αντίγραφο»

δ) τα στοιχεία του οργάνου που υπέγραψε το έγγραφο ως τελικώς υπογράφων.

ε) βεβαίωση ταύτισής τους με το έντυπο έγγραφο.

- Για τα πρωτότυπα ηλεκτρονικά δημόσια έγγραφα ισχύουν οι κανόνες α) και β).
- Για τα ηλεκτρονικά ακριβή αντίγραφα ισχύουν οι κανόνες α) , β), γ) και δ).
- Για τα ψηφιοποιημένα ηλεκτρονικά αντίγραφα ισχύουν οι κανόνες α) , β) και ε).

3.2.2 Ενδοδιοικητική οργάνωση ψηφιακής διακυβέρνησης

Ηλεκτρονική διακίνηση δημοσίων εγγράφων

Η διακίνηση Δημοσίων εγγράφων εντός του ίδιου δημόσιου φορέα σε κλειστά πληροφοριακά συστήματα προϋποθέτει την αυθεντικοποίηση κάθε χρήστη πριν από κάθε ενέργεια.

Η ηλεκτρονική διακίνηση Δημοσίων εγγράφων μεταξύ Δημοσίων φορέων γίνεται αποκλειστικά με χρήση Τ.Π.Ε και σύμφωνα με τις διατάξεις για προστασία κρατικών εγγράφων. Οι ενέργειες αυτές γίνονται σύμφωνα με τους κανόνες που αφορούν την έκδοση ηλεκτρονικών δημοσίων εγγράφων.

Ηλεκτρονικό πρωτόκολλο :Κάθε φορέας του δημοσίου τομέα καλείται να τηρεί πρωτόκολλο στο οποίο γίνονται καταχώρηση όλες οι πράξεις των εγγράφων. Πλέον ο κάθε φορέας θα τηρεί ηλεκτρονικό πρωτόκολλο για όλα τα έγγραφα τα οποία έχει στην κατοχή του στο πλαίσιο των αρμοδιοτήτων του, και η καταχώρηση στο ηλεκτρονικό πρωτόκολλο πραγματοποιείται ανεξάρτητα με τον τύπο του εγγράφου. Τα συστήματα τα οποία χρησιμοποιούνται για το ηλεκτρονικό πρωτόκολλο, μετά την καταχώρηση κάποιου εγγράφου, θα εκδίδουν ηλεκτρονικό αποδεικτικό στο οποίο θα αναγράφεται ο μοναδικός αριθμός πρωτοκόλλου, καθώς και ημερομηνιακά στοιχεία.

Για την ηλεκτρονική αρχειοθέτηση εγγράφων κάθε φορέας του δημοσίου τομέα τηρεί αποκλειστικά ηλεκτρονικά αρχεία των ηλεκτρονικών εγγράφων που απαιτούνται στο μετρώ άσκησης των

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

αρμοδιοτήτων και των δραστηριοτήτων του. Κάθε διαδικασία καταχώρισης καθώς και τα μέσα τα οποία χρησιμοποιούνται για αυτήν πρέπει να τηρούν τους όρους ασφαλείας ως προς την ακεραιότητα, την αυθεντικότητα, την εμπιστευτικότητα, την προσβασιμότητα καθώς και όλων των πληροφοριών και δεδομένων που περιέχονται στα έγγραφα αυτά. Τα έντυπα έγγραφα τα οποία έχουν αρχειοθετηθεί ηλεκτρονικά πρέπει να τηρούνται σε αρχείο για διάστημα πέντε ετών. Μετά το πέρας του συγκεκριμένου χρονικού περιθωρίου καταστρέφονται.

- I. Εμπιστευτικότητα: Εγγυάται ότι τα δεδομένα δεν αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες.
- II. Ακεραιότητα Δεδομένων :Εξασφαλίζει τη μη τροποποίηση των δεδομένων από μη εξουσιοδοτημένους χρήστες.
- III. Αυθεντικοποίηση: Η απόδειξη της ταυτότητας του χρήστη και η γνησιότητα των ενεργειών του. [7]

Χρήσιμη διαδικασία για τους φορείς του δημόσιου τομέα είναι η στατιστική επεξεργασία δεδομένων προκειμένου να υπάρχουν συμπεράσματα που αφορούν τον εκάστοτε φορέα και τον τρόπο λειτουργίας τους.

Ο δημόσιος φορέας θα επεξεργαστεί και θα εξάγει στοιχεία τα οποία προκύπτουν από ολοκληρωμένες διαδικασίες ή από έκδοση εγγράφων με χρήση Τ.Π.Ε. Τα στατιστικά στοιχεία θα τηρούνται ηλεκτρονικά με σκοπό την εξαγωγή συμπερασμάτων που αφορούν το χρόνο και το κόστος για τη διεκπεραίωση μιας διαδικασίας. Τα αποτελέσματα που εξάγονται από τη συγκεκριμένη διαδικασία θα δημοσιεύονται στον ιστότοπο του κάθε φορέα ανά συγκεκριμένο χρονικό διάστημα.

Σημαντικό βήμα στη συγκεκριμένη ενέργεια αποτελεί και το είδος των δεδομένων που τίθενται προς επεξεργασία. Εφόσον τα στοιχεία αποτελούν ή περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα, προτού συνεχίσουμε στην στατιστική επεξεργασία θα πρέπει τα δεδομένα να καταστούν ανώνυμα.

3.2.3 Παροχή ψηφιακών δημόσιων υπηρεσιών - Ενιαία ψηφιακή πύλη της δημόσιας διοίκησης.

Η Ενιαία Ψηφιακή Πύλη παροχής υπηρεσιών gov.gr, έχει ως στόχο να μετασχηματίσει τα γεγονότα ζωής (life events) σε συγκεκριμένες υπηρεσίες που παρέχουν τα πληροφοριακά συστήματα του Δημοσίου. [8] Οι βασικές λειτουργίες που θα παρέχει ορίζονται για όλες τις φιλοξενούμενες υπηρεσίες αφορούν τη παροχή ηλεκτρονικών υπηρεσιών (υπολογιστής, κινητό τηλέφωνο). Μέσω του Κέντρου Ταυτοποίησης ο πολίτης λαμβάνει ασφαλή πρόσβαση στις κυβερνητικές υπηρεσίες και την ηλεκτρονική ταυτοποίησή του. Αφότου έχει υποβάλει κάποιο αίτημα ο χρήστης λαμβάνει ειδοποιήσεις, απαντήσεις και αποτελέσματα σχετικά με την διεκπεραίωση του αιτήματος.

Η νομοθεσία προβλέπει ρυθμίσεις για την έκδοση εγγράφων μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης από κάθε φυσικό πρόσωπο που ενεργεί για τον εαυτό του ατομικά ή ως νόμιμος εκπρόσωπος νομικού προσώπου, καθώς και η ισχύς των εγγράφων αυτών. Περιγράφεται η διαδικασία που απαιτείται από τα άτομα που προχωρούν σε αίτηση για την έκδοση δημόσιων εγγράφων από τους φορείς του δημόσιου τομέα μέσω Ε.Ψ.Π., κατόπιν προηγούμενης αυθεντικοποίησης του χρήστη.

Η παροχή και η διακίνηση ηλεκτρονικών εγγράφων είτε αυτά είναι μεταξύ φορέων του δημόσιου τομέα είτε με φυσικά ή νομικά πρόσωπα πραγματοποιείται μέσω της Ενιαίας Ψηφιακής Πύλης(ΕΨΠ). Κάθε φορέας έχει την υποχρέωση να συνεργάζεται με τις αρμόδιες υπηρεσίες του Υπουργείου Ψηφιακής Διακυβέρνησης ώστε να διενεργεί τις παραπάνω ενέργειες με ασφαλή τρόπο. Κάθε φορέας του δημόσιου τομέα εφόσον σχεδιάσει ή τροποποιήσει οποιαδήποτε ψηφιακή δημόσια υπηρεσία είναι υποχρεωμένος να την υποβάλει προς αξιολόγηση και έγκριση στην υπηρεσία συντονισμού Ενιαίας Ψηφιακής Πύλης. Σκοπός της αίτησης είναι να αξιολογηθεί κατά πόσο τηρούνται όλοι οι κανόνες για τη χρήση της συγκεκριμένης υπηρεσίας.

Κάθε χρήστης της ΕΨΠ αποκτά πρόσβαση στις υπηρεσίες που παρέχονται μέσα από αυτήν, αφού προηγουμένως προβεί σε αυθεντικοποίηση. Η αυθεντικοποίηση γίνεται μετά από επιλογή του χρήστη με έναν από τους ακόλουθους τρόπους:

- Με τη χρήση των κωδικών-διαπιστευτηρίων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής Διακυβέρνησης.
- Με τη χρήση των κωδικών-διαπιστευτηρίων των συστημάτων ηλεκτρονικής τραπεζικής (e-banking) των πιστωτικών ιδρυμάτων.
- Με τη χρήση εγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής.

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

- Κάθε πρόσωπο το οποίο κατέχει διαπιστευτήρια οφείλει να λαμβάνει όλα τα μέτρα για την εμπιστευτικότητα τους και την ασφαλή φύλαξη των μέσων που κατέχει. Σε περίπτωση παρατήρησης παραβίασης ή απώλειας δεδομένων οφείλει να ειδοποιήσει άμεσα την αρμόδια υπηρεσία.

Για να προχωρήσει κάποια οντότητα σε έκδοση διαπιστευτηρίων είναι απαραίτητη η ταυτοποίηση των φυσικών προσώπων με σκοπό την αυθεντικοποίηση τους.

Η ταυτοποίηση διενεργείται με έναν από τους ακόλουθους τρόπους:

- ✓ Μέσω της Ανεξάρτητης Αρχής Δημοσίων Εσόδων.
- ✓ Με φυσική παρουσία του φυσικού προσώπου στα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ).
- ✓ Με τη χρήση εξ αποστάσεως ταυτοποίησης που παρέχει διασφάλιση ισοδύναμη με τη φυσική παρουσία. Η ταυτοποίηση αυτή μπορεί να διενεργείται μέσω του Εθνικού Μητρώου Επικοινωνίας Πολιτών.

Για την έκδοση εγγράφων μέσω της ενιαίας ψηφιακής Πύλης απαιτείται η προηγούμενη αυθεντικοποίηση του χρήστη. Κάθε έγγραφο πρέπει να φέρει επάνω του μοναδικού αναγνωριστικού αριθμό επαλήθευσης και προηγμένη εγκεκριμένη ηλεκτρονική σφραγίδα. Έγγραφα τα οποία δεν τηρούν τις συγκεκριμένες προϋποθέσεις δεν γίνονται αποδεκτά.

Οι υπάλληλοι των φορέων του δημόσιου τομέα υποχρεούνται να παραλαμβάνουν τα ηλεκτρονικά έγγραφα καθώς και τα έγγραφα που εκδίδονται ή διακινούνται μέσω της ΕΥΠ. Κατ' εξαίρεση γίνονται δεκτά έντυπα έγγραφα ή εκτυπώσεις ηλεκτρονικών εγγράφων ή των εγγράφων που εκδίδονται μέσω της ΕΥΠ όταν:

- ✓ Εφόσον υφίσταται πρόσκαιρη αντικειμενική αδυναμία παραλαβής ηλεκτρονικού εγγράφου από τον φορέα.
- ✓ Όταν υφίσταται άλλου τύπου αδυναμία παραλαβής που διαπιστώνεται με πράξη του Υπουργού Ψηφιακής Διακυβέρνησης.
- ✓ Στην περίπτωση που το φυσικό ή νομικό πρόσωπο ή νομική οντότητα έχει επιλέξει μη ηλεκτρονικό τρόπο επικοινωνίας.

Οι φορείς του δημόσιου τομέα που επιδίδουν έγγραφα σε οντότητες με χρήση ΤΠΕ υποχρεούνται να αντλούν τα στοιχεία επικοινωνίας των ανωτέρω προσώπων από το Εθνικό Μητρώο Επικοινωνίας Πολιτών.

Όλες οι ενέργειες των φορέων του δημόσιου τομέα που αφορούν τόσο υπηρεσίες και δημόσια έγγραφα όσο και εκπλήρωση αιτημάτων μπορεί να γίνει με την υποστήριξη ΤΠΕ με την προϋπόθεση ότι έχει προηγηθεί ταυτοποίηση και αυθεντικοποίηση τόσο των αιτούντων όσο και των υπαλλήλων και ότι έχουν τηρηθεί όλοι οι όροι ασφαλείας.

Ηλεκτρονικές πληρωμές

Επιτρέπεται η είσπραξη ειδικών φόρων, παραβόλων, τελών ενσήμων, χαρτοσήμων, προστίμων και εν γένει η οικονομική εκκαθάριση οφειλών φυσικών ή νομικών προσώπων ή νομικών οντοτήτων προς φορείς του δημόσιου τομέα, με χρέωση τραπεζικών λογαριασμών ή λογαριασμών πληρωμής που τηρούν οι υπόχρεοι ή με χρέωση καρτών πληρωμής που έχουν εκδοθεί στο όνομά τους.

Με την προϋπόθεση της αυθεντικοποίησης του υπόχρεου, η πληρωμή μπορεί να πραγματοποιείται είτε άμεσα από τον ίδιο είτε μέσω των Κέντρων Εξυπηρέτησης Πολιτών (ΚΕΠ) και των Ελληνικών Ταχυδρομείων (ΕΛΤΑ).

Για την εκτέλεση πράξης ηλεκτρονικής πληρωμής ο υπόχρεος υποβάλλει τουλάχιστον τις ακόλουθες πληροφορίες:

- Κωδικό υποχρέωσης που αντιστοιχεί στην οφειλή,
- Ποσό καταβολής,
- Ημερομηνία και προθεσμία καταβολής.

Εάν η ηλεκτρονική πληρωμή δεν είναι επιτυχής ή δεν ολοκληρωθεί, ο υπόχρεος ενημερώνεται αυτόματα για την αδυναμία χρήσης της συγκεκριμένης ψηφιακής δημόσιας υπηρεσίας και, εφόσον είναι δυνατόν, για τους λόγους της ανεπιτυχούς συναλλαγής.

Με την προϋπόθεση της αυθεντικοποίησης του δικαιούχου, μπορούν να καταβάλλονται οφειλές των φορέων του δημόσιου τομέα προς φυσικά ή νομικά πρόσωπα ή νομικές οντότητες μέσω της πίστωσης λογαριασμών του δικαιούχου.

Επικοινωνία και Ιστότοποι

- Οι φορείς του δημόσιου τομέα οφείλουν να χρησιμοποιούν ηλεκτρονικό τρόπο επικοινωνίας με φυσικά ή νομικά πρόσωπα και νομικές οντότητες. Με την επιφύλαξη ειδικών διατάξεων, τα φυσικά ή νομικά πρόσωπα και νομικές οντότητες έχουν δικαίωμα να επιλέξουν στο Εθνικό Μητρώο Επικοινωνίας Πολιτών μη ηλεκτρονικό τρόπο επικοινωνίας με τους ανωτέρω φορείς.
- Όλοι οι φορείς του δημόσιου τομέα υποχρεούνται να διατηρούν δικτυακούς τόπους χωρίς περιορισμούς πρόσβασης, με σκοπό την πληροφόρηση και την ενημέρωση. Είναι υπεύθυνοι για την εγκυρότητα, νομιμότητα, ποιότητα και επικαιροποίηση των πληροφοριών, δεδομένων και εγγράφων που αναρτούν ή κοινοποιούν προς ανάρτηση στον δικτυακό τους τόπο.
- Κάθε φορέας πρέπει να έχει επαρκή στοιχεία επικοινωνίας ώστε ο χρήστης να επικοινωνεί μαζί του εύκολα και γρήγορα.
- Ο ορισμένος από τον φορέα διαχειριστής είναι υπεύθυνος για την επικαιροποίηση και αναβάθμιση του δικτυακού τόπου όποτε αυτό απαιτείται.

3.2.4 Ψηφιακή προσβασιμότητα

Σύμφωνα με τις διατάξεις της ψηφιακής προσβασιμότητας είναι απαραίτητη η εισαγωγή ρυθμίσεων για την προσβασιμότητα σε ιστότοπους και εφαρμογές για φορητές συσκευές των οργανισμών του δημόσιου τομέα, προκειμένου οι υπηρεσίες τους να καταστούν περισσότερο προσβάσιμοι στους χρήστες και ιδίως στα άτομα με αναπηρίες.

Οι επιμέρους αρχές της προσβασιμότητας έχουν την ακόλουθη έννοια: [9]

1. Αντιληπτικότητα, που σημαίνει ότι οι πληροφορίες και τα συστατικά στοιχεία της διεπαφής με τον χρήστη παρουσιάζονται στους χρήστες με τρόπους που αυτοί μπορούν να αντιληφθούν
2. Χρησιμότητα, που σημαίνει ότι τα συστατικά στοιχεία διεπαφής με τον χρήστη, καθώς και η πλοήγηση είναι εύχρηστα
3. Κατανοησιμότητα, που σημαίνει ότι οι πληροφορίες και η λειτουργία της διεπαφής με τον χρήστη είναι κατανοητές
4. Στιβαρότητα, που σημαίνει ότι το περιεχόμενο είναι αρκετά στιβαρό, ώστε να ερμηνεύεται αξιόπιστα από ευρύ φάσμα πρακτόρων χρηστών, συμπεριλαμβανομένων και υποστηρικτικών τεχνολογιών.

