



UNIVERSITY *of* NICOSIA

Κοινό Μεταπτυχιακό Πρόγραμμα Σπουδών «Δίκαιο της
Οικονομίας και των
Επιχειρήσεων»

Διπλωματική Εργασία

«Η προστασία των προσωπικών δεδομένων στον δημόσιο τομέα στο
πλαίσιο της ψηφιακής μετάβασης»

Διονύσης Κόκκαλης

A.M. U234N2261

Επιβλέπων καθηγητής: «Απόστολος Μάνθος»

Πάτρα, Μάιος 2025

Περίληψη

Η προστασία των προσωπικών δεδομένων εντός του δημόσιου τομέα αποτελεί πρωταρχικό μέλημα στην ψηφιακή εποχή, λαμβάνοντας υπόψη τον τεράστιο όγκο ευαίσθητων πληροφοριών που διαχειρίζονται κυβερνητικοί οργανισμοί. Αυτή η διατριβή εξετάζει τα νομικά, τεχνολογικά και οργανωτικά πλαίσια που ρυθμίζουν την προστασία δεδομένων σε δημόσιους οργανισμούς, αξιολογώντας τα εμπόδια, τους κινδύνους και τις βέλτιστες προσεγγίσεις για τη διασφάλιση της συμμόρφωσης και της ασφάλειας. Η έρευνα αναλύει βασικά νομικά πλαίσια, όπως ο GDPR και οι εθνικοί κανονισμοί, σε συνδυασμό με καίριες δικαστικές αποφάσεις που επηρεάζουν την πολιτική προστασίας δεδομένων του δημόσιου τομέα.

Οι τεχνολογικές προστασίες, συμπεριλαμβανομένων των πρωτοκόλλων κρυπτογράφησης, ανωνυμοποίησης και ασφάλειας στον κυβερνοχώρο, αξιολογούνται στο πλαίσιο της διακυβέρνησης δεδομένων του δημόσιου τομέα. Η μελέτη δίνει έμφαση στους εσωτερικούς κινδύνους, όπως το ανθρώπινο λάθος και τις εσωτερικές απειλές, καθώς και τους εξωτερικούς κινδύνους, όπως οι επιθέσεις στον κυβερνοχώρο και τα αναδυόμενα προβλήματα απορρήτου. Η διατριβή εξετάζει επίσης την κοινή γνώμη για τις πρωτοβουλίες προστασίας δεδομένων και τις επιπτώσεις τους στην εμπιστοσύνη στους κυβερνητικούς θεσμούς.

Το τελευταίο κεφάλαιο παρουσιάζει συστάσεις πολιτικής και βέλτιστες πρακτικές για τη βελτίωση της προστασίας δεδομένων, τονίζοντας την ανάγκη για ισχυρά πλαίσια διακυβέρνησης, αναθεωρημένους κανόνες και την ενσωμάτωση της αναπτυσσόμενης τεχνολογίας. Αυτή η έκθεση παρέχει μια ενδελεχή εξέταση των τρεχόντων πλαισίων και των μελλοντικών δυσκολιών, παρέχοντας σημαντικές γνώσεις για τους υπεύθυνους χάραξης πολιτικής, τους διαχειριστές και τους νομικούς εμπειρογνώμονες στην προστασία των προσωπικών δεδομένων.

Λέξεις-κλειδιά: προστασία δεδομένων, δημόσιος τομέας, GDPR, κυβερνοασφάλεια, ιδιωτικότητα, ψηφιακή μετάβαση

Abstract

The safeguarding of personal data within the public sector is a paramount concern in the digital age, considering the vast volumes of sensitive information handled by governmental organizations. This thesis examines the legal, technological, and organizational frameworks regulating data protection in public organizations, assessing the obstacles, risks, and optimal approaches for guaranteeing compliance and security. The research analyzes essential legal frameworks, such as the GDPR and national regulations, in conjunction with pivotal court decisions that influence public sector data protection policy.

Technological protections, including encryption, anonymization, and cybersecurity protocols, are evaluated within the framework of public sector data governance. The study emphasizes internal risks, such as human error and insider threats, as well as external risks, like cyberattacks and emerging privacy problems. The thesis also examines public opinion of data protection initiatives and their effects on trust in governmental institutions.

The last chapter presents policy recommendations and optimal practices to improve data protection, highlighting the necessity for robust governance frameworks, revised rules, and the integration of developing technology. This report provides a thorough examination of current frameworks and future difficulties, delivering significant insights for policymakers, administrators, and legal experts in the protection of personal data.

Keywords: data protection, public sector, GDPR, cybersecurity, privacy, digital transformation

Περιεχόμενα

<i>Περίληψη</i>	<i>1</i>
<i>Abstract</i>	<i>3</i>
<i>Κεφάλαιο 1: Εισαγωγή</i>	<i>6</i>
1.1. Ερευνητικό πρόβλημα, συνάφεια και ερευνητικά ερωτήματα	6
1.2. Σημασία της προστασίας των δεδομένων	7
1.3. Σημασία της έρευνας.....	9
<i>Κεφάλαιο 2: Νομικό Πλαίσιο για την Προστασία Δεδομένων στον Δημόσιο Τομέα</i>	<i>10</i>
2.1. Γενικές Αρχές του Δικαίου Προστασίας Δεδομένων.....	10
2.1.1. Θεμελιώδεις αρχές	10
2.1.2. Νομική βάση για την επεξεργασία στη δημόσια διοίκηση	11
2.2. Ο ΓΚΠΔ και η νομική εφαρμογή του στον δημόσιο τομέα.....	12
2.3. Ελληνική Εθνική Νομοθεσία για την Προστασία Δεδομένων	13
2.3.1. Επισκόπηση της ελληνικής νομοθεσίας για την προστασία δεδομένων	13
2.3.2. Ειδικές νομικές διατάξεις για τον δημόσιο τομέα	14
2.3.3. Συνοχή και ενότητα της ελληνικής νομοθεσίας.....	15
<i>Κεφάλαιο 3: Θεσμικές και τεχνολογικές πτυχές της προστασίας δεδομένων</i>	<i>17</i>
3.1. Διακυβέρνηση δεδομένων σε δημόσια ιδρύματα	17
3.1.1. Οργανωτικές δομές για την προστασία των δεδομένων	17
3.1.2. Ρόλοι και αρμοδιότητες	19
3.2. Νομικές υποχρεώσεις για τεχνικά και οργανωτικά μέτρα	21
3.2.1. Νομικές απαιτήσεις για την κρυπτογράφηση και την ανωνυμοποίηση	21
3.2.2. Υποχρεώσεις κοινοποίησης περιστατικών.....	22
3.2.3. Εσωτερικοί έλεγχοι και εκτιμήσεις κινδύνου βάσει της ελληνικής νομοθεσίας.....	23
3.3. Κοινή χρήση δεδομένων και διαλειτουργικότητα	23
3.3.1. Εξισορρόπηση της κοινής χρήσης δεδομένων και της ιδιωτικής ζωής	23
3.3.2. Προκλήσεις στη διαθεσμική κοινή χρήση δεδομένων	25
<i>Κεφάλαιο 4: Νομικοί Κίνδυνοι και Προκλήσεις στην Προστασία Δεδομένων του Δημόσιου Τομέα</i>	<i>27</i>
4.1. Νομική Κατηγοριοποίηση Εσωτερικών και Εξωτερικών Κινδύνων.....	27
4.1.1. Ανθρώπινο λάθος, εσωτερικές απειλές	27
4.1.2. Επιθέσεις στον κυβερνοχώρο σε δημόσια ιδρύματα	29
4.2. Συμμόρφωση και νομικές προκλήσεις.....	31
4.2.1. Διασφάλιση της συμμόρφωσης με τον GDPR και τις κανονιστικές διατάξεις	31
4.2.2. Ζητήματα διακρατικού χειρισμού δεδομένων	33
4.3. Δημόσια αντίληψη και εμπιστοσύνη	35
4.3.1. Εμπιστοσύνη του κοινού στην προστασία των δεδομένων	35
4.3.2. Διαφάνεια και λογοδοσία.....	37
<i>Κεφάλαιο 5: Βέλτιστες πρακτικές, συστάσεις και μελλοντικές κατευθύνσεις.....</i>	<i>39</i>
5.1. Βέλτιστες πρακτικές για την προστασία των δεδομένων στον δημόσιο τομέα.....	39
5.1.1. Εφαρμογή ισχυρών πλαισίων διακυβέρνησης	39
5.1.2. Προγράμματα κατάρτισης και ευαισθητοποίησης.....	41

5.1.3. Τεχνολογικές καινοτομίες για την ασφάλεια των δημόσιων δεδομένων	42
5.2. Συστάσεις πολιτικής.....	45
5.2.1. Βελτίωση των κανονιστικών πλαισίων.....	45
5.2.2. Ενθάρρυνση συμπράξεων δημόσιου και ιδιωτικού τομέα	47
5.3. Μελλοντικές προκλήσεις και ευκαιρίες.....	49
5.3.1. Το μέλλον της προστασίας των δεδομένων στην ψηφιακή κοινωνία	49
5.3.2. Αντιμετώπιση αναδυόμενων ζητημάτων προστασίας της ιδιωτικής ζωής	51
Κεφάλαιο 6: Συμπεράσματα.....	54
Βιβλιογραφία.....	56

Κεφάλαιο 1: Εισαγωγή

1.1. Ερευνητικό πρόβλημα, συνάφεια και ερευνητικά ερωτήματα

Το απόρρητο έχει καταστεί πρωταρχικό μέλημα στο σύγχρονο ψηφιακό περιβάλλον, ειδικά στον δημόσιο τομέα, καθώς οι κυβερνητικοί οργανισμοί αποκτούν, αποθηκεύουν και επεξεργάζονται σημαντικούς όγκους ευαίσθητων πληροφοριών. Οι δημόσιοι οργανισμοί επιβλέπουν ένα πλήθος προσωπικών δεδομένων, που περιλαμβάνουν αρχεία υγειονομικής περίθαλψης, πληροφορίες κοινωνικών υπηρεσιών, φορολογικά δεδομένα και βάσεις δεδομένων επιβολής του νόμου, εντείνοντας έτσι την ανάγκη για αυστηρή ασφάλεια. Το πρωταρχικό ερευνητικό πρόβλημα αυτής της μελέτης επικεντρώνεται στις δυσκολίες που αντιμετωπίζουν οι δημόσιοι οργανισμοί στη διαφύλαξη των προσωπικών δεδομένων, ενώ τηρούν τις μεταβαλλόμενες νομικές εντολές και τις κοινωνικές προσδοκίες¹. Σε αντίθεση με τις ιδιωτικές επιχειρήσεις, ο δημόσιος τομέας λειτουργεί συχνά υπό αυστηρότερη ρυθμιστική εποπτεία και οι παραβιάσεις δεδομένων μπορούν να έχουν εκτεταμένες επιπτώσεις, επηρεάζοντας τα άτομα και διαβρώνοντας την εμπιστοσύνη του κοινού.