A. Μητρώο Δημόσιων Ιστότοπων και Εφαρμογών

Απαραίτητη η εισαγωγή/εγγραφή του ιστότοπου κάθε φορέα στο «Μητρώο Δημόσιων Ιστότοπων και Εφαρμογών» (ΜΗ.Δ.ΙΣ.ΕΦ.).

Οι οργανισμοί του δημόσιου τομέα αναρτούν στον ιστότοπο τους πλήρη στοιχεία για την κατάσταση συμμόρφωσης των ιστότοπων και των εφαρμογών τους για φορητές συσκευές προς τις διατάξεις του παρόντος.

B. Επιμόρφωση υπαλλήλων και ευαισθητοποίηση του κοινού

Οι οργανισμοί του δημόσιου τομέα μεριμνούν και αναλαμβάνουν να ενημερώσουν:

- a. Το προσωπικό τους σε θέματα προσβασιμότητας των δικτυακών τόπων και είναι υπεύθυνα για την κατάρτισή τους.
- b. Το κοινό σχετικά με τα οφέλη για τους χρήστες.

3.2.5 Πιστοποιητικά υπηρεσιών εμπιστοσύνης

Τα πιστοποιητικά υπηρεσιών εμπιστοσύνης αποτελούν ηλεκτρονικές βεβαιώσεις που εκδίδονται από έναν πάροχο υπηρεσιών εμπιστοσύνης.

Είναι απαραίτητη η συχνός και προσεκτικός έλεγχος του πιστοποιητικού ως προς την ημερομηνία λήξης του, η οποία αναγράφεται πάνω σε αυτό.

Εφόσον διαπιστωθεί κάποιο σφάλμα να ο κάτοχος του, πρέπει να επικοινωνήσει άμεσα με τον πάροχο του.

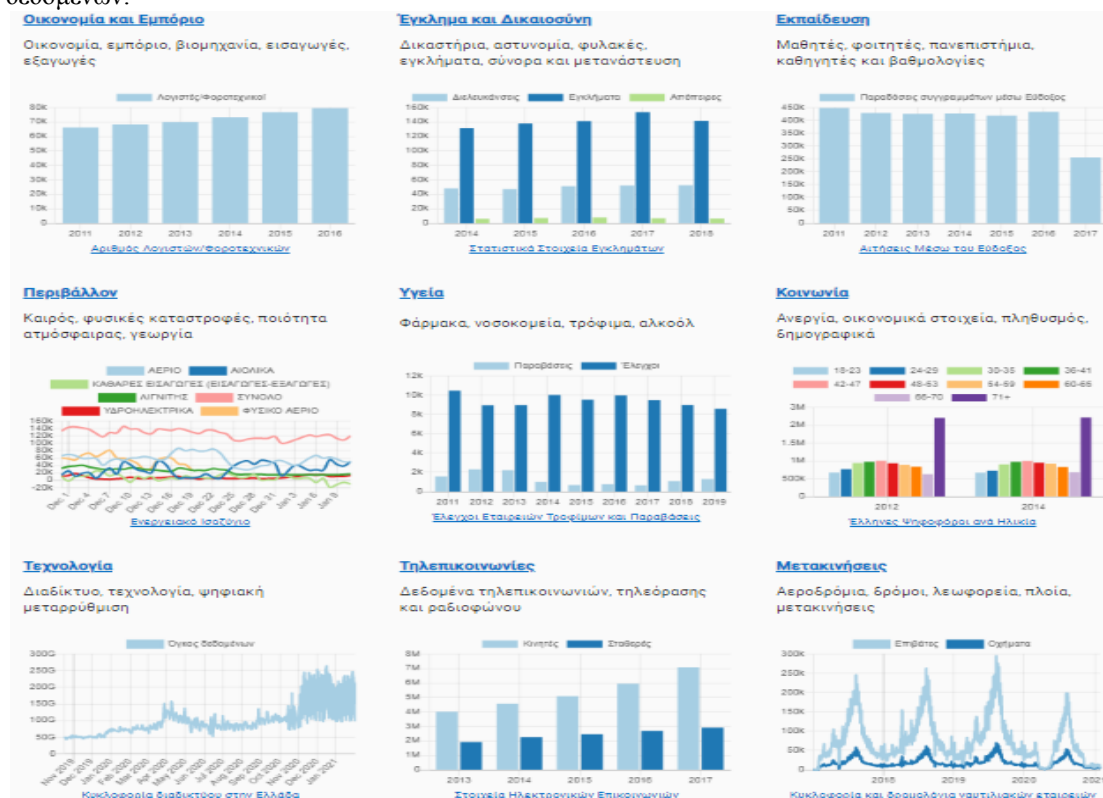
3.2.6 Ανοικτά δεδομένα και περαιτέρω χρήση πληροφοριών του δημόσιου τομέα.

Τι σημαίνει Ανοικτά δεδομένα:

Ο όρος Ανοικτά (κρατικά) δεδομένα αφορά πληροφορίες που συλλέγονται, παράγονται ή αποκτώνται δια αντιτίμου από τους δημόσιους φορείς (ένα άλλο όνομα είναι Πληροφορίες του δημόσιου τομέα) και διατίθενται δωρεάν προς περαιτέρω χρήση για οιονδήποτε σκοπό. Στην άδεια καθορίζονται οι όροι χρήσης.

- α. Πλεονεκτήματα της Χρήσης δεδομένων:
 - Οι επιδόσεις μπορούν να αυξηθούν χάρη στα Ανοικτά δεδομένα, συμβάλλοντας έτσι στη βελτίωση της απόδοσης των δημόσιων υπηρεσιών.
 - Η οικονομία έχει μόνο να ωφεληθεί από τη διευκόλυνση της πρόσβασης σε πληροφορίες, περιεχόμενο και γνώσεις, που συμβάλλουν με τη σειρά τους στην ανάπτυξη καινοτόμων υπηρεσιών και στη δημιουργία νέων επιχειρηματικών μοντέλων.
 - Δίνεται δυνατότητα βελτίωσης του κράτους πρόνοιας. [10]

Στον ιστότοπο <https://www.data.gov.gr> δίνονται 10 θεματικές ενότητες με 39 σειρές ανοικτών δεδομένων:



Εικόνα 2.1: Θεματικές Ενότητες Δεδομένων

Στην περίπτωση από κάποιο έγγραφο δεν είναι διαθέσιμο σε διαδικτυακή μορφή κάθε ενδιαφερόμενος μπορεί να υποβάλει αίτημα προς οποιονδήποτε δημόσιο φορέα για τη χορήγηση του εγγράφου. Με τη σειρά του ο δημόσιος φορέας επεξεργάζεται τις αιτήσεις και χορηγεί το έγγραφο προς τον ενδιαφερόμενο ως εξής:

- α. Οριστικοποίηση η χορήγηση του εγγράφου εντός 20 ημερών από την παραλαβή της αίτησης.
- β. Σε περίπτωση που είναι αδύνατη η χορήγηση του εγγράφου ο φορέας είναι υποχρεωμένος να ανακοινώσει προς τον ενδιαφερόμενο τους λόγους της απόρριψης.

Οι φορείς του δημόσιου τομέα υποχρεούνται να ενημερώνουν εγγράφως τους αιτούντες έγγραφα για περαιτέρω χρήση σχετικά με τη δυνατότητα άσκησης προσφυγής του άρθρου και την προθεσμία αυτής.

Ερευνητικά δεδομένα

Ως ερευνητικά δεδομένα χαρακτηρίζονται τα δεδομένα που χρησιμοποιούνται ως βασικές πηγές στην ερευνητική διαδικασία, όπως πχ. αριθμητικά δεδομένα, αρχεία κειμένων, εικόνων και ήχων. [11]

Τα ερευνητικά δεδομένα προκειμένου να χρησιμοποιηθούν θα πρέπει να:

- Προστατεύουν την ιδιωτική ζωή και τα δεδομένα προσωπικού χαρακτήρα.
- Να τηρούν την εμπιστευτικότητα και την εθνική ασφάλεια.
- Να προστατεύουν τα δικαιώματα πνευματικής ιδιοκτησίας.

3.2.7 Ψηφιακή διαφάνεια - Πρόγραμμα Διαύγεια

1. Τι είναι το πρόγραμμα Διαύγεια:

Το πρόγραμμα Διαύγεια (νόμος 3861/2010) στοχεύει στην επίτευξη της μέγιστης δυνατής δημοσιότητας της κυβερνητικής πολιτικής και της διοικητικής δραστηριότητας, τη διασφάλιση της διαφάνειας και την εμπέδωση της υπευθυνότητας και της λογοδοσίας από την πλευρά των φορέων άσκησης της δημόσιας εξουσίας.

Από τον Οκτώβριο 2010 αναρτώνται σε ένα σημείο στο διαδίκτυο όλες οι αποφάσεις πράξεων των κυβερνητικών και διοικητικών οργάνων, λαμβάνοντας ειδική μέριμνα για τις πράξεις που αφορούν στην εθνική άμυνα και τα ευαίσθητα προσωπικά δεδομένα.

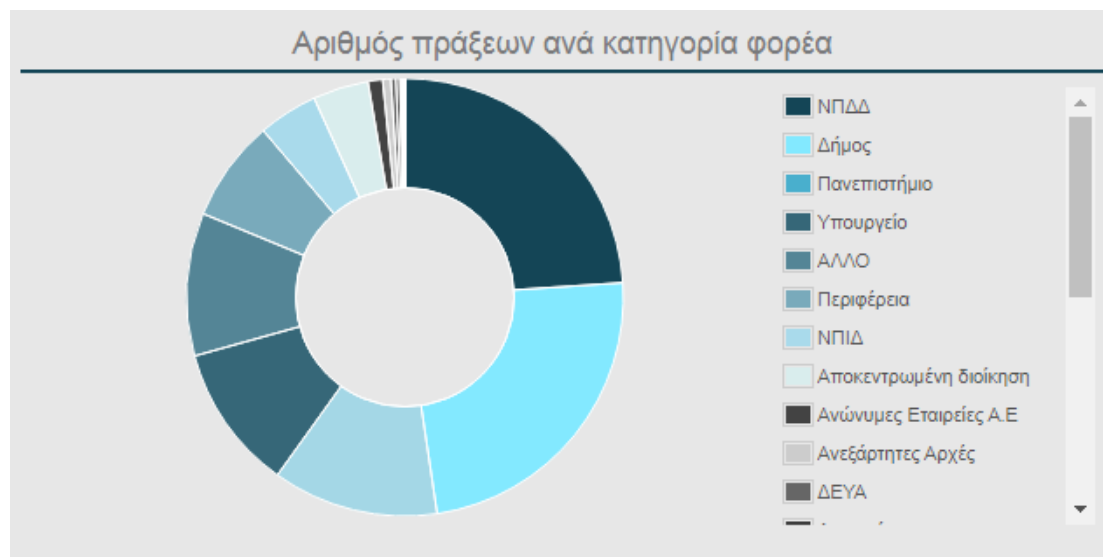
Σήμερα στο πρόγραμμα Διαύγεια είναι ενταγμένοι φορείς του στενού και ευρύτερου δημόσιου τομέα και των Οργανισμών Τοπικής Αυτοδιοίκησης Α και Β βαθμού. [12]

ΑΔΑ (ΑΡΙΘΜΟΣ ΔΙΑΔΙΚΤΥΑΚΗΣ ΑΝΑΡΤΗΣΗΣ)

Είναι ένας μοναδικός κωδικός που αποκτά κάθε πράξη μετά την ολοκλήρωση της καταχώρισης της στην εφαρμογή της Διαύγειας.

Ο κωδικοποιημένος αριθμός παράγεται αλγοριθμικά με βάση την ημερομηνία καταχώρισης, το φορέα και τον αύξοντα αριθμό πράξης του φορέα, εγγράφεται αυτόματα σε κάθε σελίδα του εγγράφου που αναρτάται και πρέπει αναγράφεται πάνω στο σχέδιο κάθε πράξης χειρόγραφα πριν διεκπεραιωθεί.

Είναι η ταυτότητα της κάθε αναρτημένης πράξης και την ακολουθεί εφεξής. Δεν μπορούν να υπάρχουν δύο ΑΔΑ για μια πράξη και όταν μια πράξη για κάποιο λόγο ακυρώνεται ο ΑΔΑ της παραμένει ανενεργός. [13]



Εικόνα 2.2: Στατιστικά αναρτημένων πράξεων ανά φορέα.

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα



Εικόνα 2.3: Στατιστικά Διαύγειας.

Τα στατιστικά είναι αναρτημένα στο διαδικτυακό τόπο: <https://diavgeia.gov.gr> / και ανανεώνονται συνεχώς.

Καθένας από τους παρακάτω έχει την υποχρέωση να αναρτά στο διαδίκτυο νόμους, διατάγματα και πράξεις που εκδίδουν:

- ✓ Πρωθυπουργός
- ✓ Υπουργικό Συμβούλιο και τα συλλογικά κυβερνητικά όργανα
- ✓ Γενικοί και Ειδικοί Γραμματείς
- ✓ Συντονιστές Αποκεντρωμένων Διοικήσεων και Εκτελεστικοί Γραμματείς Περιφερειών
- ✓ Όργανα διοίκησης νομικών προσώπων δημοσίου δικαίου (Ν.Π.Δ.Δ.)
- ✓ Ανεξάρτητες διοικητικές αρχές
- ✓ Νομικό Συμβούλιο του Κράτους
- ✓ Όργανα διοίκησης φορέων του ευρύτερου δημόσιου τομέα
- ✓ Όργανα των φορέων των Οργανισμών Τοπικής Αυτοδιοίκησης πρώτου και δεύτερου βαθμού.

2. Ανάρτηση στο Διαδίκτυο:

Οι πράξεις αναρτώνται στο Διαδίκτυο με μέριμνα του οργάνου που τις εξέδωσε.

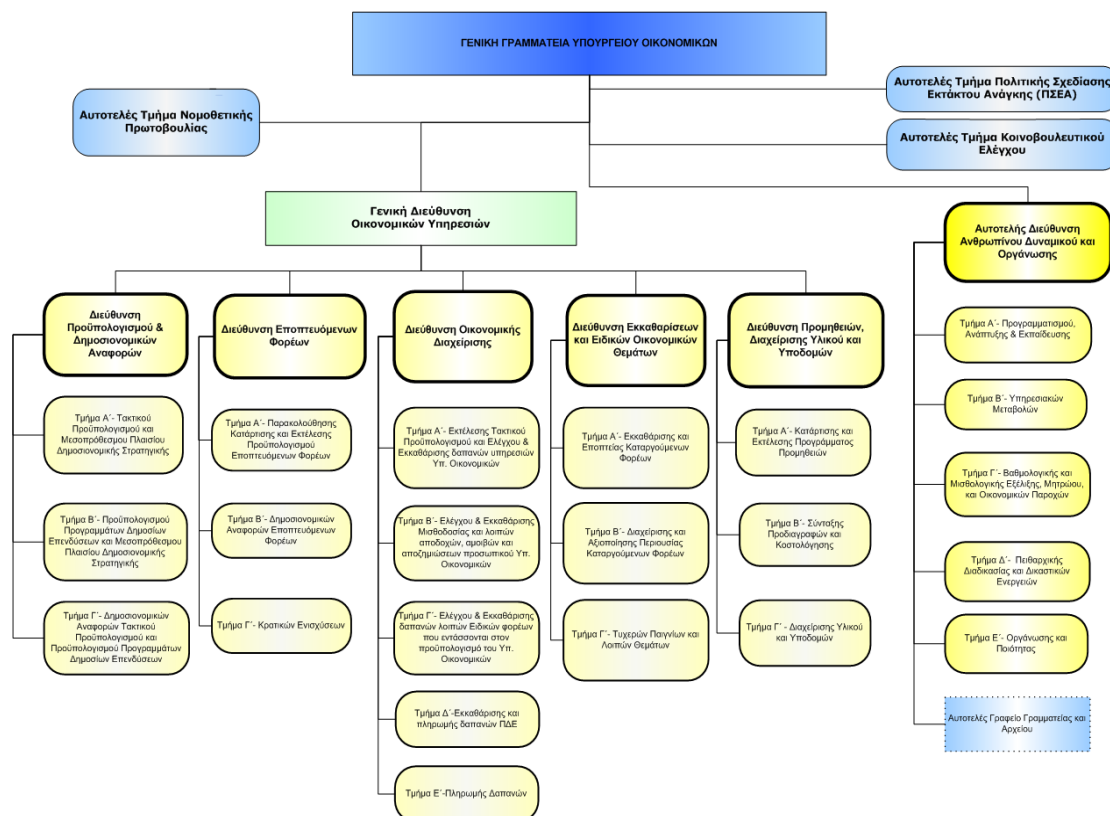
- Η μη ανάρτηση ή η μη έγκαιρη ανάρτηση στο διαδίκτυο των πράξεων συνιστά πειθαρχικό παράπτωμα για το όργανο που την εξέδωσε ή για τον υπάλληλο που έχει την ευθύνη για την ανάρτηση.
- Σε περίπτωση συναρμοδιότητας η πράξη αναρτάται με μέριμνα των συναρμοδίων σε όλους τους αντίστοιχους δικτυακούς τόπους.

3. Προστασία δεδομένων προσωπικού χαρακτήρα και απόρρητα

Δεν αναρτώνται πράξεις, στις οποίες περιλαμβάνονται οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα και δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Ανάρτηση οργανογράμματος και στοιχείων υπηρετούντων

Κάθε υπηρεσία ή φορέας του Δημοσίου οφείλουν να αναρτούν στον δικτυακό τόπο τους το οργανόγραμμα και τη διάρθρωση των υπηρεσιών και μονάδων, την περιγραφή των αρμοδιοτήτων και των οργανικών θέσεων, καθώς και τα ονόματα, τις ιδιότητες και τα πρόσφορα στοιχεία επικοινωνίας των υπηρετούντων σε αυτούς τους φορείς με οποιαδήποτε μορφή ή σχέση εργασίας και απασχόλησης.



Εικόνα 2.4: Οργανόγραμμα Γ. Γραμματείας Υπουργείου Οικονομικών. [14]

Δημοσίευση εκτέλεσης Προϋπολογισμών

Κάθε δημόσιος φορέας θα πρέπει εντός δέκα ημερών μετά από το πέρας κάθε ημερολογιακού μήνα να δημοσιεύει στην ιστοσελίδα του και στο «Πρόγραμμα Διαύγεια» στοιχεία για την εκτέλεση των προϋπολογισμών του. Τα στοιχεία θα περιλαμβάνουν: Αναλυτικό Λογαριασμό Εσόδων και Αναλυτικό Λογαριασμό Εξόδων.

3.2.8 Υποδομές

Τι είναι το υπολογιστικό νέφος;

Σύμφωνα με το «Εθνικό Πληροφοριακό Σύστημα Έρευνας και Τεχνολογίας (ΕΠΣΕΤ)» υπολογιστικό Νέφος ονομάζεται η κατ' αίτηση διαδικτυακή κεντρική διάθεση υπολογιστικών πόρων (όπως δίκτυο, εξυπηρετητές, εφαρμογές και υπηρεσίες) με υψηλή ευελιξία, ελάχιστη προσπάθεια από τον χρήστη και υψηλή αυτοματοποίηση.

Στο Υπολογιστικό Νέφος η αποθήκευση, η επεξεργασία και η χρήση δεδομένων, λογισμικού και υπηρεσιών γίνεται διαδικτυακά, μέσω απομακρυσμένων υπολογιστών σε κεντρικά Datacenter. Υπηρεσίες όπως η κατ' αίτηση παροχή εικονικών μηχανών, το διαδικτυακό ηλεκτρονικό ταχυδρομείο ή τα κοινωνικά δίκτυα συχνά βασίζονται στην τεχνολογία του Υπολογιστικού Νέφους. Οι χρήστες εξοικονομούν πόρους από την αγορά και συντήρηση λογισμικού, τη συντήρηση ακριβών εξυπηρετητών και εγκαταστάσεων αποθήκευσης δεδομένων. [15]

Μορφές υπολογιστικού νέφους

Software-as-a-Service (SaaS):

Αντί να εγκατασταθεί λογισμικό στον εξοπλισμό κάποιου φορέα, το λογισμικό εγκαθίστανται στο cloud χρησιμοποιείται μέσω του διαδικτύου

Platform-as-a-Service (PaaS):

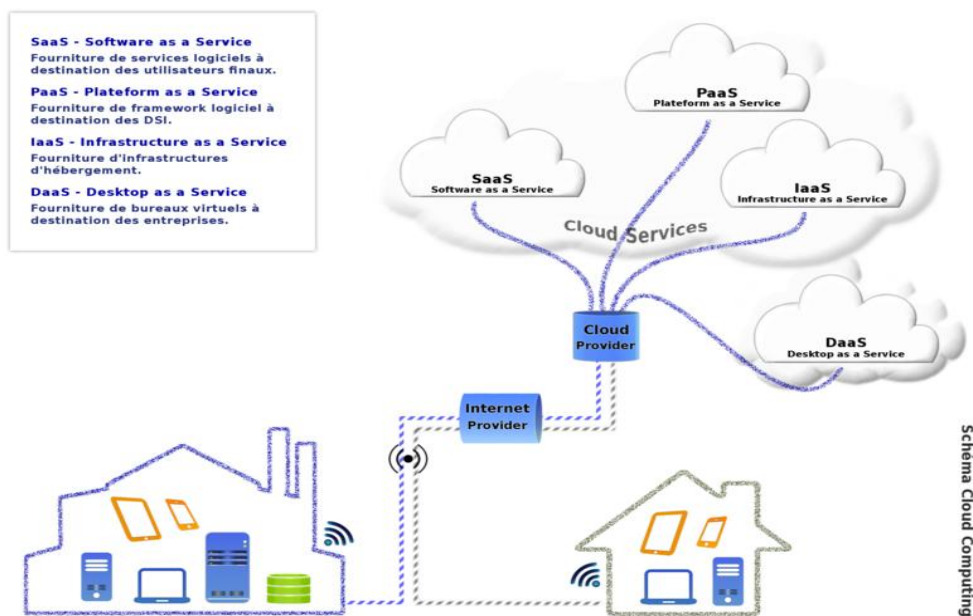
Ο πελάτης χρησιμοποιεί τις πλατφόρμες και τα εργαλεία τους χωρίς να είναι απαραίτητη η αγορά για τις απαιτούμενες άδειες χρήσης.

Infrastructure-as-a-Service (IaaS):

Γίνεται χρήση εικονικών συστημάτων στο Cloud χωρίς να απαιτείται η χρήση server, διακομιστών ή συσκευών αποθήκευσης. Η σύνδεση στα συστήματα γίνεται με τρόπο που εξασφαλίζει τον έλεγχο ταυτότητας με χρήση κωδικού πρόσβασης χρήστη.

Desktop-as-a-Service (DaaS):

Η υπηρεσία επιφάνεια εργασίας προσφέρει μια υποδομή εικονικής επιφάνειας εργασίας (Virtual Desktop Infrastructure – VDI) που φιλοξενείται από έναν πάροχο λύσεων λογισμικού cloud και βασίζεται συνήθως σε ένα μοντέλο μηνιαίας συνδρομής. Το DaaS χρησιμοποιεί μια αρχιτεκτονική πολλαπλών μισθώσεων, πράγμα που σημαίνει ότι μια μοναδική εμφάνιση μιας εφαρμογής εξυπηρετείται σε πολλούς χρήστες, που αναφέρονται ως “ενοικιαστές”. Το τελικό αποτέλεσμα αυτής της υποδομής είναι ότι οι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα και τις εφαρμογές τους από σχεδόν οποιαδήποτε συσκευή, οπουδήποτε. [16]



Εικόνα 2.5: Cloud Computing

Κάθε νέο πληροφοριακό σύστημα των φορέων του δημοσίου τομέα πρέπει να φιλοξενείται σε ένα από τα παρακάτω υπολογιστικά νέφη, με σκοπό την παροχή ψηφιακών δημοσίων υπηρεσιών ανάλογα με τον τομέα που εξυπηρετεί:

1) Κυβερνητικό Νέφος Δημόσιου Τομέα(G-Cloud): Αφορά όλες τις κεντρικές ηλεκτρονικές εφαρμογές και τα κεντρικά πληροφοριακά συστήματα που διατηρούν όλα τα υπουργεία, εκτός των υπουργείων Υγείας και Παιδείας και Θρησκευμάτων, τα Ν.Π.Δ.Δ. εκτός των Νοσοκομείων και των Κέντρων Υγείας, οι ανεξάρτητες αρχές και η Κοινωνία της Πληροφορίας (ΚτΠ ΑΕ).

2) Κυβερνητικό Νέφος Τομέα Υγείας (H-Cloud): Αφορά όλες τις ηλεκτρονικές εφαρμογές και τα κεντρικά πληροφοριακά συστήματα του Υπουργείου Υγείας, των Νοσοκομείων και των Κέντρων Υγείας, που αφορούν σε επεξεργασία ιατρικών δεδομένων, καθώς και σε συναλλαγές ιατρικής φύσεως πολιτών.

3) Κυβερνητικό Νέφος Τομέα Έρευνας και Εκπαίδευσης (RE-Cloud): Αφορά όλες τις ηλεκτρονικές εφαρμογές και τα κεντρικά πληροφοριακά συστήματα του υπουργείου Παιδείας και Θρησκευμάτων, των εποπτευόμενων φορέων του, καθώς και οι εφαρμογές και υπηρεσίες που προσφέρονται από το υπουργείο Παιδείας και Θρησκευμάτων στην εκπαιδευτική και ερευνητική κοινότητα. [9]

3.2.9 Μητρώα ψηφιακής διακυβέρνησης

Στη Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (Γ.Γ.Π.Σ.Δ.Δ.) δημιουργείται και τηρείται Μητρώο Διαλειτουργικότητας με σκοπό τη διαρκή καταγραφή και αποτύπωση των διαδικτυακών υπηρεσιών (web services) φορέων του δημοσίου τομέα. Κάθε φορέας δημοσίου τομέα που αναπτύσσει διαδικτυακές υπηρεσίες στο πλαίσιο των αρμοδιοτήτων τους, έχει την υποχρέωση να:

- Προβαίνει στην καταχώριση στο Μητρώο Διαλειτουργικότητας κάθε διαδικτυακής υπηρεσίας που παρέχουν από την ένταξή τους σε παραγωγική λειτουργία.

- Καταχώριση κάθε μεταγενέστερης μεταβολής τους

Σε περίπτωση παράλειψης της καταχώρισης κινείται η προβλεπόμενη πειθαρχική διαδικασία.

3.2.10 Έκτακτα μέτρα λόγω της πανδημίας COVID-19

Για επιτακτικούς λόγους προστασίας της δημόσιας υγείας έναντι του κορωνοϊού COVID-19, τέθηκαν σε ισχύ για την Περιφέρεια Αττικής μέτρα που αφορούν την μείωση κινητικότητας στα Μέσα Μαζικής Μεταφοράς αλλά και στους χώρους εργασίας.

Έτσι κάθε εργοδότης ή επιχείρηση καλείται να εφαρμόσει κατάλογο προσωπικού που αφορά αριθμό μεγαλύτερο του 40% του συνολικού εργατικού δυναμικού και οι οποίοι θα προσφέρουν τις υπηρεσίες τους εξ' αποστάσεως.

Πρόκειται για ένα μέτρο που μελλοντικά ίσως αφήσει το στίγμα του και στην δημόσια διοίκηση, καθώς με τον τρόπο αυτό μειώνεται η κινητικότητα των πολιτών προς τους δημόσιους φορείς και την θέση του λαμβάνει η ηλεκτρονική εξυπηρέτηση τους για ζητήματα που αφορούν τις συναλλαγές τους με το κράτος.

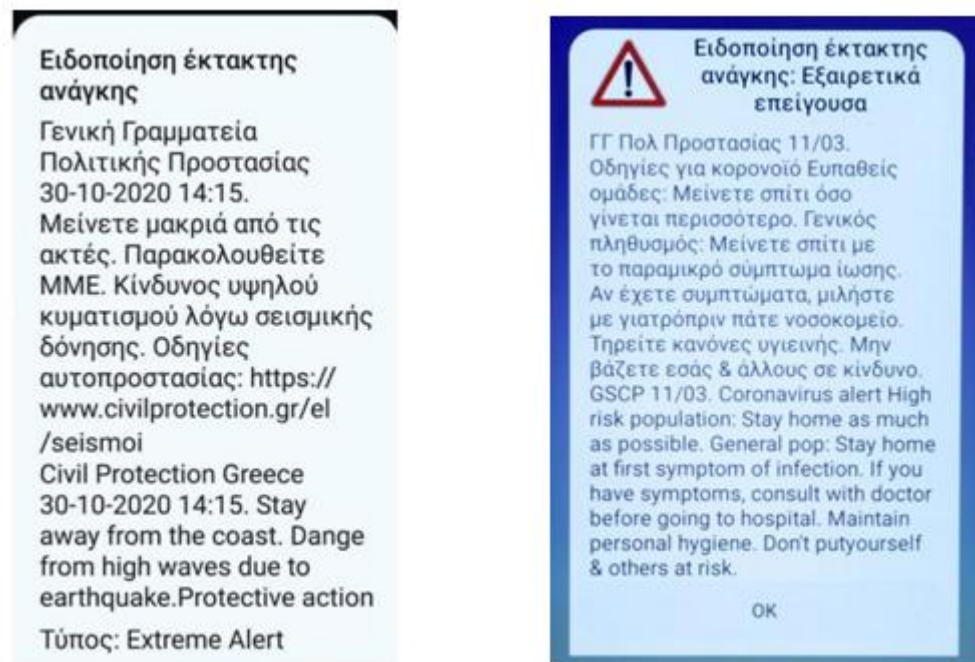
3.2.11 Ηλεκτρονικές Επικοινωνίες

Η οδηγία (ΕΕ) 2018/1972 θεσπίζει ένα σύνολο κανόνων για τη ρύθμιση των δικτύων ηλεκτρονικών επικοινωνιών (τηλεπικοινωνιών) και των υπηρεσιών τηλεπικοινωνίας.

Σκοπός της συγκεκριμένης οδηγίας είναι η αξιοποίηση των δικτύων υψηλής χωρητικότητας για όλους τους πολίτες που διαμένουν στην ΕΕ, ενισχύοντας τον αποτελεσματικό και υγιή ανταγωνισμό μεταξύ των επιχειρήσεων. Εξασφαλίζει ότι ο χρήστης θα έχει την μέγιστη ασφάλεια τόσο στα δίκτυα όσο και στις υπηρεσίες, αφού έχει διασφαλίσει για αυτούς την προστασία τους ως καταναλωτές. Στόχος της οδηγίας είναι η αύξηση των επενδύσεων σε δίκτυα 5G.

Σημαντικό επίσης είναι ότι οι χώρες της ΕΕ καλούνται δημιουργήσουν σύστημα δημόσιας προειδοποίησης για την αποστολή ειδοποιήσεων στους πολίτες στα κινητά τους τηλέφωνα σε περίπτωση φυσικής καταστροφής ή άλλης σοβαρής έκτακτης ανάγκης στην περιοχή τους.

Τέτοιου είδους μηνύματα έχουν σταλεί στην Ελλάδα κατά την διάρκεια της πανδημίας Covid-19 όσο και στον σεισμό που έπληξε το νησί της Σάμου στις 30/10/2020 ή άλλες φυσικές καταστροφές.



Εικόνα 2.6: Μηνύματα στη Ελληνική επικράτεια από το σύστημα δημόσιας
προειδοποίησης.

4. Γενικός Κανονισμός για την Προστασία Δεδομένων

4.1 Εισαγωγή

Ο Ευρωπαϊκός Κανονισμός 679/2016 General Data Protection Regulation (GDPR) της 27.04.2016 αφορά τη διαμόρφωση ενός ενιαίου νομοθετικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, χωρίς να απαιτείται ειδική προσαρμογή της εθνικής νομοθεσίας.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων θεσπίζει τους κανόνες εκείνους που αφορούν την προστασία των φυσικών προσώπων όσο αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Ο παρών Κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης. [17]

4.2 Γενικές Διατάξεις

Τι θα πει «επεξεργασία» των προσωπικών δεδομένων:

Επεξεργασία, σύμφωνα με τον Γενικό Κανονισμό, είναι κάθε ενέργεια που σχετίζεται με προσωπικά δεδομένα όπως για παράδειγμα η συλλογή, η καταγραφή, η αποθήκευση, η διόρθωση, η ενημέρωση, η τροποποίηση, η χρήση, η μεταβίβαση, η διαγραφή, ακόμη και η καταστροφή τους. Η έννοια της «επεξεργασίας» αφορά τόσο τη χρήση αυτοματοποιημένων ή ψηφιακών μέσων, όσο και τη χρήση αναλογικών ή συμβατικών μέσων, όπως η χειρόγραφη καταγραφή, ή τήρηση έντυπου αρχείου. Ο Γενικός Κανονισμός θεσπίζει πολύ αυστηρές προϋποθέσεις και διαδικασίες προκειμένου να είναι νόμιμη η επεξεργασία, ενώ σε αντίθετη περίπτωση, θεσπίζει πολύ αυστηρά πρόστιμα αλλά και υποχρέωση αποζημίωσης των προσώπων στα οποία αναφέρονται τα προσωπικά δεδομένα (υποκείμενα των δεδομένων).

Νομική βάση επεξεργασίας δεδομένων προσωπικού χαρακτήρα από δημόσιους φορείς.

Οι δημόσιοι φορείς επιτρέπεται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

4.3 Υπεύθυνος Προστασίας Δεδομένων (DPO) και διαδικασίες επεξεργασίας δεδομένων

Ο ορισμός Υπεύθυνου Προστασίας Προσωπικών Δεδομένων είναι υποχρεωτικός για όλους τους δημόσιους φορείς, καθώς επίσης και για άλλους οργανισμούς που από την κύρια δραστηριότητά τους απαιτείται η συστηματική παρακολούθηση φυσικών προσώπων σε μεγάλη κλίμακα ή η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.

Ο ρόλος του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων είναι συμβουλευτικός και υποστηρικτικός, δεδομένου ότι ενημερώνει, συμβουλεύει και παρακολουθεί τον φορέα αναφορικά με τη συμμόρφωση αυτής με τον Κανονισμό, με σκοπό την ελαχιστοποίηση του κινδύνου παραβίασης. Επίσης ενεργεί ως σημείο επικοινωνίας με την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία. [17]

Κάθε δημόσιος φορέας θα πρέπει να ορίζει υπεύθυνο προστασίας δεδομένων (ΥΠΔ) με βάση τα παρακάτω κριτήρια:

- Επιλογή με βάση τα επαγγελματικά του προσόντα. Σημαντικό ο υπεύθυνος να έχει εξειδικευμένες γνώσεις στις πρακτικές περί προστασίας δεδομένων προσωπικού χαρακτήρα.
- Μπορεί να είναι υπάλληλος δημόσιου φορέα ή εργαζόμενος με σύμβαση παροχής υπηρεσιών.