Οι κυβερνητικές υπηρεσίες πρέπει να συμβιβάσουν το καθήκον τους να παρέχουν κρίσιμες δημόσιες υπηρεσίες με την ανάγκη τους να διαφυλάξουν το ατομικό απόρρητο². Η ψηφιοποίηση των κυβερνητικών λειτουργιών έχει εντείνει τα ζητήματα απορρήτου δεδομένων, καθώς οι προσωπικές πληροφορίες επεξεργάζονται διαρκώς, διαδίδονται και περιστασιακά διατηρούνται για πάντα. Η κλιμακούμενη πολυπλοκότητα των απειλών στον κυβερνοχώρο, η ταχεία πρόοδος της τεχνολογίας επεξεργασίας δεδομένων και η τεράστια ποσότητα δεδομένων που διαχειρίζονται δημόσιοι οργανισμοί ενισχύουν τους σχετικούς κινδύνους. Αυτή η έρευνα επιδιώκει να εντοπίσει περιπτώσεις όπου οι δημόσιοι φορείς ενδέχεται να προστατεύουν ανεπαρκώς τα προσωπικά δεδομένα και να προτείνει βελτιώσεις στις τρέχουσες πολιτικές και πλαίσια.

Εκτός από τα νομικά και τεχνολογικά ζητήματα, η έκθεση τονίζει τις ευρύτερες κοινωνικοοικονομικές συνέπειες των αστοχιών προστασίας δεδομένων στον δημόσιο τομέα. Οι παραβιάσεις δεδομένων ή ο λάθος χειρισμός προσωπικών πληροφοριών από κυβερνητικούς φορείς μπορούν να διαβρώσουν την εμπιστοσύνη του κοινού, να διακόψουν βασικές υπηρεσίες και να απειλήσουν ενδεχομένως την εθνική ασφάλεια³. Επιπλέον, καθώς οι κυβερνήσεις εξαρτώνται όλο και περισσότερο από τη λήψη αποφάσεων βάσει δεδομένων, η ασφαλής διαχείριση των προσωπικών πληροφοριών είναι απαραίτητη για τη διατήρηση της αξιοπιστίας και της αποτελεσματικότητας της δημόσιας διοίκησης. Αυτό υπογραμμίζει τη σημασία του απορρήτου των δεδομένων ως θέμα διακυβέρνησης και όχι απλώς ως νομικό ή τεχνικό εμπόδιο.

Ο δημόσιος τομέας λειτουργεί με συγκεκριμένο νομικό πλαίσιο που συχνά διαφέρει από τα πρότυπα προστασίας δεδομένων του εμπορικού τομέα. Οι κρατικές οντότητες υποχρεούνται να τηρούν τους εθνικούς και διεθνείς νόμους που ρυθμίζουν την απόκτηση, την επεξεργασία και τη

¹ Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Van Der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, 34(2), 234–243. <https://doi.org/10.1016/j.clsr.2017.09.001>

² De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194. <https://doi.org/10.1016/j.clsr.2016.02.006>

³ Ρίζου, Α. Σ. (with Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης). (2023). *Η συμβολή του γενικού κανονισμού προστασίας δεδομένων στην καταπολέμηση του εργασιακού εκφοβισμού και την προστασία των whistleblowers στον δημόσιο τομέα*.

διανομή προσωπικών δεδομένων. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση έχει θεσπίσει αυστηρές εντολές προστασίας δεδομένων, απαιτώντας από τους δημόσιους φορείς να τηρούν αυστηρή συμμόρφωση⁴. Η μη συμμόρφωση μπορεί να έχει νομικές επιπτώσεις και να μειώσει την εμπιστοσύνη του κοινού, και ως εκ τούτου να απαιτεί διεξοδική αξιολόγηση της αποτελεσματικότητας των ισχυόντων κανόνων και θεσμικών διαδικασιών για την αντιμετώπιση περίπλοκων ζητημάτων προστασίας δεδομένων.

Ο κύριος στόχος αυτής της διατριβής είναι να αξιολογήσει την αποτελεσματικότητα των μέτρων προστασίας προσωπικών δεδομένων στον δημόσιο τομέα, εστιάζοντας στο νομοθετικό και διοικητικό πλαίσιο που διέπει τη συλλογή, την επεξεργασία και τη διατήρηση δεδομένων. Λαμβάνοντας υπόψη την κλιμακούμενη εξάρτηση από τις ψηφιακές τεχνολογίες και την αυξανόμενη ποσότητα δεδομένων που διακινούνται από δημόσιους οργανισμούς, είναι σημαντικό να εκτιμηθεί εάν οι υπάρχουσες πολιτικές προστασίας δεδομένων αντιμετωπίζουν επαρκώς τις αναπτυσσόμενες απειλές και συμμορφώνονται με ρυθμιστικά κριτήρια όπως ο GDPR.

Αυτή η μελέτη θα εξετάσει κρίσιμα ερωτήματα: Ποια είναι η αποτελεσματικότητα των υφιστάμενων νομοθετικών πλαισίων, όπως ο GDPR και η εθνική νομοθεσία περί προστασίας δεδομένων, στη ρύθμιση της προστασίας δεδομένων του δημόσιου τομέα; Ποιες τεχνολογικές διασφαλίσεις, συμπεριλαμβανομένης της κρυπτογράφησης, της ανωνυμοποίησης και των προτύπων ασφάλειας στον κυβερνοχώρο, χρησιμοποιούνται από τους δημόσιους φορείς και πόσο αποτελεσματικές είναι αυτές για τον μετριασμό των παραβιάσεων δεδομένων; Πώς οργανώνουν οι δημόσιοι οργανισμοί τα πλαίσια διακυβέρνησης δεδομένων τους και ποιες λειτουργίες έχουν οι υπεύθυνοι προστασίας δεδομένων και τα άλλα μέλη του προσωπικού για τη διασφάλιση της συμμόρφωσης; Επιπλέον, με ποιον τρόπο επηρεάζει η κοινή γνώμη για τις κυβερνητικές πρωτοβουλίες προστασίας δεδομένων την πίστη στις δημόσιες υπηρεσίες; Η εξέταση αυτών των ερευνών θα βελτιώσει την κατανόηση της προστασίας δεδομένων του δημόσιου τομέα και θα προσφέρει προτάσεις για τη βελτίωση των υφιστάμενων πολιτικών.

1.2. Σημασία της προστασίας των δεδομένων

Το απόρρητο των δεδομένων έχει καταστεί πρωταρχικό μέλημα στην ψηφιακή εποχή, ειδικά όταν η συλλογή και η επεξεργασία προσωπικών πληροφοριών ενσωματώνονται όλο και περισσότερο στην καθημερινή ζωή. Η σημασία της προστασίας δεδομένων έγκειται στη λειτουργία της ως ασπίδα για την ατομική ιδιωτικότητα και την προσωπική αυτονομία. Σε μια εποχή όπου τα δεδομένα αποκαλούνται συχνά το «νέο πετρέλαιο», οι εκτενείς προσωπικές πληροφορίες που διαθέτουν οι δημόσιοι οργανισμοί έχουν σημαντική σημασία, όχι μόνο για τη διακυβέρνηση αλλά και για τα ατομικά δικαιώματα. Η διαφύλαξη αυτών των δεδομένων είναι απαραίτητη για την αποτροπή της κακής χρήσης τους, τη διατήρηση του απορρήτου και τη διατήρηση της εμπιστοσύνης των πολιτών που παρέχουν αυτές τις πληροφορίες με αντάλλαγμα ζωτικής σημασίας δημόσιες υπηρεσίες.

⁴ Ρίζου, Α. Σ. (with Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης). (2023). *Η συμβολή του γενικού κανονισμού προστασίας δεδομένων στην καταπολέμηση του εργασιακού εκφοβισμού και την προστασία των whistleblowers στον δημόσιο τομέα.*

Η σημασία της προστασίας δεδομένων στον δημόσιο τομέα ξεπερνά αυτή στον ιδιωτικό τομέα. Οι κυβερνήσεις συλλέγουν τακτικά πολύ ευαίσθητα δεδομένα, συμπεριλαμβανομένων αριθμών κοινωνικής ασφάλισης, μητρώων υγείας, φορολογικών δηλώσεων και ποινικών ιστοριών. Ένας συμβιβασμός αυτών των δεδομένων μπορεί να οδηγήσει σε σοβαρές επιπτώσεις, όπως κλοπή ταυτότητας, οικονομική απάτη και αποκάλυψη ευαίσθητων προσωπικών πληροφοριών. Για τους μειονεκτούντες πληθυσμούς, συμπεριλαμβανομένων των ατόμων που λαμβάνουν κοινωνική βοήθεια ή των προσφύγων, οι επιπτώσεις της κακής διαχείρισης δεδομένων μπορεί να είναι ακόμη πιο σοβαρές, οδηγώντας ενδεχομένως σε διακρίσεις, στιγματισμό ή απειλές για την προσωπική ασφάλεια. Κατά συνέπεια, η προστασία δεδομένων δεν αποτελεί απλώς νομική υποχρέωση αλλά και ηθικό καθήκον του δημόσιου τομέα να προστατεύει τα άτομα που εξυπηρετεί.