Μετά τον ορισμό του ο φορέας δημοσιοποιεί (εφόσον επιτρέπεται) τα στοιχεία του στην Αρχή. Ο φορέας φροντίζει ότι ο ΥΠΔ εκτελεί τα καθήκοντα του με σωστό τρόπο, δίνει αναφορά στο ανώτατο ιεραρχικά προϊστάμενο όργανο και δεν λαμβάνει εντολές από μη αρμόδια άτομα.

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

Ο υπεύθυνος προστασίας δεδομένων σύμφωνα με την νομοθεσία έχει τα ακόλουθα καθήκοντα τα οποία πρέπει να ακολουθεί πιστά:

Είναι υποχρεωμένος να ενημερώνει τον εκάστοτε φορέα και τους εργαζόμενους που απασχολούνται σε αυτόν για τις υποχρεώσεις που έχουν κατά την διάρκεια της επεξεργασίας των δεδομένων. Είναι ο αρμόδιος για την παρακολούθηση των διατάξεων δίνοντας ταυτόχρονα συμβουλές στους εργαζόμενους που ασχολούνται με την επεξεργασία.

Είναι λογικό ότι η επεξεργασία των δεδομένων δεν είναι πάντα η ίδια και διαφέρει ανάλογα με το άτομο του οποίου τα στοιχεία πρέπει να επεξεργαστούν. Έτσι εφόσον πρέπει να εφαρμοστεί επεξεργασία δεδομένων που αφορούν ανήλικο άτομο τότε πρέπει:

1. Είτε το άτομο να έχει συμπληρώσει το 15ο έτος της ηλικίας του και παρέχει τη συγκατάθεσή του.
2. Εάν ο ανήλικος είναι κάτω των 15 ετών η επεξεργασία είναι σύννομη μόνο μετά την παροχή συγκατάθεσης του νομίμου αντιπροσώπου του.

Σε κάθε περίπτωση ο υπεύθυνος καλείται να έχει πιστοποιήσει την ακριβή ηλικία του τέκνου και να υπάρχει γραπτή δήλωση ότι επιτρέπεται να προχωρήσει στην επεξεργασία.

Επίσης η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα από δημόσιους φορείς επιτρέπεται, εφόσον είναι απαραίτητη:

1. Για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας.
2. Για την αποτροπή σημαντικής απειλής για την εθνική ασφάλεια ή τη δημόσια ασφάλεια.
3. Για τη λήψη ανθρωπιστικών μέτρων.

Υπάρχει και η κατηγορία στην οποία μπορεί να γίνει επεξεργασία δεδομένων για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί, και αυτή αφορά άτομα/οντότητες για τις οποίες:

- Υπάρχουν βάσιμες υποψίες ότι οι πληροφορίες που παρέχονται από το άτομο είναι εσφαλμένες.
- Είναι απαραίτητο για την διασφάλιση της εθνικής και δημόσιας ασφάλειας.
- Παρέχονται πληροφορίες για την δίωξη ποινικών αδικημάτων
- Βοηθούν στην αποτροπή βλάβης προς τρίτο πρόσωπο.

Στην περίπτωση αυτή είναι σημαντικό να υπάρχουν βάσιμα αποδεικτικά στοιχεία που αποδεικνύουν τον λόγο που θα προχωρήσουμε στις συγκεκριμένες ενέργειες.

Διαβίβαση δεδομένων προσωπικού χαρακτήρα από δημόσιους φορείς

Η διαβίβαση δεδομένων μεταξύ φορέων του δημόσιου τομέα επιτρέπεται εφόσον είναι απαραίτητο για την εκτέλεση καθηκόντων. Ο τρίτος στον οποίο διαβιβάζονται τα δεδομένα επεξεργάζεται αυτά μόνο για τον σκοπό για τον οποίο διαβιβάστηκαν.

Επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των σχέσεων απασχόλησης.



Η χρήση κλειστού κυκλώματος καταγραφής εντός χώρων εργασίας επιτρέπεται μόνο για την προστασία προσώπων και αγαθών. Σε καμία περίπτωση τα δεδομένα καταγραφής δεν χρησιμοποιούνται για αξιολόγηση των εργαζομένων. Εφόσον ο χώρος εργασίας καταγράφεται οι εργαζόμενοι πρέπει να ενημερώνονται εγγράφως.

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

Η επεξεργασία δεδομένων για επιστημονικούς ή ερευνητικούς σκοπούς επιτρέπεται, εφόσον ο υπεύθυνος επεξεργασίας έχει λάβει τα ακόλουθα μέτρα:

- α) περιορισμό πρόσβασης των υπεύθυνων επεξεργασίας και εκτελούντων την επεξεργασία.
- β) ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα.

Με τον όρο ψευδωνυμοποίηση εννοούμε : την επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών. [18]

- γ) κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα.

Επεξεργασίας δεδομένων και εθνική ασφάλεια

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα του προσωπικού της ΕΥΠ που πραγματοποιείται από δημόσιους και ιδιωτικούς φορείς στο πλαίσιο των καθηκόντων τους ή των αρμοδιοτήτων τους διενεργείται από ειδικά εξουσιοδοτημένους για αυτό υπαλλήλους, για τα ονόματα των οποίων ενημερώνεται η ΕΥΠ.

Η Αρχή ότι δεν έχει αρμοδιότητα ελέγχου των πράξεων επεξεργασίας που διενεργούνται για δραστηριότητες που αφορούν την εθνική ασφάλεια εφόσον συντρέχουν σωρευτικά οι ακόλουθες δυο προϋποθέσεις:

- α) πρόκειται για πράξεις επεξεργασίας διαβαθμισμένων δεδομένων προσωπικού χαρακτήρα, και ορθότερα, πληροφοριών καταχωρημένων σε συστήματα αρχειοθέτησης που έχουν αρμοδίως διαβαθμισθεί και οι οποίες συνιστούν δεδομένα προσωπικού χαρακτήρα.
- β) πρόκειται για πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διενεργούνται για δραστηριότητες που αφορούν την εθνική ασφάλεια. [19]

4.4 Δικαιώματα του υποκειμένου των δεδομένων

Ο υπεύθυνος επεξεργασίας παρέχει γενικές και ευχερώς προσβάσιμες στο κοινό πληροφορίες σε απλή και κατανοητή γλώσσα και μέσω του διαδικτυακού τόπου της δημόσιας αρχής αναφορικά με:

- α) τους σκοπούς της επεξεργασίας,
- β) το δικαίωμα του υποκειμένου να ζητήσει από τον υπεύθυνο επεξεργασίας πρόσβαση, διόρθωση, διαγραφή ή περιορισμό της επεξεργασίας,
- γ) την ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας και του ΥΠΔ,
- δ) το δικαίωμα υποβολής καταγγελίας στην Αρχή, και
- ε) τα στοιχεία επικοινωνίας της Αρχής.

Ο υπεύθυνος επεξεργασίας μπορεί να προχωρήσει σε επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνο εφόσον έχει λάβει την συγκατάθεση του υποκειμένου των δεδομένων. Ο καλύτερος τρόπος συγκατάθεσης είναι η γραπτή δήλωση από το άτομο. Στην δήλωση πρέπει να παρουσιάζεται με χρήση απλής και κατανοητής γλώσσας ο λόγος που τα δεδομένα του θα είναι διαθέσιμα προς επεξεργασία. Το υποκείμενο διατηρεί το δικαίωμα να ανακαλέσει την συγκατάθεση για οποιονδήποτε λόγο.

- 1) Δικαίωμα στη διαγραφή των δεδομένων («το δικαίωμα στη λήθη»).

Το δικαίωμα στη λήθη («διαγραφή» στην ορολογία του GDPR) επιτρέπει σε ιδιώτες να απαιτούν τη διαγραφή των προσωπικών τους δεδομένων από τους υπευθύνους επεξεργασίας όταν υπάρχει πρόβλημα με τη νομιμότητα της επεξεργασίας των δεδομένων, ή όταν το υποκείμενο αποσύρει τη συγκατάθεσή του.

- 2) Δικαίωμα ενημέρωσης του υποκειμένου.

Το άτομο του οποίου τα δεδομένα υπόκεινται προς επεξεργασία οφείλει να ενημερώνεται για την νομική βάση της επεξεργασίας, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα του καθώς και τους αποδέκτες των προσωπικών του στοιχείων.

- 3) Δικαίωμα πρόσβασης

Εφόσον ζητηθεί από το υποκείμενο, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το άτομο χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή για τις ακόλουθες πληροφορίες:

- ☐ Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.
- ☐ Τους σκοπούς της επεξεργασίας και τους αποδέκτες.
- ☐ Την εξέλιξη της επεξεργασίας.
- ☐ Τη λογική της αυτοματοποιημένης επεξεργασίας.
- ☐ Την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα.

- 4) Δικαίωμα διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα και περιορισμοί ως προς την επεξεργασία

Εφόσον το άτομο εντοπίσει ανακριβείς ή λανθασμένα δεδομένων έχει το δικαίωμα να ζητήσει την άμεση διόρθωση των στοιχείων αυτών.

Ο υπεύθυνος επεξεργασίας διορθώνει τα συγκεκριμένα δεδομένα μόνο εφόσον μπορεί να διαπιστώσει την ακρίβεια και την ορθότητα τους. Στην περίπτωση που αυτό δεν είναι δυνατό, τότε περιορίζει την επεξεργασία των συγκεκριμένων δεδομένων έως ότου διαπιστωθεί η ορθότητα τους.

Μόλις ο υπεύθυνος επεξεργασίας προχωρήσει στην διόρθωση των δεδομένων προσωπικού χαρακτήρα κοινοποιεί τη διόρθωση στον φορέα από τον οποίο τα έλαβε.

Ο υπεύθυνος επεξεργασίας ενημερώνει εγγράφως το υποκείμενο των δεδομένων για οποιαδήποτε άρνηση διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα ή περιορισμού της επεξεργασίας τους.

4.5 Υποχρεώσεις εκτελούντος την επεξεργασία και υπεύθυνου επεξεργασίας.

Ο υπεύθυνος επεξεργασίας, ακόμα και αν διενεργείται από τρίτο πρόσωπο για λογαριασμό του, πρέπει να μεριμνά προκειμένου να τηρούνται όλοι οι κανονισμοί και οι υποχρεώσεις που προκύπτουν από την παρούσα νομοθεσία και αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ο εκτελών την επεξεργασία ενεργεί μόνο κατ' εντολή και σύμφωνα με τις οδηγίες του υπεύθυνου επεξεργασίας και εγγυάται ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα τηρούν την εμπιστευτικότητα.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να λαμβάνουν τα απαραίτητα μέτρα(τεχνικά και οργανωτικά) που εξασφαλίζουν το μέγιστο επίπεδο ασφαλείας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Τα μέτρα πρέπει να διασφαλίζουν :

a. την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών που σχετίζονται με την επεξεργασία.

b. τη δυνατότητα να αποκατασταθεί έγκαιρα η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα σε περίπτωση φυσικού ή τεχνικού συμβάντος.

c. την απαγόρευση της πρόσβασης μη εξουσιοδοτημένων προσώπων σε εξοπλισμό που χρησιμοποιείται για την επεξεργασία.

d. την αποτροπή της μη εξουσιοδοτημένης εισαγωγής δεδομένων.

e. την αποτροπή της μη εξουσιοδοτημένης ανάγνωσης, αντιγραφής, τροποποίησης ή αφαίρεσης μέσω αποθήκευσης.

f. την εξασφάλιση ότι τα δεδομένα προσωπικού χαρακτήρα προστατεύονται από απώλεια και καταστροφή.

4.5.1 Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην Αρχή

Στην περίπτωση που διαπιστωθεί παραβίαση δεδομένων προσωπικού χαρακτήρα ο υπεύθυνος πρέπει να ενημερώνει την Αρχή εντός εβδομήντα δύο ωρών από τότε που έλαβε γνώση της παραβίασης και να γνωστοποιεί την φύση της παραβίασης, το στοιχείο επικοινωνίας του υπεύθυνου επεξεργασίας, τις συνέπειες της παραβίασης και τα μέτρα που έχουν ληφθεί για την αντιμετώπιση της παραβίασης.

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

Στον επίσημο ιστότοπο της Αρχής Προστασίας Δεδομένων(www.dpa.gr) υπάρχει η διαδικασία «υποβολής γνωστοποίησης περιστατικού παραβίασης στην Αρχή» όπου δίνεται και η αντίστοιχη φόρμα προς συμπλήρωση, όπως φαίνεται παρακάτω:

A	B	C	D	E	F	G
Φόρμα υποβολής γνωστοποίησης περιστατικού παραβίασης προσωπικών δεδομένων						
Σύμφωνα με το άρθρο 63 του ν. 4624/2019						
0. Γενικές Πληροφορίες						Επεξηγηματικά Σχόλια
Είδος γνωστοποίησης (Αρχική/Συμπληρωματική/Πλήρης)						1) Αρχική , αν πρόκειται για υποβολή κάποιων πρώτων διαθέσιμων στοιχείων, ενώ εκκρεμούν κάποια γιατί ακόμη δεν είναι διαθέσιμα 2) Συμπληρωματική , αν παρέχονται συμπληρωματικά στοιχεία επί προηγούμενης υποβληθείσας ως αρχικής 3) Πλήρης , αν παρέχονται όλες οι πληροφορίες επί του περιστατικού
Ημερομηνία υποβολής προηγούμενης γνωστοποίησης για το ίδιο περιστατικό						Συμπληρώνεται <u>εφόσον</u> η παρούσα γνωστοποίηση είναι συμπληρωματική
1. Ποιος υποβάλλει την παρούσα γνωστοποίηση περιστατικού (υπεύθυνος επεξεργασίας)						
1.1 Επωνυμία υπεύθυνου επεξεργασίας						
Όνομασία Αρχής						
Εποπτεύον Υπουργείο						
ΑΦΜ						
Διεύθυνση επικοινωνίας						

Εικόνα 3.1: Φόρμα υποβολής γνωστοποίησης

Εφόσον ενημερωθεί η Αρχή, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμέσως στο υποκείμενο των δεδομένων το περιστατικό της παραβίασης και τον ενημερώνει για την κατάσταση των δεδομένων του, των κινδύνων που υπάρχουν από την συγκεκριμένη ενέργεια και τα μέτρα που έχουν ληφθεί προκειμένου να διασφαλιστεί η ιδιωτικότητα και τα δεδομένα του.

Ο υπεύθυνος επεξεργασίας πρέπει να τηρεί αρχείο για όλες τις κατηγορίες δραστηριοτήτων επεξεργασίας. Το αρχείο πρέπει να περιλαμβάνει τα ακόλουθα:

- i. το ονοματεπώνυμο ή την επωνυμία και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας.
- ii. τον σκοπό της επεξεργασίας.
- iii. τους αποδέκτες στους οποίους θα γνωστοποιηθούν τα δεδομένα.
- iv. κατηγορίες δεδομένων.
- v. νομική βάση της επεξεργασίας.
- vi. το χρονικό διάστημα στο οποίο πρέπει να γίνει διαγραφή δεδομένων.

4.5.2 Προστασία δεδομένων από τον σχεδιασμό και εξ' ορισμού

Ο υπεύθυνος επεξεργασίας, έχοντας ως παράμετρο την κατάσταση της τεχνολογίας και τους σκοπούς της επεξεργασίας, λαμβάνει τα κατάλληλα μέτρα για την εφαρμογή των αρχών προστασίας των δεδομένων προσωπικού χαρακτήρα, όπως η ελαχιστοποίηση των δεδομένων ώστε να διασφαλίζεται η συμμόρφωση με τις νομικές απαιτήσεις και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων.

Τα δεδομένα Προσωπικού Χαρακτήρα καθίστανται ανώνυμα ή προχωρούν στην ψευδωνυμοποίηση τους όσο το δυνατόν ταχύτερα σύμφωνα με τον σκοπό της επεξεργασίας. Σκοπός των ενεργειών είναι η διασφάλιση ότι τα δεδομένα δεν μπορούν να προσπελαστούν με αυτοματοποιημένα μέσα.

Ο υπεύθυνος επεξεργασίας εξασφαλίζει, στο μέγιστο δυνατό, τα κατάλληλα μέτρα που διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα τα οποία δεν είναι πλέον επικαιροποιημένα δεν διατίθενται προς επεξεργασία ούτε διαβιβάζονται. Πριν την οποιαδήποτε ενέργεια προτείνεται η επαλήθευση όσο το δυνατό περισσότερων στοιχείων που αφορούν την ποιότητα των δεδομένων. Εφόσον είναι δυνατό, πρέπει να περιλαμβάνονται όλες οι πληροφορίες που αποδεικνύουν την ορθότητα των δεδομένων και τον βαθμό επικαιροποίησής τους.

Κατά την διαδικασία διόρθωσης και διαγραφής δεδομένων προσωπικού χαρακτήρα Ο υπεύθυνος επεξεργασίας διορθώνει ανακριβή δεδομένα προσωπικού χαρακτήρα είτε προχωράει στην διαγραφή των δεδομένων προσωπικού χαρακτήρα εάν η επεξεργασία τους είναι παράνομη.

4.6 Εκτίμηση Αντικτύπου- Data Protection Impact Assesment (ΕΑΠΔ - DPIA).

Κάθε οργανισμός θα πρέπει να διενεργεί μελέτη εκτίμησης επιπτώσεων στην οποία θα λαμβάνονται υπόψη και θα αξιολογούνται όλα τα πιθανά ενδεχόμενα για τυχόν κινδύνους που μπορεί να προκύψουν. Με βάση αυτά τα ενδεχόμενα αξιολογούνται οι συνέπειες για τα δεδομένα προσωπικού χαρακτήρα που διαχειρίζεται ο εκάστοτε φορέας και λαμβάνονται τα απαιτούμενα μέτρα για τον περιορισμό τους.