Επιπλέον, ο δημόσιος τομέας πρέπει να διασχίσει το περίπλοκο τοπίο της διαφύλαξης δεδομένων, διατηρώντας παράλληλα τη διαφάνεια και την αποτελεσματικότητα στην παροχή υπηρεσιών. Η εμπιστοσύνη του κοινού είναι ένα κρίσιμο στοιχείο αυτής της εξίσωσης. Εάν τα άτομα αντιλαμβάνονται τα προσωπικά τους στοιχεία ως ανασφαλή εντός των κρατικών θεσμών, η εμπιστοσύνη τους στο κράτος και η ικανότητά του να παρέχει σημαντικές υπηρεσίες μπορεί να μειωθεί. Η απουσία εμπιστοσύνης μπορεί να οδηγήσει σε επιδείνωση της σχέσης μεταξύ του κράτους και των κατοίκων του, αναγκάζοντας τα άτομα να διστάζουν να μοιραστούν βασικές πληροφορίες ή να εμπλακούν σε δημόσιες υπηρεσίες. Σε σοβαρές περιπτώσεις, όπως η διαρροή ή η κακή χρήση ευαίσθητων δεδομένων από τις αρχές, η δημόσια αγανάκτηση μπορεί να οδηγήσει σε διάχυτη καχυποψία για κυβερνητικές οντότητες, διαβρώνοντας τη νομιμότητα των κρατικών θεσμών.

Η προστασία δεδομένων είναι απαραίτητη από νομική και κανονιστική άποψη. Η εφαρμογή εκτεταμένων νομοθετικών πλαισίων όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων στην Ευρωπαϊκή Ένωση έχει θεσπίσει αυστηρά πρότυπα για την προστασία δεδομένων που ισχύουν τόσο για ιδιωτικές επιχειρήσεις όσο και για δημόσιους φορείς. Οι κυβερνήσεις οφείλουν πλέον να τηρούν αυτά τα πρότυπα, διασφαλίζοντας ότι χειρίζονται τα δεδομένα νόμιμα, δίκαια και ανοιχτά. Η μη συμμόρφωση μπορεί να οδηγήσει σε σημαντικές κυρώσεις, νομικές συγκρούσεις και βλάβη στη φήμη. Αυτό το κανονιστικό πλαίσιο υπογραμμίζει την αναγκαιότητα της προστασίας των δεδομένων ως νομική υποχρέωση που οι δημόσιοι φορείς δεν πρέπει να παραμελούν.

Εκτός από τις νομικές και ηθικές ευθύνες, η προστασία δεδομένων είναι απαραίτητη σε μια κοινωνία που επηρεάζεται όλο και περισσότερο από κινδύνους στον κυβερνοχώρο. Οι δημόσιοι οργανισμοί αποτελούν πρωταρχικούς στόχους για κυβερνοεπιθέσεις λόγω των σημαντικών ποσοτήτων ευαίσθητων πληροφοριών που διαθέτουν. Μια επιτυχημένη κυβερνοεπίθεση σε ένα κυβερνητικό σύστημα μπορεί να θέσει σε κίνδυνο όχι μόνο προσωπικά δεδομένα αλλά και την εθνική ασφάλεια, εμπλέκοντας δυνητικά βασικές υποδομές ή διαβαθμισμένες πληροφορίες. Η διαφύλαξη των προσωπικών δεδομένων μετατρέπεται κατά συνέπεια σε ζήτημα εθνικής ασφάλειας, συγχωνεύοντας το ατομικό απόρρητο με το πρωταρχικό καθήκον της διατήρησης της κοινωνικής σταθερότητας.

1.3. Σημασία της έρευνας

Αυτή η έρευνα είναι ζωτικής σημασίας καθώς αντιμετωπίζει το πιεστικό ζήτημα της προστασίας των προσωπικών δεδομένων στον δημόσιο τομέα. Καθώς οι κυβερνητικές οντότητες εξαρτώνται όλο και περισσότερο από τις ψηφιακές τεχνολογίες, οι κίνδυνοι που σχετίζονται με παραβιάσεις δεδομένων, παράνομη πρόσβαση και κατάχρηση κλιμακώνονται. Είναι επιτακτική ανάγκη για τα δημόσια ιδρύματα να προστατεύουν τα προσωπικά δεδομένα για να διασφαλίζουν τη νομική συμμόρφωση και να υποστηρίζουν την εμπιστοσύνη του κοινού⁵. Οι κυβερνήσεις επιβλέπουν ευαίσθητες πληροφορίες, όπως αρχεία υγειονομικής περίθαλψης, οικονομικά δεδομένα και στοιχεία ταυτότητας, καθιστώντας τις ισχυρές διαδικασίες προστασίας δεδομένων απαραίτητες για την αποφυγή βλάβης σε άτομα και κοινωνία.

Σε αντίθεση με τον ιδιωτικό τομέα, όπου οικονομικά κίνητρα ωθούν την προστασία των δεδομένων, οι δημόσιοι φορείς καλούνται να συμβιβάσουν την ασφάλεια με τη διαφάνεια και τη δημόσια ευθύνη. Αυτή η μελέτη εξετάζει πώς οι δημόσιες οντότητες διαχειρίζονται αυτές τις αντιφατικές απαιτήσεις διατηρώντας παράλληλα την αποτελεσματική παροχή υπηρεσιών. Εντοπίζοντας κρίσιμες ανησυχίες και λύσεις, παρέχει πληροφορίες για τη βελτίωση των πλαισίων προστασίας δεδομένων διατηρώντας παράλληλα τη λειτουργική αποτελεσματικότητα.

Αυτή η έρευνα είναι απαραίτητη λόγω του μεταβαλλόμενου νομικού πλαισίου, που περιλαμβάνει τον GDPR και τους εθνικούς κανονισμούς. Καθώς οι κανονισμοί περί απορρήτου δεδομένων εντείνονται, οι δημόσιοι οργανισμοί πρέπει να προσαρμοστούν στις νομικές απαιτήσεις και στην ταχεία τεχνολογική πρόοδο. Η αξιολόγηση των τεχνικών συμμόρφωσής τους θα επιτρέψει στους υπεύθυνους χάραξης πολιτικής και στους διαχειριστές να εκτελέσουν πιο αποτελεσματικά μέτρα.

Η έρευνα εξετάζει επίσης τους κλιμακούμενους κινδύνους κυβερνοασφάλειας που αντιμετωπίζουν οι κυβερνητικές οντότητες. Οι δημόσιες βάσεις δεδομένων είναι πρωταρχικοί στόχοι για επιθέσεις στον κυβερνοχώρο, που ενδέχεται να οδηγήσουν σε κλοπή ταυτότητας, διακοπές υπηρεσιών ή συμβιβασμούς της εθνικής ασφάλειας. Αυτό το έργο θα προσφέρει μεθόδους για την ενίσχυση της ανθεκτικότητας των δημόσιων ιδρυμάτων έναντι των επιθέσεων στον κυβερνοχώρο, εξετάζοντας τα τρέχοντα μέτρα.

Η μελέτη διερευνά τελικά τις ευρύτερες επιπτώσεις της προστασίας δεδομένων στην εμπιστοσύνη του κοινού. Η ανεπαρκής ασφάλεια μπορεί να υπονομεύσει την εμπιστοσύνη των πολιτών στους κυβερνητικούς θεσμούς, επηρεάζοντας την ετοιμότητά τους να χρησιμοποιήσουν τις δημόσιες υπηρεσίες. Η κατανόηση της σχέσης μεταξύ προστασίας δεδομένων και εμπιστοσύνης θα επιτρέψει στις κυβερνήσεις να ενισχύσουν τη διαφάνεια και να ενισχύσουν την κοινωνική διακυβέρνηση.

⁵ Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25(4), 307–317. <https://doi.org/10.1016/j.clsr.2009.05.001>

Κεφάλαιο 2: Νομικό Πλαίσιο για την Προστασία Δεδομένων στον Δημόσιο Τομέα

2.1. Γενικές Αρχές του Δικαίου Προστασίας Δεδομένων

2.1.1. Θεμελιώδεις αρχές

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων ορίζει ένα πλαίσιο θεμελιωδών αρχών που ρυθμίζουν τον νόμιμο και ηθικό χειρισμό των προσωπικών δεδομένων. Οι αρχές που περιγράφονται στο Άρθρο 5 του GDPR αποτελούν το κανονιστικό θεμέλιο για όλες τις δραστηριότητες επεξεργασίας δεδομένων, ιδίως στον δημόσιο τομέα, όπου η εξουσία του κράτους να συλλέγει και να επεξεργάζεται προσωπικά δεδομένα πρέπει να συμβιβάζεται με τα ατομικά δικαιώματα.

Η πρωταρχική αρχή είναι η νομιμότητα, η δικαιοσύνη και η διαφάνεια, γεγονός που απαιτεί τα προσωπικά δεδομένα να αντιμετωπίζονται με νομικά δικαιολογημένο τρόπο, ο οποίος να είναι επίσης σαφής και κατανοητός για το υποκείμενο των δεδομένων⁶. Οι δημόσιοι φορείς υποχρεούνται, κατά συνέπεια, να ενημερώνουν τα άτομα σχετικά με τους στόχους της συλλογής δεδομένων και τη νομική βάση που υποστηρίζει την εν λόγω επεξεργασία. Η έννοια του περιορισμού του σκοπού απαγορεύει την επεξεργασία προσωπικών δεδομένων για σκοπούς πέραν αυτών που αναφέρθηκαν αρχικά, εκτός εάν αποδεικνύεται επαρκής νομική βάση.

Η έννοια της ελαχιστοποίησης των δεδομένων υποχρεώνει τις δημόσιες αρχές να εγγυώνται ότι τα συλλεγόμενα δεδομένα είναι επαρκή, σχετικά και περιορίζονται σε ό,τι είναι απαραίτητο για τον καθορισμένο σκοπό. Αυτό σχετίζεται με την έννοια της ακρίβειας, η οποία απαιτεί τα προσωπικά δεδομένα να διατηρούνται ενημερωμένα και να διορθώνονται άμεσα μετά την ανακάλυψη ανακρίβειών.

Η έννοια του περιορισμού της αποθήκευσης είναι εξίσου σημαντική. Αυτή η έννοια περιορίζει τη διατήρηση των προσωπικών δεδομένων στη διάρκεια που είναι απαραίτητη για την επίτευξη του επιδιωκόμενου σκοπού, σύμφωνα με τις νομικές απαιτήσεις αρχειοθέτησης ή με λόγους δημόσιου συμφέροντος. Στον ελληνικό δημόσιο τομέα, οι εντολές διατήρησης αρχείων μπορούν να απορρέουν από εθνικούς νόμους που διέπουν τη διαφάνεια και τη δημόσια λογοδοσία.

Επιπλέον, οι αρχές της ακεραιότητας και της εμπιστευτικότητας επιβάλλουν στους υπεύθυνους επεξεργασίας δεδομένων να χρησιμοποιούν κατάλληλα τεχνικά και οργανωτικά μέσα για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, ακούσια απώλεια ή καταστροφή. Αυτή η ευθύνη επιβάλλει την άμεση ειδοποίηση παραβιάσεων προσωπικών δεδομένων στην εποπτική αρχή, γενικά εντός 72 ωρών, όπως ορίζεται στο Άρθρο 33 του ΓΚΠΔ και αντικατοπτρίζεται στις ελληνικές νομικές ερμηνείες και σχόλια⁷.

Η αρχή της λογοδοσίας υποχρεώνει τους δημόσιους φορείς να τηρούν αυτά τα πρότυπα και να επαληθεύουν τη συμμόρφωσή τους μέσω τεκμηρίωσης, εσωτερικών ελέγχων και, όπου εφαρμόζεται, του διορισμού Υπεύθυνου Προστασίας Δεδομένων. Αυτό το κανονιστικό κριτήριο απαιτεί κάτι περισσότερο από απλή διαδικαστική συμμόρφωση· απαιτεί μια κουλτούρα

⁶ Νόμος 4624/2019 (Κωδικοποιημένος)—ΦΕΚ Α 137/29.08.2019. (n.d.). Retrieved 12 May 2025, from <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>

⁷ Νόμος 4624/2019. (2019, August 31). Lawspot. <https://www.lawspot.gr/node/265098>

λογοδοσίας εντός της δημόσιας διοίκησης σχετικά με τη διαχείριση των προσωπικών δεδομένων των πολιτών.

2.1.2. Νομική βάση για την επεξεργασία στη δημόσια διοίκηση

Οι φορείς της δημόσιας διοίκησης, που είναι υπεύθυνοι για τη διαχείριση εκτεταμένων δεδομένων, πρέπει να λειτουργούν εντός ενός αυστηρά καθορισμένου νομικού πλαισίου για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το άρθρο 6(1)(ε) του ΓΚΠΔ ορίζει ότι η νόμιμη βάση για την επεξεργασία πληρούται όταν είναι «απαραίτητη για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή για την εκτέλεση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας». Αυτή η διάταξη είναι ιδιαίτερα σημαντική για τη διακυβέρνηση δεδομένων του δημόσιου τομέα, καθώς νομιμοποιεί πολλές κρατικές αρμοδιότητες - όπως οι φόροι, η υγειονομική περίθαλψη, η επιβολή του νόμου και η δημόσια ασφάλεια - εάν αυτά τα καθήκοντα βασίζονται στο δίκαιο της ΕΕ ή στην εθνική νομοθεσία.

Στην Ελλάδα, ο νόμος 4624/2019 θεσπίζει τον ΓΚΠΔ σε εθνικό επίπεδο, προσφέροντας την απαραίτητη νομοθετική σαφήνεια, συμπεριλαμβανομένων των εγγυήσεων, των εξαιρέσεων και των περιορισμών ανά τομέα. Το ελληνικό νομοθετικό πλαίσιο οριοθετεί το πεδίο εφαρμογής των πράξεων επεξεργασίας που επιτρέπονται για σκοπούς δημόσιου συμφέροντος⁸. Το άρθρο 33 του ΓΚΠΔ, όπως διευκρινίζεται από την ελληνική νομοθεσία και τα σχετικά σχόλια, ορίζει ότι οι δημόσιες αρχές ειδοποιούν άμεσα την Ελληνική Αρχή Προστασίας Δεδομένων για παραβιάσεις δεδομένων. Ο υπεύθυνος επεξεργασίας πρέπει να αξιολογήσει τον πιθανό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων και να ανταποκριθεί κατάλληλα, προσφέροντας ολοκληρωμένες περιγραφές της φύσης της παραβίασης, τις πιθανές συνέπειες και τα διορθωτικά μέτρα που έχουν ληφθεί.

Η εξάρτηση από το Άρθρο 6(1)(ε) απαιτεί από τους δημόσιους οργανισμούς να οριοθετούν ρητά τη νομική εξουσία που διέπει κάθε δραστηριότητα επεξεργασίας⁹. Αυτό περιλαμβάνει την τήρηση των συνταγματικών αρχών, ορισμένων νομοθετικών εξουσιοδοτήσεων και γενικών στόχων δημόσιας πολιτικής. Το ελληνικό νομικό σύστημα, που βασίζεται στο αστικό δίκαιο και στους κανόνες που προέρχονται από την ΕΕ, ορίζει την αναλογικότητα και την αναγκαιότητα ως βασικά κριτήρια για τη νόμιμη άσκηση διοικητικής εξουσίας σχετικά με τα προσωπικά δεδομένα.

Επιπλέον, όταν τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία για σκοπούς δημόσιου συμφέροντος, ο ΓΚΠΔ επιτρέπει συγκεκριμένες εξαιρέσεις από τα ατομικά δικαιώματα, αλλά μόνο στο βαθμό που κρίνεται κατάλληλος σε μια δημοκρατική κοινωνία και όπως ορίζεται στην εθνική νομοθεσία. Αυτοί οι περιορισμοί μπορεί να αφορούν τις απαιτήσεις διαφάνειας, τα δικαιώματα πρόσβασης ή διαγραφής ή την υποχρέωση ειδοποίησης των υποκειμένων των δεδομένων για παραβιάσεις, ιδίως σε πλαίσια που αφορούν τη δημόσια ασφάλεια, ποινικές έρευνες ή ανθρωπιστικά ζητήματα. Η ελληνική νομοθεσία αντικατοπτρίζει αυτήν την αρχή ενσωματώνοντας εγγυήσεις στις διοικητικές διαδικασίες και τα συστήματα δικαστικής παρακολούθησης για τη διατήρηση μιας κατάλληλης ισορροπίας μεταξύ δημόσιας εξουσίας και ιδιωτικής ζωής.

⁸ Νόμος 4624/2019 (Κωδικοποιημένος)—ΦΕΚ Α 137/29.08.2019. (n.d.). Retrieved 12 May 2025, from <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>

⁹ Άρθρο 6—Γενικός κανονισμός για την προστασία δεδομένων—Νομιμότητα της επεξεργασίας. (2016, May 7). Lawspot. <https://www.lawspot.gr/node/67400>