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

Για να αξιολογηθεί το επίπεδο κινδύνου, πρέπει να εξεταστεί τόσο η πιθανότητα όσο και η σοβαρότητα των επιπτώσεων στα άτομα. Ο βαθμός του κινδύνου ανά περίπτωση γίνεται με την αξιολόγηση κριτηρίων και θεωρείται υψηλός εφόσον διενεργείται αυτοματοποιημένη επεξεργασία, με βάση την οποία γίνεται συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών φυσικών προσώπων (περιλαμβανομένης της κατάρτισης προφίλ) και στην οποία λαμβάνονται αποφάσεις που παράγουν έννομα ή σημαντικά αποτελέσματα για φυσικά πρόσωπα. Επίσης όταν εκτελείται σε μεγάλη κλίμακα επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων ή προσωπικών δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα. Τέλος όταν διενεργείται συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Στο «ΦΕΚ Β΄ 1622/10-5-2019» δημοσιεύτηκε ο κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με τον οποίο τα κριτήρια για την διενέργεια ΕΑΠΔ ομαδοποιούνται στις παρακάτω τρεις κατηγορίες:

- ✓ 1η κατηγορία: με βάση τα είδη και τους σκοπούς επεξεργασίας.
- ✓ 2η κατηγορία: με βάση το είδος των δεδομένων και/ή τις κατηγορίες των υποκειμένων.
- ✓ 3η κατηγορία: με βάση τα πρόσθετα χαρακτηριστικά και/ή τα χρησιμοποιούμενα μέσα της επεξεργασίας.

5. Εργαλείο Αξιολόγησης

Όνομα του εργαλείου:

«Εργαλείο Αξιολόγησης Συμμόρφωσης με τις νομοθεσίες της Ηλεκτρονικής Διακυβέρνησης και την Ασφάλεια Προσωπικών Δεδομένων»

Σκοπός του εργαλείου

Είναι φανερό ότι η Ηλεκτρονική Διακυβέρνηση ενός κράτους ωφελεί τόσο τους πολίτες, και γενικότερα τις οντότητες, που καθημερινά έρχονται σε διάφορες συναλλαγές με τους κρατικούς φορείς όσο και το ίδιο ο κράτος. Κάθε μορφή συναλλαγής διεκπεραιώνεται γρηγορότερα προσφέροντας στους πολίτες ικανοποίηση, και από την άλλη το κράτος σπαταλάει λιγότερους πόρους. Ωστόσο προκειμένου οι συναλλαγές να γίνονται με ασφάλεια είναι σημαντικό να εξασφαλίζεται η προστασία των προσωπικών δεδομένων των πολιτών.

Η ανάγκη για την συμμόρφωση με τις νομοθεσίες, μας οδήγησε στην κατασκευή ενός εργαλείου που θα έχει ως στόχο τον έλεγχο των δημόσιων φορέων.

Το εργαλείο αξιολόγησης αφορά φορείς του δημόσιου τομέα και σκοπός του είναι ο έλεγχος συμμόρφωσης με τον νόμο 4727/2020 που αφορά την Ηλεκτρονική Διακυβέρνηση και τον Γενικό Κανονισμό Προστασίας Δεδομένων (Νόμος 4624/2019). Με την χρήση του συγκεκριμένου εργαλείου κάθε δημόσιος φορέας είναι σε θέση να γνωρίζει το μέτρο τήρησης των σημαντικότερων διατάξεων του κάθε νόμου προκειμένου η ηλεκτρονική διακυβέρνηση να γίνεται με ασφάλεια χωρίς να υπάρχει κίνδυνος για τα δεδομένα που επεξεργάζεται ο δημόσιος τομέας.

5.1 Δημιουργία Ερωτήσεων Εργαλείου

Στους πίνακες που ακολουθούν αναφέρονται τα άρθρα για κάθε έναν από τους νόμους που αφορούν σημαντικές διατάξεις. Τα “τσεκαρισμένα” άρθρα είναι όλα εκείνα που βρίσκονται και εξετάζονται στο εργαλείο αξιολόγησης. Η επιλογή των ερωτήσεων με βάση τα άρθρα έγινε με γνώμονα τα μέτρα που καλείται να πάρει ο εκάστοτε φορέας που εφαρμόζει μέσα ηλεκτρονικής διακυβέρνησης σε συνδυασμό με την προστασία των προσωπικών δεδομένων. Προφανώς δεν εξετάζονται άρθρα που αναφέρονται στην πλευρά των πολιτών- οντοτήτων που προχωρούν σε συναλλαγές με το κράτος. Κύριο μέλημα του εργαλείου είναι η εξέταση βασικών άρθρων των δύο νομοθεσιών σε σημαντικές λειτουργίες και μέτρα που θα εξασφαλίζουν την μέγιστη δυνατή συμμόρφωση.

Νόμος 4727/2020

Άρθρο 11	Προσωπικός Αριθμός	✓
Άρθρο 13	Έκδοση Ηλεκτρονικών Δημοσίων Εγγράφων	✓
Άρθρο 15	Ηλεκτρονικά ιδιωτικά έγγραφα	
Άρθρο 17	Ηλεκτρονική διακίνηση δημοσίων εγγράφων εντός του ίδιου φορέα	✓
Άρθρο 18	Ηλεκτρονική διακίνηση δημοσίων εγγράφων μεταξύ δημοσίων φορέων	✓
Άρθρο 19	Ηλεκτρονικό πρωτόκολλο	✓
Άρθρο 20	Ηλεκτρονική αρχειοθέτηση	✓
Άρθρο 21	Στατιστική επεξεργασία δεδομένων	✓
Άρθρο 22	Παροχή ψηφιακών δημόσιων υπηρεσιών	

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας
Δεδομένων στην Ελλάδα

Άρθρο 24	Τρόποι αυθεντικοποίησης για χρήση υπηρεσιών μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης	
Άρθρο 25	Ταυτοποίηση για την έκδοση διαπιστευτηρίων	✓
Άρθρο 27	Έκδοση εγγράφων μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης	
Άρθρο 30	Προσδιορισμός χρόνου παραλαβής και υπολογισμός προθεσμιών κατάθεσης	
Άρθρο 32	Ηλεκτρονικές πληρωμές	✓
Άρθρο 33	Ηλεκτρονική καταβολή οφειλών των δημοσίων φορέων	✓
Άρθρο 34	Επικοινωνία μεταξύ δημοσίων φορέων και φυσικών ή νομικών προσώπων ή νομικών οντοτήτων	✓
Άρθρο 35	Ιστοσελίδες δημοσίων φορέων	✓
Άρθρο 43	Μητρώο Δημοσίων Ιστότοπων και Εφαρμογών	✓
Άρθρο 44	Υποχρέωση δημοσιοποίησης στοιχείων	✓
Άρθρο 45	Υποβολή παρατηρήσεων, αιτημάτων για παροχή πληροφοριών και αναφορών	
Άρθρο 46	Επιμόρφωση υπαλλήλων και ευαισθητοποίηση του κοινού	
Άρθρο 47	Παρακολούθηση και υποβολή εκθέσεων	
Άρθρο 77	Υποχρεώσεις ανάρτησης στο διαδίκτυο	✓
Άρθρο 80	Διαδικασία ανάρτησης στο Διαδίκτυο	
Άρθρο 81	Ανάρτηση οργανογράμματος και στοιχείων υπηρετούντων	✓
Άρθρο 82	Δημοσίευση εκτέλεσης Προϋπολογισμών	✓
Άρθρο 85	Πολιτική υπολογιστικού νέφους	✓
Άρθρο 86	Παροχή ψηφιακών δημοσίων υπηρεσιών μέσω υπολογιστικών υποδομών νέφους	
Άρθρο 87	Κυβερνητικά νέφη	✓

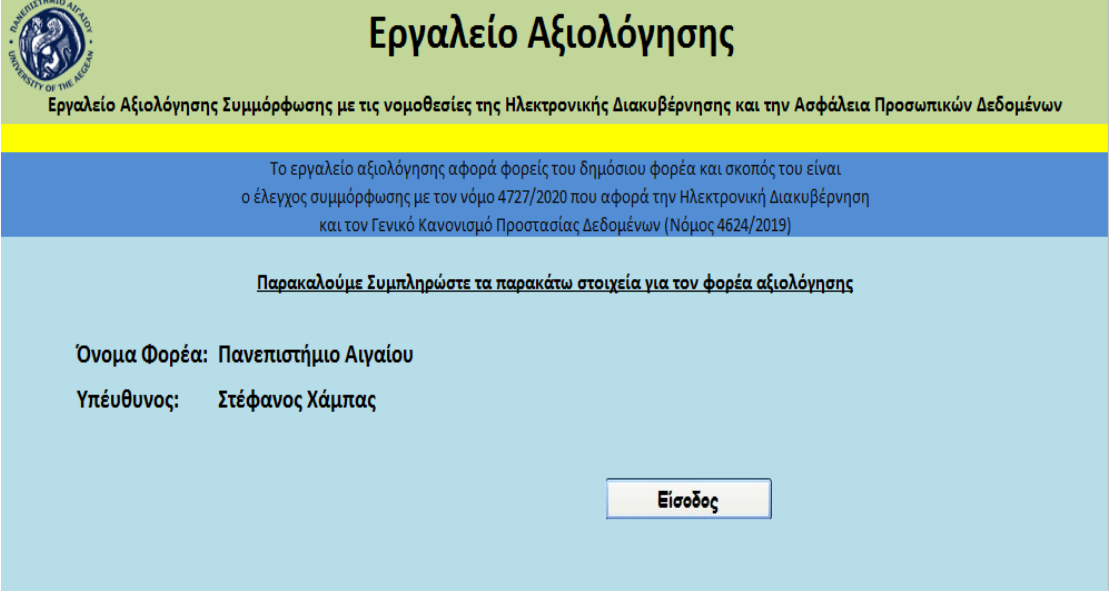
Νόμος 4624/2019

Άρθρο 5	Νομική βάση επεξεργασίας δεδομένων προσωπικού χαρακτήρα από δημόσιους φορείς	✓
Άρθρο 6	Ορισμός του υπεύθυνου προστασίας δεδομένων σε δημόσιους φορείς	✓
Άρθρο 21	Συγκατάθεση ανηλίκου	✓
Άρθρο 22	Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα	✓
Άρθρο 25	Επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς από ιδιωτικούς φορείς	
Άρθρο 27	Επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των σχέσεων απασχόλησης	✓
Άρθρο 28	Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης	

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας
Δεδομένων στην Ελλάδα

Άρθρο 29	Επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον	
Άρθρο 33	Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων/Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων	✓
Άρθρο 36	Διασφάλιση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για λόγους εθνικής ασφάλειας	✓
Άρθρο 37	Διαπίστευση φορέων πιστοποίησης και πιστοποίηση	
Άρθρο 42	Πρόσβαση του κοινού σε έγγραφα	✓
Άρθρο 49	Συγκατάθεση	✓
Άρθρο 50	Επεξεργασία υπό την εποπτεία του υπεύθυνου επεξεργασίας	✓
Άρθρο 52	Αυτοματοποιημένη ατομική λήψη αποφάσεων	
Άρθρο 53	Γενικές πληροφορίες σχετικά με την επεξεργασία δεδομένων	✓
Άρθρο 54	Δικαίωμα ενημέρωσης του υποκειμένου	
Άρθρο 58	Δικαίωμα υποβολής καταγγελίας στην Αρχή	
Άρθρο 59	Δικαιώματα του υποκειμένου των δεδομένων σε ποινικές έρευνες και διαδικασίες	
Άρθρο 62	Ασφάλεια επεξεργασίας	✓
Άρθρο 63	Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην Αρχή	✓
Άρθρο 64	Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων	✓
Άρθρο 65	Εκτίμηση αντίκτυπου της επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα	✓
Άρθρο 75	Γενικές αρχές που διέπουν τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα	✓
Άρθρο 76	Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις	
Άρθρο 78	Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς αποδέκτες εγκατεστημένους σε τρίτες χώρες	

5.2 Οδηγίες Συμπλήρωσης Εργαλείου Αξιολόγησης



Εργαλείο Αξιολόγησης

Εργαλείο Αξιολόγησης Συμμόρφωσης με τις νομοθεσίες της Ηλεκτρονικής Διακυβέρνησης και την Ασφάλεια Προσωπικών Δεδομένων

Το εργαλείο αξιολόγησης αφορά φορείς του δημόσιου φορέα και σκοπός του είναι ο έλεγχος συμμόρφωσης με τον νόμο 4727/2020 που αφορά την Ηλεκτρονική Διακυβέρνηση και τον Γενικό Κανονισμό Προστασίας Δεδομένων (Νόμος 4624/2019)

Παρακαλούμε Συμπληρώστε τα παρακάτω στοιχεία για τον φορέα αξιολόγησης

Όνομα Φορέα: Πανεπιστήμιο Αιγαίου

Υπεύθυνος: Στέφανος Χάμπας

Είσοδος

Εικόνα 5.1: Αρχική Εικόνα Εργαλείου

Περιγραφή Εργαλείου

Στην πρώτη καρτέλα ο χρήστης καλείται να δώσει το όνομα φορέα και τον υπεύθυνο που θα διενεργήσει την αξιολόγηση του φορέα

Στο παράδειγμα: Ως όνομα φορέα δηλώσαμε το «Πανεπιστήμιο Αιγαίου» και ως υπεύθυνο τον «Στέφανο Χάμπας».

Ο εκτελών την αξιολόγηση αφού πατήσει στο κουμπί «Είσοδος» μεταφέρεται στην επόμενη καρτέλα. Στην επόμενη καρτέλα ο χρήστης καλείται να απαντήσει σε συνολικά 49 ερωτήσεις οι οποίες είναι χωρισμένες σε 2 κατηγορίες με βάση την νομοθεσία που ανήκουν.

Πρώτος εξετάζεται ο νόμος 4727/2020 που αφορά την Ηλεκτρονική Διακυβέρνηση με 25 ερωτήσεις:

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

Νομοθεσία	Περιγραφή Άρθρου	Συμμόρφωση
4727/2020	Γίνεται χρήση του προσωπικού αριθμού(Π.Α) ταυτοποίησης	Πλήρως
4727/2020	Προχωράτε στην έκδοση Ηλεκτρονικών Δημόσιων Εγγράφων	Μερικώς
4727/2020	Τήρηση Ηλεκτρονικού πρωτοκόλλου έναντι της χειρόγραφης πρωτοκόλλησης	Στοιχειωδώς
4727/2020	Είναι διαθέσιμη η ηλεκτρονική Αρχειοθέτηση εγγράφων	Στοιχειωδώς
4727/2020	Γίνεται στατιστική επεξεργασία δεδομένων με σκοπό την έκδοση αποτελεσμάτων χρήσης	Πλήρως
4727/2020	Είναι διαθέσιμη η παροχή ψηφιακών δημόσιων εγγράφων για οποιαδήποτε χρήση	Δ/Α
4727/2020	Υπάρχει τρόπος αυτοποίησης για την έκδοση διαπιστευτηρίων	Πλήρως
4727/2020	Γίνεται έκδοση εγγράφων μέσω της Ενιαίας Ψηφιακής Πύλης	Μερικώς
4727/2020	Είναι διαθέσιμη η ηλεκτρονική Διακίνηση Δημόσιων Εγγράφων :	
4727/2020	Εντός του ίδιου φορέα	Μερικώς
4727/2020	Μεταξύ δημοσίων φορέων	Στοιχειωδώς
4727/2020	Δίνεται η δυνατότητα Ηλεκτρονικής πληρωμής οφειλών προς τον φορέα	Πλήρως
4727/2020	Υπάρχει η επιλογή για ηλεκτρονική καταβολή οφειλών των δημοσίων φορέων	Στοιχειωδώς
4727/2020	Για την εξυπηρέτηση πολιτών είναι διαθέσιμος ηλεκτρονικός τρόπος επικοινωνίας	Πλήρως
4727/2020	Διατήρηση διαδικτυακού ιστότοπου για τον φορέα με σκοπό την ενημέρωση	Πλήρως
4727/2020	Υπάρχουν οι κατάλληλες ρυθμίσεις προκειμένου οι υπηρεσίες σας να καταστούν περισσότερο προσβάσιμες στους χρήστες	Πλήρως
4727/2020	Έχετε στην διάθεση σας ηλεκτρονικές βεβαιώσεις που εκδίδονται από έναν πάροχο υπηρεσιών εμπιστοσύνης	Δ/Α
4727/2020	Διάθεση για περαιτέρω χρήση πληροφοριών του δημόσιου τομέα(ανοικτά δεδομένα)	Πλήρως
4727/2020	Προχωράτε στην ανάρτηση όλων των πράξεων στο διαύγεια	Πλήρως
4727/2020	Ανάρτηση οργανογράμματος και στοιχείων υπηρετούντων	Πλήρως
4727/2020	Δημοσίευση εκτέλεσης προπολογισμού	Μερικώς
4727/2020	Χρήση υπολογιστικού νέφους (cloud)	Πλήρως
4727/2020	Προτεραιότητα στην επιλογή υπηρεσιών νέφους από όλους τους δημόσιους φορείς (Cloud First Policy)	Πλήρως
	Έχετε προχωρήσει στα παρακάτω:	
4727/2020	Εγγραφή στο Μητρώο Ψηφιακής Διακυβέρνησης	Πλήρως
4727/2020	Εγγραφή στο Μητρώο δικτυακών τόπων	Στοιχειωδώς