2.2. Ο ΓΚΠΔ και η νομική εφαρμογή του στον δημόσιο τομέα

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), που ισχύει από τον Μάιο του 2018, θεσπίζει ένα υποχρεωτικό νομικό πλαίσιο για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ευρωπαϊκή Ένωση, επηρεάζοντας ιδιαίτερα τους δημόσιους φορείς¹⁰. Αυτοί οι φορείς συχνά διαχειρίζονται ευαίσθητες πληροφορίες, συμπεριλαμβανομένων δεδομένων υγείας, φορολογίας ή κοινωνικών υπηρεσιών, καθιστώντας τους ιδιαίτερα υπόλογους βάσει των θεμελιωδών αρχών του GDPR. Αυτές περιλαμβάνουν τη νομιμότητα, την ισότητα και τη σαφήνεια, τον περιορισμό του σκοπού, την ελαχιστοποίηση των δεδομένων, την ακρίβεια, τον περιορισμό της διατήρησης, την ακεραιότητα και το απόρρητο, και τη λογοδοσία. Στη δημόσια διοίκηση, η τήρηση αυτών των αρχών είναι υποχρεωτική και νομικά δεσμευτική. Η αρχή της νομιμότητας διέπει όλες τις δραστηριότητες επεξεργασίας, οι οποίες πρέπει να τεκμηριώνονται από μία από τις νομικές βάσεις που ορίζονται στο Άρθρο 6(1) του GDPR - ιδίως στο στοιχείο (ε), το οποίο επιτρέπει την επεξεργασία που είναι απαραίτητη για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας¹¹. Στο ελληνικό πλαίσιο, η παρούσα ρήτρα αναλύεται από την εσωτερική νομοθεσία και την ειδική ανά τομέα νομοθεσία, η οποία οριοθετεί τις παραμέτρους της επιτρεπόμενης επεξεργασίας από δημόσιους φορείς. Η διαφάνεια και η λογοδοσία απαιτούν από τους δημόσιους οργανισμούς να αναφέρουν ρητά τις μεθόδους και το σκεπτικό πίσω από τη συλλογή, αποθήκευση και επεξεργασία προσωπικών δεδομένων, ενώ παράλληλα να θεσπίζουν κατάλληλους τεχνικούς και οργανωτικούς μηχανισμούς για τη διασφάλιση της συμμόρφωσης. Η απαίτηση ορισμού Υπεύθυνου Προστασίας Δεδομένων (DPO), υποχρεωτική για τις δημόσιες αρχές όπως ορίζεται στο Άρθρο 37 του ΓΚΠΔ, καταδεικνύει αυτήν την αναγκαιότητα.¹² Ο Υπεύθυνος Προστασίας Δεδομένων είναι υπεύθυνος για την εποπτεία των εσωτερικών πρωτοβουλιών προστασίας δεδομένων, τη διασφάλιση της νομικής συμμόρφωσης και τη λειτουργία του ως ενδιάμεσος μεταξύ του οργανισμού, των ατόμων και των ρυθμιστικών αρχών. Ο ΓΚΠΔ επιβάλλει αυστηρές υποχρεώσεις αναφοράς παραβιάσεων: σε περίπτωση παραβίασης δεδομένων, οι δημόσιοι φορείς πρέπει να ειδοποιούν τις αρμόδιες αρχές (στην Ελλάδα, τις ελληνικές αρχές προστασίας δεδομένων) εντός 72 ωρών, εκτός εάν η παραβίαση θεωρείται απίθανο να αποτελέσει απειλή για τα δικαιώματα και τις ελευθερίες των ατόμων. Αυτή η διάταξη, που περιγράφεται στο Άρθρο 33 του ΓΚΠΔ και διευκρινίζεται σε εθνικές ερμηνείες, ενσωματώνει την έννοια της λογοδοσίας και είναι κρίσιμη για την ενίσχυση της εμπιστοσύνης στις δημόσιες υπηρεσίες.

Οι θεσμοί της δημόσιας διοίκησης είναι νομικά υποχρεωμένοι να εγγυώνται ότι κάθε επεξεργασία προσωπικών δεδομένων βασίζεται σε νόμιμη νομική βάση. Το Άρθρο 6(1)(ε) του ΓΚΠΔ είναι απαραίτητο, καθώς επιτρέπει την επεξεργασία όταν είναι «απαραίτητη για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την εκτέλεση δημόσιας εξουσίας». Αυτή η νομική βάση είναι ιδιαίτερα σημαντική για κυβερνητικές υπηρεσίες, δήμους, εκπαιδευτικά ιδρύματα και παρόχους υγειονομικής περίθαλψης που λειτουργούν βάσει της

¹⁰ Άρθρο 33—Γενικός κανονισμός για την προστασία δεδομένων—Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή. (2016, May 7). Lawspot. <https://www.lawspot.gr/node/67427>

¹¹ Άρθρο 6—Γενικός κανονισμός για την προστασία δεδομένων—Νομιμότητα της επεξεργασίας. (2016, May 7). Lawspot. <https://www.lawspot.gr/node/67400>

¹² Vollmer, N. (2023, April 4). Άρθρο 37 ee γενικός κανονισμός για την προστασία δεδομένων [Text]. <https://www.privacy-regulation.eu/el/37.htm>

εθνικής νομοθεσίας¹³. Τα ελληνικά νομοθετικά εργαλεία οριοθετούν και περιορίζουν περαιτέρω τις παραμέτρους αυτών των ευθυνών δημόσιου συμφέροντος, διασφαλίζοντας ότι η επεξεργασία δεδομένων είναι εύλογη και επιτρεπτή. Ο ΓΚΠΔ ορίζει ότι η επεξεργασία πρέπει να συμμορφώνεται με τον περιορισμό του σκοπού και την ελαχιστοποίηση των δεδομένων, ορίζοντας ότι οι δημόσιοι οργανισμοί μπορούν να συλλέγουν μόνο δεδομένα που είναι απαραίτητα για τους ρητά καθορισμένους νομικούς στόχους και να τα διατηρούν όχι περισσότερο από όσο είναι απαραίτητο.

Εκτός από την ΕΕ, ένα αναπτυσσόμενο πλαίσιο διεθνών κανόνων περί απορρήτου δεδομένων επηρεάζει επίσης τις λειτουργίες του δημόσιου τομέα¹⁴. Νομοθεσία όπως ο Νόμος περί Προστασίας Προσωπικών Δεδομένων της Καλιφόρνια (CCPA), ο LGPD της Βραζιλίας, ο APPI της Ιαπωνίας και ο Νόμος περί Προστασίας Προσωπικών Δεδομένων Ψηφιακών Δεδομένων της Ινδίας αποτελεί παράδειγμα μιας παγκόσμιας στροφής προς αυστηρότερη ρύθμιση και ενισχυμένη λογοδοσία. Παρά τις διαφορές στα νομικά πλαίσια και τους μηχανισμούς επιβολής, όλα αυτά τα συστήματα επιβάλλουν πρότυπα που αντικατοπτρίζουν τις θεμελιώδεις αρχές του ΓΚΠΔ - νόμιμη βάση για την επεξεργασία, διαφάνεια, δικαιώματα των υποκειμένων των δεδομένων και μέτρα ασφαλείας. Οι δημόσιοι οργανισμοί που λειτουργούν σε διάφορες δικαιοδοσίες ή διαχειρίζονται δεδομένα αλλοδαπών πρέπει να επαληθεύουν ότι οι δραστηριότητές τους συμμορφώνονται με τον ΓΚΠΔ και τα σχετικά διεθνή πλαίσια, ιδίως κατά τη διάρκεια της διεθνούς συνεργασίας ή των διασυνοριακών μεταφορών δεδομένων. Η παραμέληση της συμμόρφωσης μπορεί να οδηγήσει σε νομική ευθύνη, βλάβη στη φήμη ή διακοπή των μεταφορών δεδομένων. Σε αυτό το περιβάλλον, η τήρηση από τον δημόσιο τομέα τόσο των τοπικών όσο και των διεθνών κανονισμών προστασίας δεδομένων δεν αποτελεί απλώς μια νομοθετική υποχρέωση, αλλά μια θεμελιώδη απαίτηση για νόμιμη, ηθική και ασφαλή διακυβέρνηση δεδομένων.

2.3. Ελληνική Εθνική Νομοθεσία για την Προστασία Δεδομένων

2.3.1. Επισκόπηση της ελληνικής νομοθεσίας για την προστασία δεδομένων

Το ελληνικό νομικό πλαίσιο για την προστασία δεδομένων ορίζεται κυρίως από τον Νόμο 4624/2019, ο οποίος θεσπίστηκε για την εναρμόνιση της εθνικής νομοθεσίας με τον GDPR της Ευρωπαϊκής Ένωσης και την Οδηγία για την Επιβολή του Νόμου (2016/680). Η νομοθεσία αυτή θεσπίζει τη βάση για την προστασία των προσωπικών δεδομένων στην Ελλάδα, ορίζοντας σαφείς απαιτήσεις για τον χειρισμό προσωπικών δεδομένων από δημόσιους και εμπορικούς φορείς. Ο κύριος στόχος του Νόμου 4624/2019 είναι να διασφαλίσει τη συμμόρφωση της Ελλάδας με τις εντολές του GDPR, διαφυλάσσοντας έτσι την ατομική ιδιωτικότητα και διασφαλίζοντας τον εξουσιοδοτημένο χειρισμό προσωπικών δεδομένων¹⁵.

Ο Νόμος 4624/2019 επιδιώκει να θεσπίσει ένα ολιστικό εθνικό πλαίσιο για την προστασία δεδομένων ενσωματώνοντας πολλαπλές οδηγίες της ΕΕ στην ελληνική νομοθεσία, που περιλαμβάνουν τις διατάξεις του GDPR και της Οδηγίας για την Επιβολή του Νόμου. Ο νόμος αυτός ορίζει τις υποχρεώσεις του δημόσιου τομέα, των επιχειρηματικών οντοτήτων και των υποκειμένων των δεδομένων σχετικά με την προστασία των προσωπικών δεδομένων,

¹³ Dove, E. S. (2018). The eu general data protection regulation: Implications for international scientific research in the digital era. *Journal of Law, Medicine & Ethics*, 46(4), 1013–1030. <https://doi.org/10.1177/1073110518822003>

¹⁴ Kiesow Cortez, E. (2021). Data protection around the world: An introduction. In E. Kiesow Cortez (Ed.), *Data Protection Around the World: Privacy Laws in Action* (pp. 1–6). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-407-5_1

¹⁵ Νόμος 4624/2019 (Κωδικοποιημένος)—ΦΕΚ Α 137/29.08.2019. (n.d.). Retrieved 12 May 2025, from <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>

αντικατοπτρίζοντας το γενικό κανονιστικό πλαίσιο της Ευρωπαϊκής Ένωσης. Η ουσιαστική πτυχή του νόμου είναι οι ολοκληρωμένες διατάξεις του για την οργάνωση και τη λειτουργία της Ελληνικής Αρχής Προστασίας Δεδομένων, η οποία είναι υπεύθυνη για τη διασφάλιση της τήρησης των προτύπων προστασίας δεδομένων. Η νομοθεσία οριοθετεί τις λειτουργίες και τις υποχρεώσεις των υπευθύνων επεξεργασίας δεδομένων, των επεξεργαστών και των ΥΠΔ, θεσπίζοντας παράλληλα αυστηρά πρότυπα για τη διαφανή διαχείριση των προσωπικών δεδομένων των ατόμων σύμφωνα με τα δικαιώματά τους βάσει του ΓΚΠΔ.

2.3.2. Ειδικές νομικές διατάξεις για τον δημόσιο τομέα

Ο δημόσιος τομέας στην Ελλάδα υπόκειται σε συγκεκριμένες νομικές διατάξεις σχετικά με την προστασία δεδομένων, όπως ορίζεται στον Νόμο 4624/2019 και την αλληλεπίδρασή του με άλλη σχετική νομοθεσία. Η νομοθεσία ορίζει τις υποχρεώσεις των οργανισμών του δημόσιου τομέα που χειρίζονται προσωπικά δεδομένα, συμπεριλαμβανομένου του υποχρεωτικού ορισμού ΥΠΔ εντός αυτών των φορέων¹⁶. Οι δημόσιοι φορείς στην Ελλάδα είναι υπεύθυνοι για την προστασία των προσωπικών δεδομένων, ώστε να διασφαλίζεται η προστασία των δικαιωμάτων απορρήτου των ατόμων, επιτρέποντας παράλληλα την εκτέλεση των δημόσιων καθηκόντων τους.

Οι φορείς του δημόσιου τομέα μπορούν να επεξεργάζονται προσωπικά δεδομένα μόνο όταν η επεξεργασία αυτή είναι απαραίτητη για την εκπλήρωση νομικών καθηκόντων ή για την εκτέλεση εργασίας προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας. Κατά συνέπεια, οι δημόσιοι φορείς περιορίζονται στις κατηγορίες προσωπικών δεδομένων που μπορούν να συλλέγουν και να διαχειρίζονται, δίνοντας προτεραιότητα στην αναγκαιότητα και την αναλογικότητα. Οι δημόσιοι φορείς πρέπει να συμμορφώνονται με αυστηρές απαιτήσεις διαφάνειας, διασφαλίζοντας ότι τα άτομα ενημερώνονται πλήρως για τους στόχους της επεξεργασίας δεδομένων, τις διάρκειες διατήρησης και τα νόμιμα δικαιώματά τους.

Επιπλέον, οι δημόσιοι φορείς υποχρεούνται να παρέχουν στο κοινό μια διαφανή διαδικασία για την άσκηση των δικαιωμάτων προστασίας δεδομένων, συμπεριλαμβανομένης της πρόσβασης σε προσωπικά δεδομένα, της διόρθωσης, της διαγραφής και της αντίρρησης στην επεξεργασία. Οι επιχειρήσεις του δημόσιου τομέα υποχρεούνται να διαθέτουν συστήματα για την αναφορά παραβιάσεων δεδομένων εντός 72 ωρών από την ανακάλυψή τους, σύμφωνα με τον ΓΚΠΔ και τον Νόμο 4624/2019.

Μια σημαντική διάταξη της ελληνικής νομοθεσίας περί προστασίας δεδομένων για τον δημόσιο τομέα είναι η υποχρέωση ορισμού ΥΠΔ σε δημόσιους φορείς. Ο Υπεύθυνος Προστασίας Δεδομένων εγγυάται την τήρηση της νομοθεσίας περί προστασίας δεδομένων, παρέχει συμβουλές σχετικά με τις ευθύνες προστασίας δεδομένων και αξιολογεί την αποτελεσματικότητα των μέτρων απορρήτου εντός των φορέων του δημόσιου τομέα¹⁷. Ο ΥΠΔ λειτουργεί ως σύνδεσμος μεταξύ του φορέα του δημόσιου τομέα και της Ελληνικής Αρχής Προστασίας Δεδομένων. Σε πολλές περιπτώσεις, ένας μόνος Υπεύθυνος Προστασίας Δεδομένων μπορεί να επιβλέπει τα πρωτόκολλα προστασίας δεδομένων διαφόρων δημόσιων φορέων, ανάλογα με το μέγεθος και τη δομή του φορέα.

Επιπλέον, οι δημόσιοι φορείς υποχρεούνται να αξιολογούν και να βελτιώνουν με συνέπεια τα πρωτόκολλα προστασίας δεδομένων τους. Αυτό είναι ιδιαίτερα σημαντικό για τους κλάδους

¹⁶ Νόμος 4624/2019 (Κωδικοποιημένος)—ΦΕΚ Α 137/29.08.2019. (n.d.). Retrieved 12 May 2025, from <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>

¹⁷ Άρθρο 33—Γενικός κανονισμός για την προστασία δεδομένων—Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή. (2016, May 7). Lawspot. <https://www.lawspot.gr/node/67427>

που διαχειρίζονται σημαντικές ποσότητες ευαίσθητων προσωπικών πληροφοριών, όπως η υγειονομική περίθαλψη, οι κοινωνικές υπηρεσίες και οι υπηρεσίες επιβολής του νόμου. Οι δημόσιοι φορείς πρέπει να διενεργούν συχνές εκτιμήσεις αντικτύπου στην προστασία δεδομένων (ΕΕΠΔ) για να αξιολογούν τους κινδύνους που συνδέονται με την επεξεργασία προσωπικών δεδομένων, ειδικά όταν εφαρμόζονται νέες δραστηριότητες επεξεργασίας δεδομένων.

2.3.3. Συνοχή και ενότητα της ελληνικής νομοθεσίας

Το ελληνικό πλαίσιο προστασίας δεδομένων επηρεάζεται κυρίως από τον ΓΚΠΔ και τον Νόμο 4624/2019, με στόχο τη θέσπιση μιας συνεκτικής και ομοιόμορφης νομοθετικής προσέγγισης για την προστασία των προσωπικών δεδομένων. Παρ' όλα αυτά, η εφαρμογή αυτών των νόμων στην πράξη προκαλεί ερωτήματα σχετικά με την αλληλεπίδρασή τους με άλλους εθνικούς νόμους και κανονισμούς, ιδίως στον δημόσιο τομέα.

Η σύνδεση μεταξύ του Νόμου 4624/2019 και άλλων ελληνικών νομικών μέτρων θα πρέπει, θεωρητικά, να είναι αρμονική, με την εθνική νομοθεσία που συμμορφώνεται με τις απαιτήσεις της ΕΕ¹⁸. Στην πράξη, η ελληνική νομοθεσία για την προστασία δεδομένων περιστασιακά διασταυρώνεται με συγκεκριμένους εθνικούς κανονισμούς που επιβλέπουν τομείς όπως η εθνική ασφάλεια, η επιβολή του νόμου και η δημόσια υγεία. Η εφαρμογή των κανόνων προστασίας δεδομένων που αφορούν την αστυνομία και τις δικαστικές οντότητες μπορεί να είναι περίπλοκη, ειδικά κατά τον χειρισμό ευαίσθητων πληροφοριών που χρησιμοποιούνται σε ποινικές έρευνες ή νομικές διαδικασίες.

Η σύγκλιση της νομοθεσίας για την προστασία δεδομένων με άλλα εθνικά νομικά πλαίσια μπορεί να δημιουργήσει σύγκρουση μεταξύ της επιτακτικής ανάγκης για την προστασία των προσωπικών δεδομένων και της ανάγκης για την τήρηση της δημόσιας ασφάλειας, της επιβολής του νόμου και άλλων κυβερνητικών συμφερόντων. Σε ορισμένες περιπτώσεις, το ελληνικό νομικό σύστημα προσπαθεί να συμβιβάσει τα ατομικά δικαιώματα απορρήτου με το δημόσιο συμφέρον στην εθνική ασφάλεια, την αποτροπή του εγκλήματος και τη δημόσια υγεία¹⁹. Η Οδηγία για την Επιβολή του Νόμου επιτρέπει στις υπηρεσίες επιβολής του νόμου να επεξεργάζονται προσωπικά δεδομένα υπό ορισμένες προϋποθέσεις, συνήθως παρέχοντάς τους μεγαλύτερη ευελιξία από άλλους οργανισμούς του δημόσιου τομέα, όπως οι πάροχοι υγειονομικής περίθαλψης.

Ένας άλλος τομέας στον οποίο η ελληνική νομοθεσία ενδέχεται να αντιμετωπίσει δυσκολίες στη διατήρηση της συνοχής είναι ο τομέας των δημόσιων μητρώων. Οι υπηρεσίες του δημόσιου τομέα στην Ελλάδα έχουν νομική υποχρέωση να τηρούν μητρώα που περιέχουν ευαίσθητα προσωπικά δεδομένα, συμπεριλαμβανομένων των κτηματολογίων, των ληξιαρχικών αρχείων και των φορολογικών πληροφοριών. Αυτά τα μητρώα ενδέχεται να τηρούν ποικίλους κανονισμούς σχετικά με την πρόσβαση, τη διατήρηση και την κοινοποίηση δεδομένων, με αποτέλεσμα πιθανές συγκρούσεις μεταξύ των γενικών αρχών απορρήτου του ΓΚΠΔ και των συγκεκριμένων εντολών άλλων νόμων που διέπουν την πρόσβαση του κοινού σε τέτοια αρχεία. Η πρόσβαση στα μητρώα πρέπει να ρυθμίζεται σχολαστικά για να διασφαλίζεται η τήρηση της νομοθεσίας περί απορρήτου δεδομένων, ικανοποιώντας παράλληλα το δικαίωμα του κοινού στην ενημέρωση.