Εικόνα 5.2: Ερωτήσεις που αφορούν το νόμο 4727/2020

Στην συνέχεια εξετάζεται ο νόμος 4624/2019 που αφορά την προστασία των Προσωπικών Δεδομένων με 24 ερωτήσεις:

Νομοθεσία	Περιγραφή Άρθρου	Συμμόρφωση
4624/2019	Έχετε προχωρήσει σε ορισμό υπεύθυνου προστασίας δεδομένων (DPO)	Πλήρως
4624/2019	Γίνεται λήψη συγκατάθεσης γονέα σε περίπτωση επεξεργασίας δεδομένων ανηλίκου κάτω των 15 ετών.	Πλήρως
4624/2019	Χρήση κλειστού κυκλώματος μόνο για την προστασία αγαθών και προσώπων και όχι για αξιολόγηση υπαλλήλων	Πλήρως
4624/2019	Έχετε προχωρήσει στην απαραίτητη μελέτη αντικτύπου σχετικά με την προστασία προσωπικών δεδομένων	Πλήρως
4624/2019	Γίνεται ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων	Πλήρως
4624/2019	Έχει συνταχθεί πολιτική προστασίας προσωπικών δεδομένων	Πλήρως
4624/2019	Διασφάλιση της επεξεργασίας δεδομένων για λόγους εθνικής ασφάλειας	Πλήρως
4624/2019	Υπάρχει νομική βάση για κάθε είδος επεξεργασίας δεδομένων	Στοιχειωδώς
4624/2019	Γραπτή συγκατάθεση του υποκειμένου για της επεξεργασία των δεδομένων του	Πλήρως
4624/2019	Επεξεργασία δεδομένων υπο την εποπτεία του υπεύθυνου επεξεργασίας	Πλήρως
4624/2019	Υπάρχει καταγραφή των απαραίτητων μέτρων για την κάλυψη των κανόνων ασφαλείας	Μερικώς
4624/2019	Προσβάσιμες πληροφορίες στο κοινό μέσω διαδικτυακού τόπου της δημόσιας αρχής	Πλήρως
4624/2019	Γίνεται ενημέρωση του υποκειμένου για την νομική βάση της επεξεργασίας των δεδομένων	Μερικώς
4624/2020	Εφόσον ζητήσει από το υποκείμενο των δεδομένων ποια από τα παρακάτω είναι διαθέσιμα:	
4624/2019	Δικαίωμα πρόσβασης του ατόμου στα δεδομένα	Πλήρως
4624/2019	Δικαίωμα διόρθωσης προσωπικών δεδομένων	Πλήρως
4624/2019	Δικαίωμα διαγραφής προσωπικών δεδομένων	Πλήρως
4624/2019	Δικαίωμα περιορισμού της επεξεργασίας	Πλήρως
4624/2019	Υπάρχουν μέτρα που αφορούν την διασφάλιση μη εξουσιοδοτημένης πρόσβαση	Πλήρως
4624/2019	Τηρείται κατάλογος με τυχόν παραβιάσεις προσωπικών δεδομένων	Πλήρως
4624/2019	Εφόσον προχωράτε στην καταγραφή κλήσεων, υπάρχει η αντίστοιχη ενημέρωση προς το άτομο που συνομιλείτε;	Πλήρως
4624/2019	Γίνεται τήρηση αρχείων των δραστηριοτήτων επεξεργασίας	Στοιχειωδώς
4624/2019	Έχει καταρτιστεί σχέδιο ανάκαμψης από τυχόν καταστροφές	Πλήρως
4624/2019	Εξασφαλίζεται η προστασία δεδομένων από απώλεια ή καταστροφή	Πλήρως
4624/2019	Τήρηση backup σε περίπτωση τεχνικού συμβάντος	Καθόλου
4624/2019	Αποτροπή μη εξουσιοδοτημένης εισαγωγής ,αντιγραφής ή τροποποίησης δεδομένων	Πλήρως

Υποβολή

Εικόνα 5.3: Ερωτήσεις που αφορούν το νόμο 4624/2019

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

Η συμπλήρωση που αφορά την «Συμμόρφωση» γίνεται από αναδυόμενο μενού που περιλαμβάνει 5 απαντήσεις και διαμορφώνεται βάσει του κάθε άρθρου.

Έτσι για τις ερωτήσεις που αφορούν την νομοθεσία 4727/20 έχουμε τα εξής:

Καθόλου	Όχι /Χειρόγραφη διαδικασία
Στοιχειωδώς	Τηρείται σε κάποια τμήματα/διευθύνσεις
Μερικώς	Τηρείται αλλά με διαφορετικές εφαρμογές
Πλήρως	Τηρήση στο σύνολο του φορέα
Δ/Α	Δεν απαιτείται

Για την νομοθεσία 4624/2019:

Καθόλου	Δεν γίνεται τήρηση του κανονισμού
Στοιχειωδώς	Συμμόρφωση υπό προϋποθέσεις
Μερικώς	Υπάρχει τήρηση σε μεγάλο βαθμό αλλά όχι παντα
Πλήρως	Πλήρης συμμόρφωση/ Τηρείται πάντα
Δ/Α	Δεν απαιτείται

Και για τις ερωτήσεις που αφορούν το «Cloud First Policy» έχουμε:

Καθόλου	Όλα τοπικά
Στοιχειωδώς	Τα περισσότερα τοπικά / κάποια σε cloud
Μερικώς	Τα περισσότερα σε cloud
Πλήρως	Όλα στο cloud
Δ/Α	Δεν απαιτείται

Στην συνέχεια ο χρήστης πατάει την «Υποβολή»

Καρτέλα αποτελεσμάτων

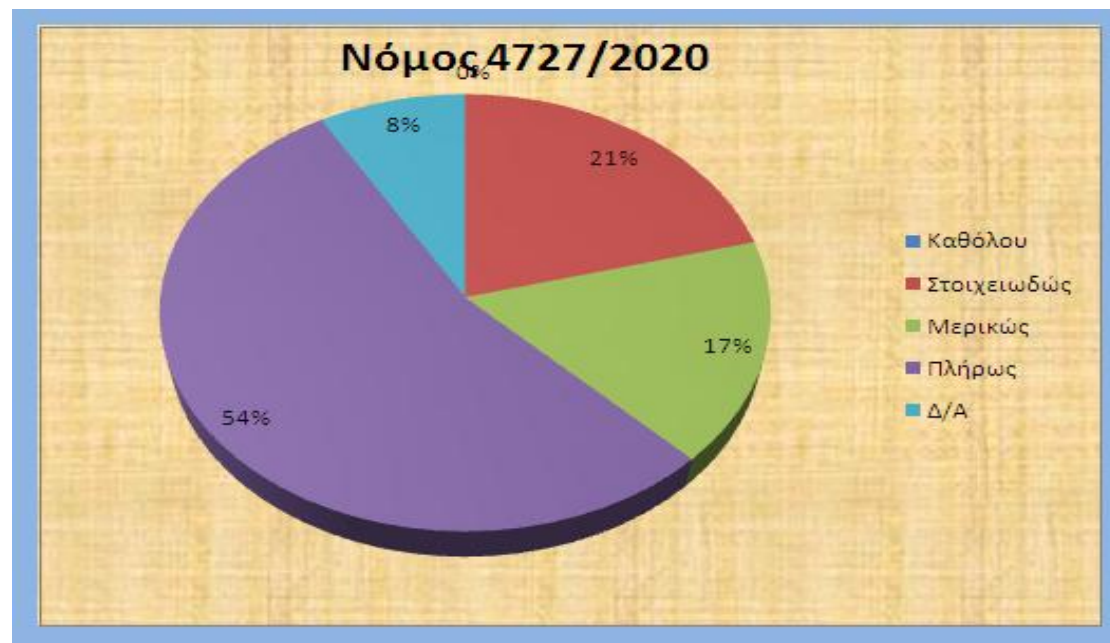
Εμφάνιση των αποτελεσμάτων για κάθε νομοθεσία ξεχωριστά.

Αποτελέσματα Αξιολόγησης								
Νομοθεσία								
4727/2020		Καθόλου	Στοιχειωδώς	Μερικώς	Πλήρως	Δ/Α	Σύνολο	Απαιτούμενα
		0	5	4	13	2	24	22
Νομοθεσία								
4624/2019		Καθόλου	Στοιχειωδώς	Μερικώς	Πλήρως	Δ/Α	Σύνολο	Απαιτούμενα
		1	2	2	20	0	25	25

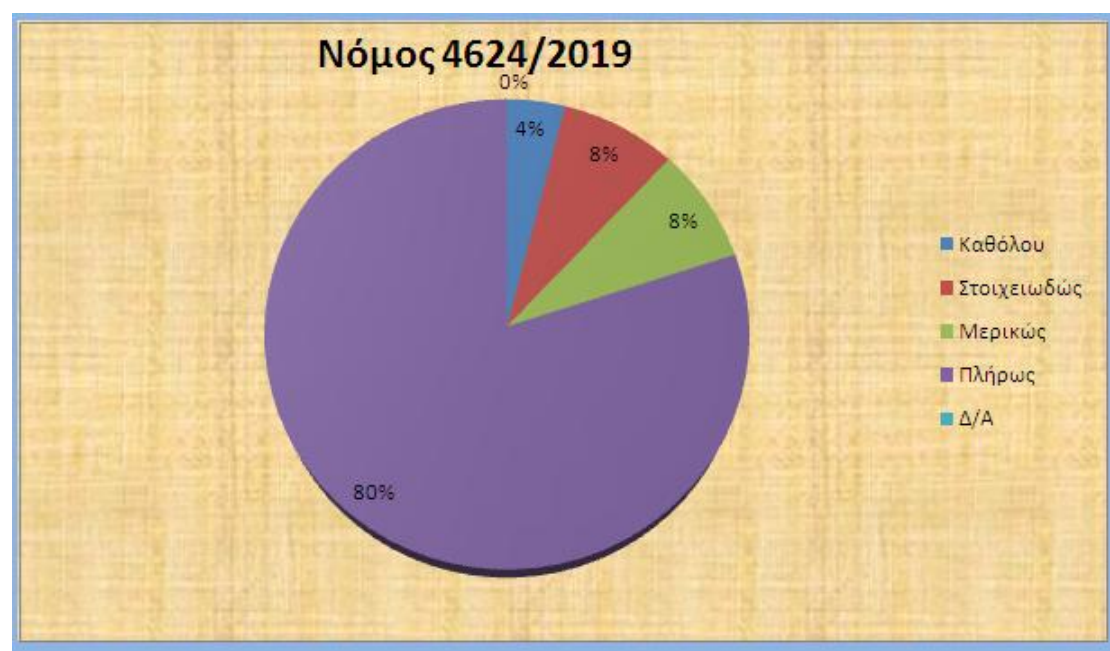
Εικόνα 5.4: Αριθμητικά αποτελέσματα

Η αξιολόγηση γίνεται πάντα με τα απαιτούμενα άρθρα για τον εκάστοτε φορέα. Από τον συνολικό αριθμό ερωτήσεων ανά νομοθεσία αφαιρούνται οι ερωτήσεις που έλαβαν ως απάντηση «Δ/Α -Δεν απαιτείται»

Και τα αντίστοιχα γραφήματα που αφορούν τις απαντήσεις που δόθηκαν.



Εικόνα 5.5: Ποσοστά επί των απαντήσεων για τον Νόμο 4727/2020



Εικόνα 5.6: Ποσοστά επί των απαντήσεων για τον Νόμο 4624/2019

Μετά την εμφάνιση των αποτελεσμάτων ο χρήστης έχει την δυνατότητα να λάβει πιστοποιητικό συμμόρφωσης με τις νομοθεσίες.

Το εργαλείο υπολογίζει και εμφανίζει συνολικά 3 βαθμούς αξιολόγησης:

- Ο πρώτος αφορά τον νόμο 4727/2020
- Ο δεύτερος αφορά τον νόμο 4624/2019
- Ο τρίτος αφορά τον συνολικό βαθμό του πιστοποιητικού και υπολογίζεται συναρτήσει των 2 πρώτων βαθμών αξιολόγησης.

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

Ο βαθμός αξιολόγησης υπολογίζεται βάσει του παρακάτω πίνακα:

ΠΙΝΑΚΑΣ ΑΞΙΟΛΟΓΗΣΗΣ	
Ποσοστό Συμμόρφωσης	Βαθμός
90-100	A
80-89	B
70-79	C
60-69	D
50-60	E
<50	F

Η επιλογή της συγκεκριμένης κλίμακας αξιολόγησης έγινε με βάση την κλίμακα 0%-100% που είναι γνωστή στα περισσότερα Πανεπιστήμια της Ευρώπης και της Αμερικής και με λατινικούς χαρακτήρες σημαίνει : A (90-100), B (80-89), C (70-79), D (60-69) και E (50-60) και F (<50), όπου F σημαίνει αποτυχία.

6. Εφαρμογή – Αξιολόγηση Δημόσιου Φορέα

Για τις ανάγκες αξιολόγησης της χρηστικότητας του εργαλείου και με σκοπό την αξιολόγηση ενός δημόσιου φορέα απευθύνθηκα στον Δήμο Ζωγράφου και συγκεκριμένα στον Υπεύθυνο Προστασίας Δεδομένων (DPO). Οι απαντήσεις που έλαβα σχετικά με την Συμμόρφωση με τις νομοθεσίες της Ηλεκτρονικής Διακυβέρνησης και την Ασφάλεια Προσωπικών Δεδομένων αναλύονται παρακάτω.

6.1 Αποτελέσματα Αξιολόγησης

α/α	Νομοθεσία	Περιγραφή Άρθρου	Συμμόρφωση
1	4727/2020	Γίνεται χρήση του προσωπικού αριθμού(Π.Α) ταυτοποίησης	Μερικώς
2	4727/2020	Προχωράτε στην έκδοση Ηλεκτρονικών Δημόσιων Εγγράφων	Πλήρως
3	4727/2020	Τήρηση Ηλεκτρονικού πρωτοκόλλου έναντι της χειρόγραφης πρωτοκόλλησης	Πλήρως
4	4727/2020	Είναι διαθέσιμη η ηλεκτρονική Αρχαιοθήκη εγγράφων	Πλήρως
5	4727/2020	Γίνεται στατιστική επεξεργασία δεδομένων με σκοπό την έκδοση αποτελεσμάτων χρήσης	Δ/Α
6	4727/2020	Είναι διαθέσιμη η παροχή ψηφιακών δημόσιων εγγράφων για οποιαδήποτε χρήση	Μερικώς
7	4727/2020	Υπάρχει τρόπος ταυτοποίησης για την έκδοση διαπιστευτηρίων	Μερικώς
8	4727/2020	Γίνεται έκδοση εγγράφων μέσω της Ενιαίας Ψηφιακής Πύλης	Πλήρως
9	4727/2020	Είναι διαθέσιμη η ηλεκτρονική Διακίνηση Δημόσιων Εγγράφων :	
10	4727/2020	Εντός του ίδιου φορέα	Πλήρως
11	4727/2020	Μεταξύ δημοσίων φορέων	Πλήρως
12	4727/2020	Δίνεται η δυνατότητα Ηλεκτρονικής πληρωμής οφειλών προς τον φορέα	Πλήρως
13	4727/2020	Υπάρχει η επιλογή για ηλεκτρονική καταβολή οφειλών των δημοσίων φορέων	Πλήρως
14	4727/2020	Για την εξυπηρέτηση πολιτών είναι διαθέσιμος ηλεκτρονικός τρόπος επικοινωνίας	Πλήρως
15	4727/2020	Διατήρηση διαδικτυακού ιστότοπου για τον φορέα με σκοπό την ενημέρωση	Πλήρως
16	4727/2020	Υπάρχουν οι κατάλληλες ρυθμίσεις προκειμένου οι υπηρεσίες σας να καταστούν περισσότερο προσβάσιμοι στους χρήστες	Πλήρως
17	4727/2020	Έχετε στην διάθεση σας ηλεκτρονικές βεβαιώσεις που εκδίδονται από έναν πάροχο υπηρεσιών εμπιστοσύνης	Πλήρως
18	4727/2020	Διάθεση για περαιτέρω χρήση πληροφοριών του δημόσιου τομέα(ανοικτά δεδομένα)	Πλήρως
19	4727/2020	Προχωράτε στην ανάρτηση όλων των πράξεων στο Διαύγεια	Πλήρως
20	4727/2020	Ανάρτηση οργανογράμματος και στοιχείων υπηρετούντων	Πλήρως
21	4727/2020	Δημοσίευση εκτέλεσης προϋπολογισμού	Πλήρως
22	4727/2020	Χρήση υπολογιστικού νέφους (cloud)	Πλήρως
23	4727/2020	Προτεραιότητα στην επιλογή υπηρεσιών νέφους από όλους τους δημόσιους φορείς (Cloud First Policy)	Μερικώς
24		Έχετε προχωρήσει στα παρακάτω:	
25	4727/2020	Εγγραφή στο Μητρώο Ψηφιακής Διακυβέρνησης	Μερικώς
26	4727/2020	Εγγραφή στο Μητρώο δικτυακών τόπων	Μερικώς

Εικόνα 6.1: Απαντήσεις που αφορούν το νόμο 4727/2020

Σχετικά με το νόμο 4727/2020 παρατηρούμε ότι ο συγκεκριμένος Δημόσιος φορέας συμβαδίζει σε μεγάλο ποσοστό στα επιμέρους άρθρα της Νομοθεσίας.