Παρά τις πιθανές αυτές αντιφάσεις, η ελληνική νομοθεσία περί προστασίας δεδομένων στοχεύει στη διατήρηση της συνοχής δίνοντας προτεραιότητα στους κανόνες του ΓΚΠΔ. Ο νόμος 4624/2019 ενσωματώνει τη νομοθεσία της ΕΕ και εισάγει συμπληρωματικά μέτρα για την

¹⁸ Νόμος 4624/2019. (2019, August 31). Lawspot. <https://www.lawspot.gr/node/265098>

αποσαφήνιση των λειτουργιών των ιδρυμάτων του δημόσιου τομέα και την ενίσχυση της διαφάνειας στις δραστηριότητες επεξεργασίας δεδομένων. Αυτό διευκολύνει τη δημιουργία μιας πιο συνεκτικής δομής, την οποία μπορούν να διασχίσουν πιο εύκολα τόσο οι κυβερνητικοί φορείς όσο και οι εμπορικές επιχειρήσεις.

Επιπλέον, το ελληνικό νομικό πλαίσιο προωθεί μια ενιαία στρατηγική για την προστασία των δεδομένων, υποχρεώνοντας τους δημόσιους φορείς να ορίζουν ΥΠΔ, οι οποίοι είναι καθοριστικοί για τη διασφάλιση της συμμόρφωσης σε διάφορους τομείς. Αυτό εγγυάται ότι, παρά τις πιθανές εντάσεις μεταξύ διαφόρων κανονισμών, υπάρχει ένα οριστικό σημείο λογοδοσίας για την προστασία των δεδομένων εντός των φορέων του δημόσιου τομέα, συμβάλλοντας στον μετριασμό των συγκρούσεων και στη διατήρηση ενός συνεκτικού νομικού πλαισίου.

Κεφάλαιο 3: Θεσμικές και τεχνολογικές πτυχές της προστασίας δεδομένων

3.1. Διακυβέρνηση δεδομένων σε δημόσια ιδρύματα

3.1.1. Οργανωτικές δομές για την προστασία των δεδομένων

Οι οργανωτικές δομές προστασίας δεδομένων είναι απαραίτητες για τις επιχειρήσεις του δημόσιου τομέα ώστε να χειρίζονται και να προστατεύουν τα προσωπικά δεδομένα σύμφωνα με τους σχετικούς νόμους και κανονισμούς²⁰. Αυτά τα πλαίσια οριοθετούν τα καθήκοντα, τις ευθύνες και τις διαδικασίες που πρέπει να χρησιμοποιούν οι οργανισμοί για την προστασία των προσωπικών πληροφοριών ενώ παρέχουν σημαντικές υπηρεσίες στο κοινό. Στον δημόσιο τομέα, όπου η διαχείριση των προσωπικών δεδομένων είναι συχνά περίπλοκη και πολυσχιδής, οι οργανωτικές δομές που οριοθετούνται με σαφήνεια είναι ζωτικής σημασίας για την αντιμετώπιση των ζητημάτων που παρουσιάζουν οι εντολές προστασίας δεδομένων και ιδιωτικότητας.

Το θεμέλιο της αποτελεσματικής προστασίας δεδομένων σε οργανισμούς του δημόσιου τομέα είναι ο διορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ - DPO)²¹. Ο Υπεύθυνος Προστασίας Δεδομένων είναι απαραίτητος για την παρακολούθηση της συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων, ενεργώντας ως σύνδεσμος για εσωτερικά και εξωτερικά μέρη και για τη διασφάλιση της συμμόρφωσης του οργανισμού με κανόνες όπως ο GDPR. Ο ΥΠΔ είναι υπεύθυνος για την εκτέλεση αξιολογήσεων επιπτώσεων στην προστασία δεδομένων, την επίβλεψη της τήρησης των πολιτικών προστασίας δεδομένων και την παροχή πρωτοβουλιών κατάρτισης και ευαισθητοποίησης για τους εργαζόμενους²². Ο ΥΠΔ υποχρεούται επίσης να αναφέρει στην ανώτατη διοίκηση για θέματα προστασίας δεδομένων, διασφαλίζοντας ότι η ηγεσία παραμένει ενημερωμένη και εμπλέκεται σε δραστηριότητες προστασίας δεδομένων. Η ανεξαρτησία και η εξουσία του ΥΠΔ εντός του οργανισμού είναι ουσιαστικής σημασίας για την αποτελεσματικότητα των πρωτοβουλιών προστασίας δεδομένων, επιτρέποντας στον υπάλληλο να λειτουργεί αμερόληπτα και να υπερασπίζεται τα δικαιώματα των υποκειμένων των δεδομένων.

Παράλληλα με το διορισμό ενός ΥΠΔ, οι οντότητες του δημόσιου τομέα πρέπει να διαθέτουν ρητά πλαίσια διακυβέρνησης που καθορίζουν τους διαύλους πληροφόρησης και λήψης αποφάσεων σχετικά με την προστασία δεδομένων. Αυτό συνήθως συνεπάγεται τη σύσταση μιας εξειδικευμένης επιτροπής προστασίας δεδομένων ή ομάδας εργασίας που αποτελείται από εκπροσώπους από διάφορα τμήματα, συμπεριλαμβανομένων νομικών, συμμόρφωσης, πληροφορικής, ανθρώπινων πόρων και επικοινωνιών²³. Αυτή η διεπιστημονική προσέγγιση εγγυάται την ενσωμάτωση των αρχών προστασίας δεδομένων σε κάθε πτυχή των λειτουργιών του

²⁰ Greco, S., Palmieri, R., & Rigotti, E. (2016). Institutional argumentation and conflict prevention: The case of the swiss federal data protection and information commissioner. *Journal of Pragmatics*, 105, 39–53. <https://doi.org/10.1016/j.pragma.2016.09.014>

²¹ Αναστασία Κολοφωτία, Σ. (2022). *Το διαδίκτυο των πραγμάτων στο δημόσιο τομέα: η μετάβαση στην έξυπνη διακυβέρνηση, εφαρμογές και νομικές προκλήσεις* [Working Paper]. <http://repositoryesdda.ekdd.gr/jspui/handle/123456789/560>

²² Ράμια, Κ. Σ. (2022). *Η τεχνολογία blockchain και η συμβατότητάς της με τον γενικό κανονισμό προστασίας δεδομένων*. <http://dspace.lib.uom.gr/handle/2159/26464>

²³ Ζούνη, Α. (2024). *Η προστασία των δεδομένων υγείας στην εποχή της πανδημίας Covid-19. Η διαχείριση των δεδομένων υγείας από το δημόσιο νοσοκομείο*. <http://dspace.lib.uom.gr/handle/2159/30921>

οργανισμού. Με την προώθηση της διυπηρεσιακής επικοινωνίας, οι οργανισμοί μπορούν να εντοπίζουν αποτελεσματικότερα πιθανούς κινδύνους και ζητήματα που σχετίζονται με την προστασία δεδομένων και να εφαρμόζουν ολοκληρωμένες λύσεις.

Ένα ρητό πλαίσιο διακυβέρνησης δεδομένων είναι ζωτικής σημασίας για τη διασφάλιση ότι τα προσωπικά δεδομένα επεξεργάζονται, αποθηκεύονται και διαδίδονται με ασφάλεια και σύμφωνα με τους κανονισμούς²⁴. Αυτό το πλαίσιο οριοθετεί τους κανόνες, τις μεθόδους και τα πρότυπα για τη διαχείριση δεδομένων εντός του οργανισμού. Τα βασικά στοιχεία ενός ολοκληρωμένου πλαισίου διακυβέρνησης δεδομένων περιλαμβάνουν συστήματα ταξινόμησης δεδομένων, περιορισμούς πρόσβασης δεδομένων και πρωτόκολλα διατήρησης δεδομένων. Κατηγοριοποιώντας τα δεδομένα ανάλογα με την ευαισθησία και τη σημασία τους, οι οργανισμοί μπορούν να δημιουργήσουν κατάλληλα πρωτόκολλα ασφαλείας για την προστασία των προσωπικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και παραβιάσεις²⁵. Οι έλεγχοι πρόσβασης δεδομένων οριοθετούν πρωτόκολλα για τον προσδιορισμό του ποιος μπορεί να έχει πρόσβαση σε συγκεκριμένους τύπους δεδομένων και τις προϋποθέσεις υπό τις οποίες παρέχεται πρόσβαση, διασφαλίζοντας έτσι ότι μόνο εξουσιοδοτημένα άτομα διαχειρίζονται ευαίσθητες πληροφορίες. Οι κανόνες διατήρησης ορίζουν τη διάρκεια για την οποία πρέπει να διατηρούνται τα προσωπικά δεδομένα και τις διαδικασίες για την ασφαλή διαγραφή ή την ανωνυμοποίηση δεδομένων όταν δεν απαιτείται πλέον, μειώνοντας έτσι τον κίνδυνο έκθεσης ή κακής χρήσης.

Οι πρωτοβουλίες κατάρτισης και ευαισθητοποίησης αποτελούν ουσιαστικό στοιχείο των οργανωτικών πλαισίων για την προστασία των δεδομένων²⁶. Οι υπάλληλοι του δημόσιου τομέα πρέπει να ενημερώνονται για τις υποχρεώσεις τους για την προστασία των δεδομένων, συμπεριλαμβανομένης της διαχείρισης των προσωπικών πληροφοριών, τη σημασία της ασφαλείας των δεδομένων και τις πιθανές συνέπειες των παραβιάσεων δεδομένων. Οι συνεπείς εκπαιδευτικές συνεδρίες ενισχύουν μια κουλτούρα προστασίας δεδομένων σε ολόκληρο τον οργανισμό, ωθώντας το προσωπικό να δώσει προτεραιότητα σε ζητήματα απορρήτου στις καθημερινές του ενέργειες. Επιπλέον, ενισχύοντας την κατανόηση των δικαιωμάτων των υποκειμένων των δεδομένων, οι οργανισμοί μπορούν να επιτρέψουν στο προσωπικό να εντοπίζει και να αντιμετωπίζει αποτελεσματικά τα προβλήματα προστασίας δεδομένων.