Η παροχή ψηφιακών δημόσιων εγγράφων για οποιαδήποτε χρήση και ταυτοποίηση για την έκδοση διαπιστευτηρίων βρίσκονται στο επίπεδο «Μερικώς» που συνεπάγεται ότι οι ενέργειες αυτές τηρούνται αλλά με διαφορετικές εφαρμογές. Η μη τήρηση των δύο αυτών ενεργειών έρχεται σε συνέχεια της μη ύπαρξης Προσωπικού Αριθμού για κάθε φυσικό πρόσωπο. Αυτό σημαίνει ότι δεν υπάρχει ο μέγιστος δυνατός βαθμός διαλειτουργικότητας μεταξύ των συστημάτων του συγκεκριμένου φορέα. Αποτέλεσμα αυτού είναι ότι πιθανά χρειάζονται περισσότερες από μία ταυτοποιήσεις ανάλογα με την φύση του αιτήματος που καταχωρείται από κάποιο πολίτη.

Επίσης σημαντικό είναι ότι ο συγκεκριμένος φορέας δεν έχει εφαρμόσει πλήρως την Εγγραφή στο Μητρώο ψηφιακής διακυβέρνησης και την Εγγραφή στο Μητρώο δικτυακών τόπων (ΜΗ.Δ.ΙΣ.ΕΦ). Η οδηγία αναφέρει ότι όλοι οι δημόσιοι φορείς να προχωρήσουν στην καταγραφή των ιστοτόπων τους έως την 23η/09/2020 ανεξάρτητα αν στην παρούσα χρονική στιγμή πληρούν τις προϋποθέσεις της ψηφιακής προσβασιμότητας ή όχι.

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Δεδομένων στην Ελλάδα

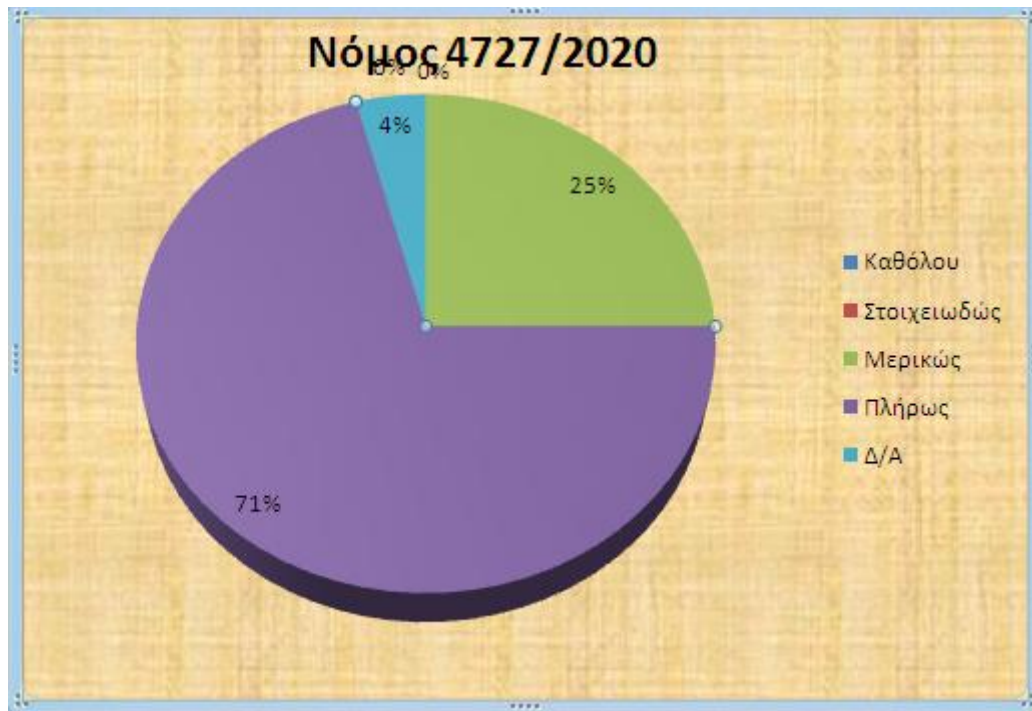
27	4624/2019	Έχετε προχωρήσει σε ορισμό υπεύθυνου προστασίας δεδομένων (DPO)	Πλήρως
28	4624/2019	Γίνεται λήψη συγκατάθεσης γονέα σε περίπτωση επεξεργασίας δεδομένων ανηλίκου κάτω των 15 ετών.	Πλήρως
29	4624/2019	Χρήση κλειστού κυκλώματος μόνο για την προστασία αγαθών και προσώπων και όχι για αξιολόγηση υπαλλήλων	Πλήρως
30	4624/2019	Έχετε προχωρήσει στην απαραίτητη μελέτη αντικτύπου σχετικά με την προστασία προσωπικών δεδομένων	Πλήρως
31	4624/2019	Γίνεται ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων	Πλήρως
32	4624/2019	Έχει συνταχθεί πολιτική προστασίας προσωπικών δεδομένων	Πλήρως
33	4624/2019	Διασφάλιση της επεξεργασίας δεδομένων για λόγους εθνικής ασφάλειας	Πλήρως
34	4624/2019	Υπάρχει νομική βάση για κάθε είδος επεξεργασίας δεδομένων	Πλήρως
35	4624/2019	Γραπτή συγκατάθεση του υποκειμένου για της επεξεργασία των δεδομένων του	Πλήρως
36	4624/2019	Επεξεργασία δεδομένων υπο την εποπτεία του υπεύθυνου επεξεργασίας	Πλήρως
37	4624/2019	Υπάρχει καταγραφή των απαραίτητων μέτρων για την κάλυψη των κανόνων ασφαλείας	Πλήρως
38	4624/2019	Προσβάσιμες πληροφορίες στο κοινό μέσω διαδικτυακού τόπου της δημόσιας αρχής	Πλήρως
39	4624/2019	Γίνεται ενημέρωση του υποκειμένου για την νομική βάση της επεξεργασίας των δεδομένων	Πλήρως
40	4624/2020	Εφόσον ζητηθεί από το υποκείμενο των δεδομένων ποια από τα παρακάτω είναι διαθέσιμα:	
41	4624/2019	Δικαίωμα πρόσβασης του ατόμου στα δεδομένα	Πλήρως
42	4624/2019	Δικαίωμα διόρθωσης προσωπικών δεδομένων	Πλήρως
43	4624/2019	Δικαίωμα διαγραφής προσωπικών δεδομένων	Πλήρως
44	4624/2019	Δικαίωμα περιορισμού της επεξεργασίας	Πλήρως
45	4624/2019	Υπάρχουν μέτρα που αφορούν την διασφάλιση μη εξουσιοδοτημένης πρόσβαση	Πλήρως
46	4624/2019	Τηρείται κατάλογος με τυχόν παραβιάσεις προσωπικών δεδομένων	Πλήρως
47	4624/2019	Εφόσον προχωράτε στην καταγραφή κλήσεων, υπάρχει η αντίστοιχη ενημέρωση προς το άτομο που συνομιλείτε;	Πλήρως
48	4624/2019	Γίνεται τήρηση αρχείων των δραστηριοτήτων επεξεργασίας	Πλήρως
49	4624/2019	Έχει καταρτιστεί σχέδιο ανάκαμψης από τυχόν καταστροφές	Πλήρως
50	4624/2019	Εκασφαλίζεται η προστασία δεδομένων από απώλεια ή καταστροφή	Πλήρως
51	4624/2019	Τήρηση backup σε περίπτωση τεχνικού συμβάντος	Πλήρως
52	4624/2019	Αποτροπή μη εξουσιοδοτημένης εισαγωγής, αντιγραφής ή τροποποίησης δεδομένων	Πλήρως

Εικόνα 6.2: Απαντήσεις που αφορούν το νόμο 4624/2019

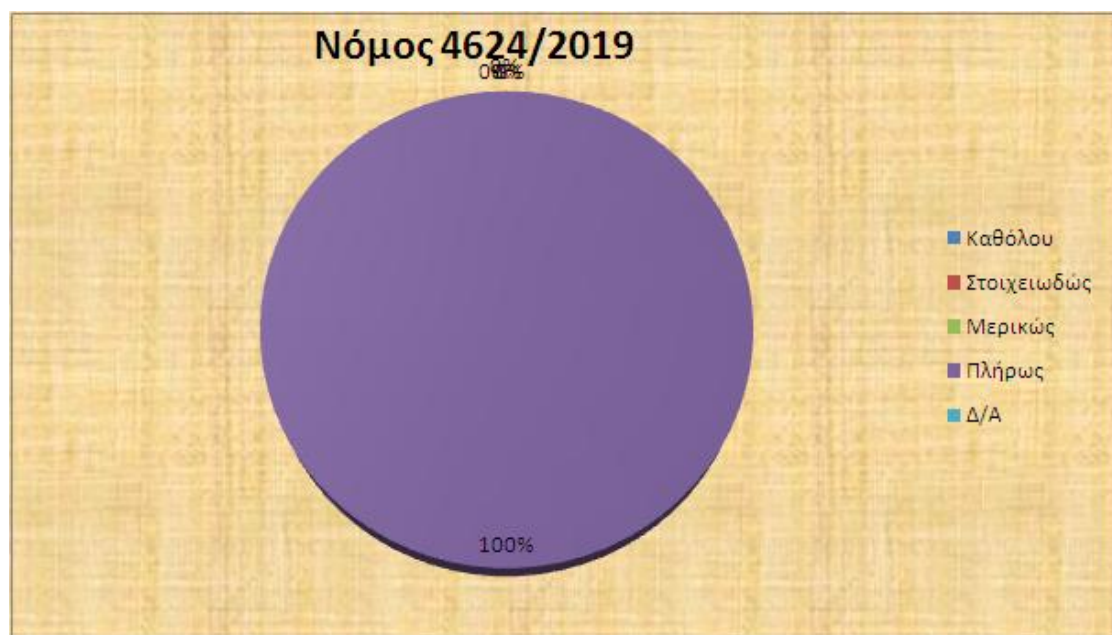
Όσο αφορά το νόμο 4624/2019 παρατηρούμε ότι το ποσοστό συμμόρφωσης είναι στο 100% όπως θα δούμε και στα παρακάτω διαγράμματα.

Αποτελέσματα Αξιολόγησης								
Νομοθεσία								
4727/2020	Καθόλου	Στοιχειωδώς	Μερικώς	Πλήρως	Δ/Α	Σύνολο	Απαιτούμενα	
	0	0	6	17	1	24	23	
Νομοθεσία								
4624/2019	Καθόλου	Στοιχειωδώς	Μερικώς	Πλήρως	Δ/Α	Σύνολο	Απαιτούμενα	
	0	0	0	25	0	25	25	

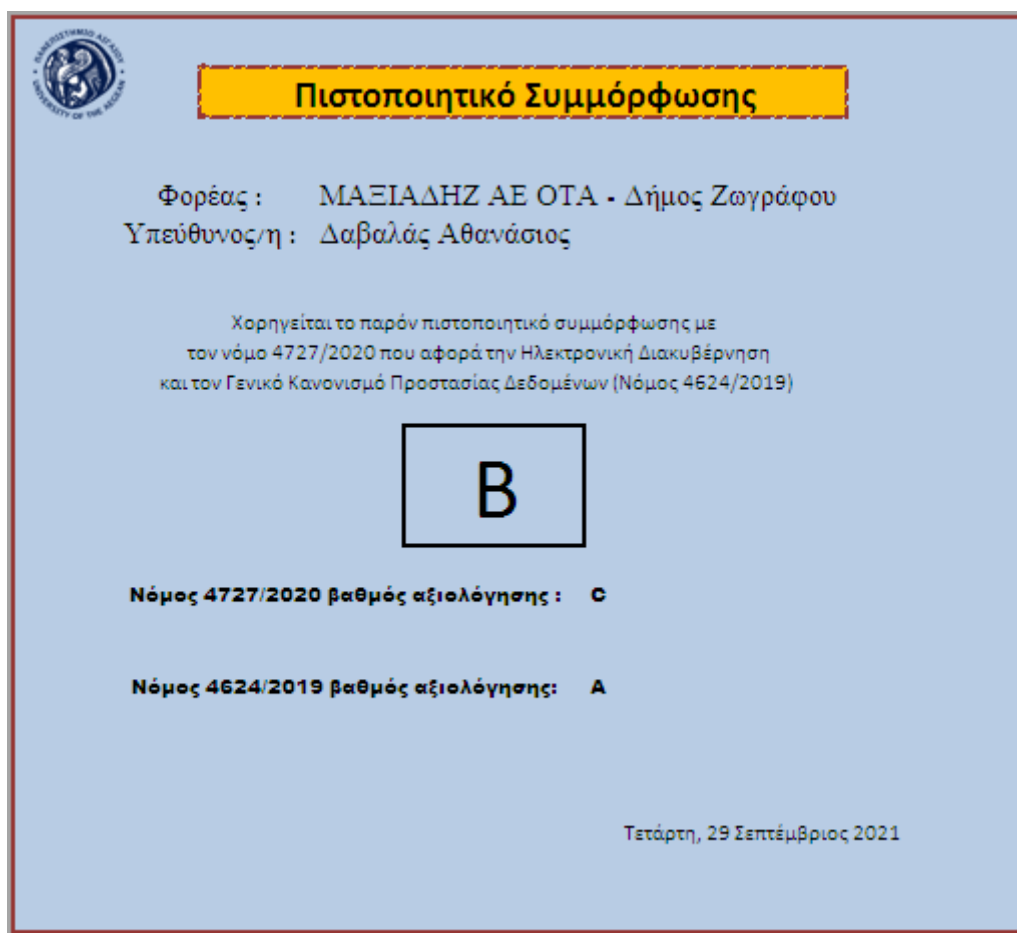
Εικόνα 6.3: Αριθμητικά αποτελέσματα Αξιολόγησης



Εικόνα 6.4: Ποσοστά επί των απαντήσεων για τον Νόμο 4727/2020



Εικόνα 6.5: Ποσοστά επί των απαντήσεων για τον Νόμο 4624/2019



Εικόνα 6.6: Πιστοποιητικό Συμμόρφωσης του Δημόσιου Φορέα

6.2 Συμπεράσματα από την αξιολόγηση του Φορέα.

Όπως παρουσιάστηκε στην προηγούμενη εικόνα, ο τελικός βαθμός αξιολόγησης του Δημόσιου φορέα είναι «B». Η συμμόρφωση με τον Νόμο 4727/2020 έχει σημεία βελτίωσης που θα ωφελήσουν τον βαθμό διαλειτουργικότητας μεταξύ των συστημάτων του και θα έχουν ως αποτέλεσμα την αμεσότερη διεκπεραίωση ζητημάτων και αιτημάτων από φυσικά πρόσωπα. Σημαντικότερη ενέργεια είναι η χρήση προσωπικού αριθμού (Π.Α) που είναι με απλή ενέργεια που προσφέρει σημαντικά οφέλη. Η ύπαρξη Υπεύθυνου Προστασίας Δεδομένων D.P.O δίνει ποσοστό συμμόρφωσης με την νομοθεσία περί Προστασίας Προσωπικών Δεδομένων. Διασφαλίζει κάθε ενέργεια που κάνει ο Δημόσιος φορέας με γνώμονα πάντα να μην υπάρξει κίνδυνος για τα φυσικά πρόσωπα και τα δεδομένα που καλείται να διαχειριστεί-επεξεργαστεί ο φορέας στον οποίο βρίσκεται.

7. Συμπεράσματα

7.1 Συμπεράσματα επί των αποτελεσμάτων

Σκοπός της παρούσας διπλωματικής εργασίας ήταν η θεωρητική επισκόπησης τριών βασικών ζητημάτων: α) του Νόμου 4727/2020 που αφορά την Ψηφιακή Διακυβέρνηση, β) του Γενικού Κανονισμού Προστασίας Δεδομένων – GDPR(Νόμος 4624/2019) και γ) τον βαθμό συμμόρφωσης ,με τις δύο νομοθεσίες, των φορέων του δημόσιου τομέα με την χρήση εργαλείου αξιολόγησης. Μέσα από την παρουσίαση των νομοθεσιών γίνεται προσπάθεια να δοθεί στον αναγνώστη μια πλήρης εικόνα για τις νομοθεσίες που βρίσκονται σε ισχύ.

Ο Νόμος 4727/2020 συστηματοποιεί και επικαιροποιεί ένα μεγάλο αριθμό διατάξεων από διάσπαρτες νομοθεσίες , ενώ ταυτόχρονα θεσμοθετεί το νέο πλαίσιο για τη συγκρότηση του Ψηφιακού Κράτους. Ειδικότερα με την καθιέρωση του προσωπικού αριθμού δίνεται το έναυσμα για την απλοποίηση και αυτοματοποίηση όλων των διαδικασιών που απαιτούνται για την ταυτοποίηση των οντοτήτων δίνοντας έμφαση στη διαλειτουργικότητα των ψηφιακών συστημάτων που χρησιμοποιούν οι φορείς του δημόσιου τομέα. Για την παροχή ψηφιακών δημόσιων υπηρεσιών και ιδίως για τη διακίνηση των ηλεκτρονικών εγγράφων ο ορισμός της Ενιαίας Ψηφιακής Πύλης (Ε.Ψ.Π.) δίνει την δυνατότητα άμεσης χρήσης εγγράφων χωρίς χρονοτριβές και γραφειοκρατία. Έτσι η διεκπεραίωση ζητημάτων γίνεται σε μικρότερο χρόνο με σεβασμό πάντα στην προστασία των προσωπικών δεδομένων.

Για την εξασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα απαιτείται η πλήρης συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων όπως θεσπίστηκε από τον νόμο 4624/2019. Βασικό στόχος του κανονισμού είναι η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ειδικότερα του δικαιώματός τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Ο ορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO) διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία σύμφωνα με τις διατάξεις του ΓΚΠΔ, χωρίς να παραβιάζεται η ιδιωτικότητα της κάθε οντότητας.

Είναι σημαντικό να αναφέρουμε τους περιορισμούς που συναντάμε με τις διατάξεις, κυρίως της Ηλεκτρονικής Διακυβέρνησης, στην συμμόρφωση δημόσιων φορέων. Γίνεται αντιληπτό ότι η εφαρμογή στοιχείων της Ηλεκτρονικής διακυβέρνησης είναι δύσκολη σε μικρές δημόσιες υπηρεσίες όπως για παράδειγμα σε ένα Αγροτικό Ιατρείο ή σε υπηρεσίες της αυτοδιοίκησης που βρίσκονται σε απομακρυσμένες περιοχές ή εξυπηρετούν μικρό αριθμό συναλλαγών (κοινοτικά γραφεία). Κάποιες φορές οι πόροι που διαχειρίζονται οι συγκεκριμένες υπηρεσίες είναι πολύ μικροί και έχουν ως αποτέλεσμα την αδυναμία εξασφάλισης περισσότερων πόρων με σκοπό την βελτίωση της ποιότητας των συναλλαγών.

7.2 Συμπεράσματα επί των εργαλείων

Για τις ανάγκες ελέγχου και πιστοποίησης της συμμόρφωσης για κάθε φορέα του δημόσιου τομέα που ακολουθεί την τεχνολογία και βαδίζει στο δρόμο της Ψηφιακής Διακυβέρνησης του κράτους είναι αναγκαία η δημιουργία ενός εργαλείου που θα ελέγχει τον βαθμό συμμόρφωσης με τις νομοθεσίες που αναφέρθηκαν παραπάνω. Έτσι σχεδιάστηκε το «Εργαλείο Αξιολόγησης Συμμόρφωσης με τις νομοθεσίες της Ηλεκτρονικής Διακυβέρνησης και την Ασφάλεια Προσωπικών Δεδομένων» ως μέσο ελέγχου για τους φορείς του δημόσιου τομέα. Πρόκειται για ένα χρήσιμο εργαλείο που σε πρώτη φάση μπορεί να χρησιμοποιηθεί σαν βοήθημα από το δημόσιο για να εντοπίσει τις αδυναμίες του κάθε φορέα, με σκοπό τον βέλτιστο βαθμό συμμόρφωσης.

Το εργαλείο θα έπρεπε να δημιουργηθεί με τον πλέον εύκολο τρόπο χρήσης ώστε να είναι λειτουργικό για όλους τους χρήστες. Επιλέχθηκε να γίνει με την χρήση του Microsoft Office Excel αν και πρόκειται για μια περισσότερο χρονοβόρα λύση σε σχέση με κάποιο online εργαλείο ή εφαρμογή. Μεταξύ της ευκολίας στην χρήση του εργαλείου μας και της ταχύτερης αλλά πιθανά πολυπλοκότερης διαδικασίας μιας εφαρμογής η επιλογή έγινε με βάση την ευχρηστία.

Παρόλα αυτά το εργαλείο ανταποκρίθηκε πλήρως στις απαιτήσεις που είχαμε θέσει κατά την αρχική προσέγγιση της διπλωματικής εργασίας και η λειτουργία του κρίνεται με επιτυχία.

Ο μόνος περιορισμός που θα μπορούσε να υπάρξει είναι η μη ύπαρξη D.P.O σε κάποιο δημόσιο φορέα(αν και υποχρεωτικός) με αποτέλεσμα να είναι δύσκολη η απάντηση των ερωτήσεων που αφορά την προστασία των προσωπικών δεδομένων.

Επίσης μια σημαντική δυσκολία κατά την ανάπτυξη του εργαλείου ήταν ο καθορισμός όσο των δυνατόν συντομότερων ερωτήσεων ώστε ο χρήστης να μη κληθεί να διαβάζει μεγάλους όγκους κειμένων. Ίσως αυτός ο περιορισμός να οδηγήσει σε λανθασμένη κατανόηση από τον χρήστη που καλείται να απαντήσει σε αυτές τις ερωτήσεις.

Κατά την διάρκεια της υλοποίησης απευθυνθήκαμε στον Δήμο Ζωγράφου και συγκεκριμένα στον Υπεύθυνο Προστασίας Δεδομένων (DPO) με κύριο στόχο τον βαθμό ελέγχου του Εργαλείου που δημιουργήθηκε και σκοπό την Αξιολόγηση ενός Δημόσιου Φορέα ως προς τον βαθμό συμμόρφωσης του με τις δύο νομοθεσίες.

Τα αποτελέσματα που λάβαμε μας δείχνουν σε απόλυτο βαθμό την σημαντικότητα ύπαρξης D.P.O σε κάθε δημόσιο φορέα καθώς τα ποσοστά συμμόρφωσης ως προς την προστασία των προσωπικών δεδομένων είναι 100%.

Ένα σημαντικό αποτέλεσμα που λάβαμε από την συγκεκριμένη διαδικασία είναι η ανάγκη για την ύπαρξη ενός ατόμου που θα είναι υπεύθυνο για την διασφάλιση όλων των ενεργειών που αφορά την Ηλεκτρονική Διακυβέρνηση σε κάθε φορέα, εξασφαλίζοντας με αυτό τον τρόπο την πλήρη διαλειτουργικότητα όλων των συστημάτων με σκοπό την ταχύτερη διεκπεραίωση διαδικασιών μέσω της χρήσης όλων των διαθέσιμων πόρων που θα εξασφαλίζει την μείωση λειτουργικών εξόδων για το κράτος.

7.3 Επόμενα βήματα-Μελλοντικοί στόχοι

Πρόκειται για τον βασικό κορμό ενός εργαλείου αξιολόγησης που ωστόσο έχει την δυνατότητα για μελλοντικές βελτιώσεις. Όπως προανέφερα το ιδανικό εργαλείο θα είχε την μορφή online χρήσης ή την κατασκευή εφαρμογής που θα έχει την δυνατότητα το Υπουργείο Ψηφιακής Διακυβέρνησης να γνωρίζει ανά πάσα στιγμή το βαθμό συμμόρφωσης όλων των φορέων του Δημόσιου Τομέα. Κάθε εργαλείο που δημιουργείται πάντα θα έχει περιθώρια βελτίωσης στο επόμενο στάδιο λειτουργίας του, με γνώμονα πάντοτε την ευχρηστία και την απλή διαδικασία.

8. Λεξικό όρων

8.1 Λεξικό όρων Νόμου 4727/2020

Για την καλύτερη κατανόηση των κεφαλαίων ακολουθεί μια λίστα με χρήσιμους ορισμούς σύμφωνα με τον Νόμο 4727/2020: [9]

Αρχή Πιστοποίησης: Η οντότητα που είναι αρμόδια για την τεχνική διαχείριση των πιστοποιητικών ηλεκτρονικής υπογραφής ή ηλεκτρονικής σφραγίδας ή ηλεκτρονικής χρονοσφραγίδας για ολόκληρο τον κύκλο ζωής τους.

Ασφάλεια Πληροφοριακών Συστημάτων: Η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, με δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών.

Ασφάλεια πληροφοριών-δεδομένων: Η ασφάλεια των πληροφοριών και δεδομένων που διακινούνται, υποβάλλονται σε επεξεργασία και αποθηκεύονται στα στοιχεία του πληροφοριακού συστήματος για τη διατήρηση της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των πληροφοριών.

Αυθεντικοποίηση: Ηλεκτρονική διαδικασία επαλήθευσης/επιβεβαίωσης ταυτότητας και των τυχόν ειδικών χαρακτηριστικών φυσικού ή νομικού προσώπου ή νομικής οντότητας, που βασίζεται σε χορηγηθέντα διαπιστευτήρια.

Δεδομένα δημιουργίας ηλεκτρονικής σφραγίδας: Μοναδικά δεδομένα που χρησιμοποιούνται από τον δημιουργό (νομικό πρόσωπο ή νομική οντότητα ή φορέας) της ηλεκτρονικής σφραγίδας για τη δημιουργία αυτής.

Δεδομένα δημιουργίας ηλεκτρονικής υπογραφής: Μοναδικά δεδομένα που χρησιμοποιούνται από τον υπογράφο για τη δημιουργία ηλεκτρονικής υπογραφής.

Δεδομένα μέτρησης: Τα ποσοτικά αποτελέσματα της δραστηριότητας παρακολούθησης που διενεργείται, προκειμένου να διαπιστωθεί η συμβατότητα των ιστότοπων και των εφαρμογών για φορητές συσκευές των οργανισμών του δημόσιου τομέα. Καλύπτουν τόσο ποσοτικές πληροφορίες σχετικά με το δείγμα ιστότοπων και εφαρμογών για φορητές συσκευές που ελέγχονται όπως, ιδίως, αριθμό ιστότοπων και εφαρμογών δυνητικά με τον αριθμό επισκεπτών και χρηστών τους, καθώς και ποσοτικές πληροφορίες σχετικά με το επίπεδο προσβασιμότητας.

Εγκεκριμένο πιστοποιητικό ηλεκτρονικής σφραγίδας: Πιστοποιητικό ηλεκτρονικής σφραγίδας που εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης.

Ηλεκτρονικά δημόσια έγγραφα: Τα δημόσια έγγραφα που παράγονται από φορείς του δημόσιου τομέα με χρήση Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ).

Ηλεκτρονική σφραγίδα: Δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή, με σκοπό τη διασφάλιση της προέλευσης και της ακεραιότητάς τους. Η ηλεκτρονική σφραγίδα χρησιμοποιείται από νομικά πρόσωπα, νομικές οντότητες και φορείς (δημιουργοί ηλεκτρονικής σφραγίδας).

Ηλεκτρονική υπογραφή: Δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή και τα οποία χρησιμοποιούνται από τον υπογράφο για να υπογράψει.

Ηλεκτρονική χρονοσφραγίδα: Δεδομένα σε ηλεκτρονική μορφή τα οποία συνδέουν άλλα δεδομένα σε ηλεκτρονική μορφή με ένα συγκεκριμένο χρονικό σημείο, τεκμηριώνοντας ότι τα εν λόγω δεδομένα υπήρχαν κατά το χρονικό σημείο εκείνο.

Ηλεκτρονικό έγγραφο: Οποιοδήποτε περιεχόμενο έχει αποθηκευτεί σε ηλεκτρονική μορφή και ειδικότερα ως κείμενο ή με ηχητική, οπτική ή οπτικοακουστική εγγραφή.

Ηλεκτρονικό πρωτόκολλο: Το πληροφοριακό σύστημα που εξυπηρετεί τη συλλογή, καταγραφή και διανομή των διακινούμενων εγγράφων με όποιο μέσο κι αν αυτά παράγονται, καταχωρίζονται ή διακινούνται.

Πιστοποιητικό ηλεκτρονικής σφραγίδας: Ηλεκτρονική βεβαίωση που συνδέει τα δεδομένα επικύρωσης ηλεκτρονικής σφραγίδας με νομικό πρόσωπο και επιβεβαιώνει το όνομα του εν λόγω προσώπου.

Πιστοποιητικό ηλεκτρονικής υπογραφής: Ηλεκτρονική βεβαίωση που συνδέει τα δεδομένα επικύρωσης ηλεκτρονικής υπογραφής με φυσικό πρόσωπο και επιβεβαιώνει τουλάχιστον το όνομα ή το ψευδώνυμο του εν λόγω προσώπου

Ταυτοποίηση: Διαδικασία εξακρίβωσης της ταυτότητας και των τυχόν ειδικών χαρακτηριστικών φυσικού ή νομικού προσώπου ή νομικής οντότητας, με τη χρήση δεδομένων που συνδέονται κατά τρόπο μοναδικό με αυτό

Υποστηρικτικές τεχνολογίες: ΤΠΕ, όπως υλικό υπολογιστή, λογισμικό, εφαρμογές, εργαλεία ανάπτυξης και βοηθήματα, για άτομα με αναπηρία γενικά ή και εξειδικευμένα για συγκεκριμένους τύπους αναπηρίας.

8.2 Λεξικό όρων Νόμου 4624/2019

Για την καλύτερη κατανόηση των κεφαλαίων ακολουθεί μια λίστα με χρήσιμους ορισμούς σύμφωνα με τον Νόμο 4624/2019: [20]

Βιομετρικά δεδομένα: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεδεμένη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλосκοπικά δεδομένα.

Γενετικά δεδομένα: τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.

Δεδομένα που αφορούν την υγεία: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

Δεδομένα προσωπικού χαρακτήρα: Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»): το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

Δημόσιος φορέας: Οι δημόσιες αρχές, οι ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, τα νομικά πρόσωπα δημοσίου δικαίου, οι οργανισμοί τοπικής αυτοδιοίκησης πρώτου και δεύτερου βαθμού και τα νομικά πρόσωπα και οι επιχειρήσεις αυτών, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα νομικά πρόσωπα ιδιωτικού δικαίου που ανήκουν στο κράτος ή επιχορηγούνται κατά 50% τουλάχιστον του ετήσιου προϋπολογισμού τους ή η διοίκησή τους ορίζεται από αυτό,

Εκτελών την επεξεργασία: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Επεξεργασία: Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Παραβίαση δεδομένων προσωπικού χαρακτήρα: Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,

Περιορισμός της επεξεργασίας: Η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.

Συγκατάθεση του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με

δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

Σύστημα αρχειοθέτησης: είναι κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε καταναμημένο σε λειτουργική ή γεωγραφική βάση,

Υπεύθυνος επεξεργασίας: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

9. Αναφορές

1. EUR-Lex - I24226b - EN - EUR-Lex. <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM:I24226b>.
2. <http://www.oecd.org/gov/budgeting/43496369.pdf> page 63
3. ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΗΜΟΣΙΑΣ ΙΟΙΚΗΣΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΙΑΚΥΒΕΡΝΗΣΗΣ. Ψηφιακή δημόσια διοίκηση για όλους. <https://docplayer.gr/29898384-Υπουργείο-esoterikon-geniki-grammateia-imosias-ioikisis-kai-ilektronikis-iakynvernisis-psifiaki-dimosia-dioikisi-gia-oloy.html>.
4. Διαλειτουργικότητα – Ανοικτή Διακυβέρνηση. <https://opengov.minedu.gov.gr/%CE%B4%CE%B9%CE%B1%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1/>.
5. Άρθρο 1 Σκοπός και πεδίο εφαρμογής του Κώδικα | Υπουργείο Ψηφιακής Διακυβέρνησης. <http://www.opengov.gr/digitalandbrief/?p=1942>.
6. <https://www.hellenicparliament.gr/UserFiles/c8827c35-4399-4fbb-8ea6-aebdc768f4f7/11367041.pdf>
7. http://www.icsd.aegean.gr/website_files/proptyxiako/525297129.pdf
8. 6.1. Ενιαία Ψηφιακή Πύλη (GOV.GR) | Υπουργείο Ψηφιακής Διακυβέρνησης. <http://www.opengov.gr/digitalandbrief/?p=2142>.
9. ΦΕΚ Α 184/23.09.2020-ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4727 Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.
10. Τι σημαίνει Ανοιχτά δεδομένα; | data.europa.eu. <https://data.europa.eu/el/trening/what-open-data>.
11. Η Ανοικτή Πρόσβαση στα ερευνητικά δεδομένα | OpenAccess.gr. <http://www.openaccess.gr/el/oa-researchdata>.
12. Ανάρτηση Πράξεων στο Διαδίκτυο | Πρόγραμμα Δι@ύγεια -. <https://diavgeia.gov.gr/info>.
13. ΑΔΑ (ΑΡΙΘΜΟΣ ΔΙΑΔΙΚΤΥΑΚΗΣ ΑΝΑΡΤΗΣΗΣ) | Diavgeia blog. <https://diavgeia.gov.gr/blog/?p=59>.
14. Οργανόγραμμα Γ.Γ.Υ.Ο. - Υπουργείο Οικονομικών. <https://www.minfin.gr/web/g.g.-ypourgeiou-oikonomikon/organogramma-g.g.y.o>.
15. Υπολογιστικό Νέφος (Cloud Computing) | ΕΠΣΕΤ. <http://www.epset.gr/el/content/ypologistiko-nefos-cloud-computing>.
16. <https://computertechinfo.gr/cloud-storage-computing/>
17. Τι είναι ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation) | ΠΕΡΙΟΔΙΚΟ ACCOUNTANCY GREECE. <https://www.accountancygreece.gr/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%BF-%CE%B3%CE%B5%CE%BD%CE%B9%CE%BA%CF%8C%CF%82-%CE%BA%CE%B1%CE%BD%CE%BF%CE%BD%CE%B9%CF%83%CE%BC%CF%8C%CF%82-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83/>

Ανάλυση του Θεσμικού Πλαισίου Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας
Δεδομένων στην Ελλάδα

18. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 άρθρο 4
19. 'Προσωπικά δεδομένα, στρατιωτικές εγκαταστάσεις και εθνική ασφάλεια: Μία ενδιαφέρουσα απόφαση της ΑΠΔΠΧ'. Lawspot, 24 Ιούλιος 2020, <https://www.lawspot.gr/node/268943>
20. *ΦΕΚ 137/Α/29-8-2019-Νόμος 4624/2019 : Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων.*