Ένας επιπλέον κρίσιμος παράγοντας στα οργανωτικά πλαίσια για την προστασία των δεδομένων είναι ο σχηματισμός ομάδων ή πρωτοκόλλων αντιμετώπισης περιστατικών. Παραβιάσεις δεδομένων και αστοχίες ασφαλείας μπορεί να εμφανιστούν ακόμη και σε οργανισμούς με αυστηρά πρωτόκολλα προστασίας δεδομένων. Κατά συνέπεια, είναι επιτακτική ανάγκη για τους οργανισμούς του δημόσιου τομέα να θεσπίσουν ξεκάθαρα πρωτόκολλα για την αντιμετώπιση τέτοιων καταστάσεων. Αυτό συνεπάγεται τον εντοπισμό του προσωπικού που είναι υπεύθυνο για τη διερεύνηση παραβιάσεων, την ενημέρωση των επηρεαζόμενων μερών και την αναφορά περιστατικών στις ρυθμιστικές αρχές, όπως απαιτείται. Μια αποτελεσματικά

²⁴ Ahl, A., Goto, M., Yarime, M., Tanaka, K., & Sagawa, D. (2022). Challenges and opportunities of blockchain energy applications: Interrelatedness among technological, economic, social, environmental, and institutional dimensions. *Renewable and Sustainable Energy Reviews*, 166, 112623. <https://doi.org/10.1016/j.rser.2022.112623>

²⁵ Jimmy, F. (2024). Enhancing data security in financial institutions with blockchain technology. *Journal of Artificial Intelligence General Science (JAIGS)* ISSN:3006-4023, 5(1), 424–437. <https://doi.org/10.60087/jaigs.v5i1.217>

καθιερωμένη στρατηγική αντιμετώπισης περιστατικών όχι μόνο μετριάξει τις συνέπειες των παραβιάσεων δεδομένων, αλλά υποδηλώνει επίσης την αφοσίωση του οργανισμού στην προστασία δεδομένων και τη συμμόρφωση με τους κανονισμούς.

Επιπλέον, τα οργανωτικά πλαίσια για την προστασία δεδομένων πρέπει να διαθέτουν μεθόδους για τη συμμετοχή των ενδιαφερομένων, που να περιλαμβάνουν το κοινό, τους ρυθμιστικούς φορείς και τις οργανώσεις της κοινωνίας των πολιτών. Η διαφάνεια και η λογοδοσία είναι απαραίτητες για τη δημιουργία εμπιστοσύνης με άτομα των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία²⁷. Οι οργανισμοί του δημόσιου τομέα πρέπει να θεσπίσουν σαφείς στρατηγικές επικοινωνίας για να ενημερώνουν τους πολίτες σχετικά με τις δραστηριότητές τους επεξεργασίας δεδομένων, τους στόχους για τους οποίους συλλέγονται προσωπικά δεδομένα και τα δικαιώματα των ατόμων σχετικά με τα δεδομένα τους. Μέσω της ενεργού δέσμευσης με τα ενδιαφερόμενα μέρη, οι οργανισμοί μπορούν να καλλιεργήσουν μια ατμόσφαιρα συνεργασίας που ενισχύει τις δραστηριότητες προστασίας δεδομένων και ζητά πληροφορίες για τις πρακτικές τους.

3.1.2. Ρόλοι και αρμοδιότητες

Τα καθήκοντα και οι ευθύνες του απορρήτου των δεδομένων σε οργανισμούς του δημόσιου τομέα είναι πολύπλοκα και απαραίτητα για τη διασφάλιση της συμμόρφωσης με τους σχετικούς νόμους και κανονισμούς. Κάθε εργασία εντός του οργανισμού συμβάλλει στον πρωταρχικό στόχο της προστασίας των προσωπικών δεδομένων, ενώ παράλληλα διευκολύνει την αποτελεσματική και αποδοτική παροχή δημόσιων υπηρεσιών²⁸. Ο καθορισμός αυτών των θέσεων καλλιεργεί μια κουλτούρα λογοδοσίας και κατανόησης σχετικά με την προστασία δεδομένων, η οποία είναι ζωτικής σημασίας για τον περιορισμό των κινδύνων που σχετίζονται με παραβιάσεις δεδομένων και παραβιάσεις της ιδιωτικής ζωής.

Μια επιπλέον σημαντική θέση, εκτός του ΥΠΔ που προαναφέρθηκε, είναι αυτή των υπευθύνων επεξεργασίας δεδομένων και των υπευθύνων επεξεργασίας δεδομένων εντός του οργανισμού. Ο υπεύθυνος επεξεργασίας δεδομένων είναι ο φορέας που καθορίζει τους στόχους και τις μεθόδους επεξεργασίας προσωπικών δεδομένων, ενώ ο υπεύθυνος επεξεργασίας δεδομένων είναι επιφορτισμένος με την επεξεργασία δεδομένων για λογαριασμό του υπευθύνου επεξεργασίας²⁹. Στον δημόσιο τομέα, οι υπεύθυνοι επεξεργασίας δεδομένων είναι γενικά ανώτεροι διαχειριστές ή προϊστάμενοι τμημάτων με την εξουσία να καθορίζουν τις πρακτικές επεξεργασίας δεδομένων. Είναι υπεύθυνοι για τη διασφάλιση ότι οι ομάδες τους συμμορφώνονται με τους κανόνες προστασίας δεδομένων και ότι όλες οι δραστηριότητες επεξεργασίας δεδομένων συμμορφώνονται με τις νομικές εντολές. Οι υπεύθυνοι επεξεργασίας δεδομένων, είτε είναι προσωπικό πληροφορικής είτε εξωτερικοί πάροχοι υπηρεσιών, υποχρεούνται να συμμορφώνονται με τις οδηγίες του υπευθύνου επεξεργασίας δεδομένων και να εκτελούν τα βασικά τεχνικά και οργανωτικά βήματα για την προστασία των προσωπικών δεδομένων.

²⁷ Abed, Y., & Chavan, M. (2019). The challenges of institutional distance: Data privacy issues in cloud computing. *Science, Technology and Society*, 24(1), 161–181. <https://doi.org/10.1177/0971721818806088>

²⁸ Ράμια, Κ. Σ. (2022). *Η τεχνολογία blockchain και η συμβατότητάς της με τον γενικό κανονισμό προστασίας δεδομένων*. <http://dspace.lib.uom.gr/handle/2159/26464>

²⁹ Jimmy, F. (2024). Enhancing data security in financial institutions with blockchain technology. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, 5(1), 424–437. <https://doi.org/10.60087/jaigs.v5i1.217>

Επιπλέον, πολλαπλές λειτουργίες του τμήματος ενισχύουν τις πρωτοβουλίες προστασίας δεδομένων σε ολόκληρο τον οργανισμό. Οι ειδικοί πληροφορικής διαδραματίζουν κρίσιμο ρόλο στην εφαρμογή και τη συντήρηση των τεχνικών προστασιών, συμπεριλαμβανομένης της κρυπτογράφησης, των τειχών προστασίας και των περιορισμών πρόσβασης, για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση ή παραβιάσεις³⁰. Τα καθήκοντά τους περιλαμβάνουν την επίβλεψη συστημάτων για πιθανές απειλές ασφαλείας και τη διασφάλιση συχνών ενημερώσεων λογισμικού και υλικού για τη μείωση των τρωτών σημείων. Μέσω στενής συνεργασίας με τον ΥΠΔ και άλλους ενδιαφερόμενους φορείς, το προσωπικό πληροφορικής εγγυάται την ενσωμάτωση των μέτρων προστασίας δεδομένων στην τεχνολογική υποδομή του οργανισμού.

Τα τμήματα Ανθρώπινου Δυναμικού (HR) είναι ζωτικής σημασίας για την προστασία των δεδομένων, ειδικά στον χειρισμό των πληροφοριών των εργαζομένων. Το τμήμα Ανθρώπινου Δυναμικού έχει καθήκον να διασφαλίζει ότι οι πληροφορίες των εργαζομένων συλλέγονται, διατηρούνται και υποβάλλονται σε επεξεργασία σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων. Αυτό περιλαμβάνει τη θέσπιση πολιτικών σχετικά με τη συναίνεση των εργαζομένων, τα αιτήματα πρόσβασης σε δεδομένα και τη διατήρηση δεδομένων. Τα τμήματα Ανθρώπινου Δυναμικού είναι επιφορτισμένα με τη διευκόλυνση των εκπαιδευτικών συνεδριών για την ενημέρωση των εργαζομένων σχετικά με τις υποχρεώσεις τους σχετικά με την προστασία δεδομένων και την ιδιωτική ζωή³¹. Καλλιεργώντας μια κουλτούρα ευαισθητοποίησης, το ανθρώπινο δυναμικό μπορεί να βοηθήσει στην άμβλυνση των κινδύνων που συνδέονται με την ακατάλληλη διαχείριση των προσωπικών δεδομένων εντός του οργανισμού.

Εκτός από αυτές τις διακριτές λειτουργίες, όλοι οι εργαζόμενοι σε έναν οργανισμό του δημόσιου τομέα έχουν κοινή υποχρέωση για προστασία δεδομένων. Όλο το προσωπικό πρέπει να κατανοήσει τη σημασία της προστασίας των προσωπικών δεδομένων και να συμμορφώνεται με τους κανόνες και τις διαδικασίες προστασίας δεδομένων του οργανισμού. Αυτό περιλαμβάνει την κατανόηση της κατάλληλης διαχείρισης των προσωπικών πληροφοριών, την αναφορά πιθανών παραβιάσεων ή περιστατικών δεδομένων και την αναγνώριση της σημασίας του απορρήτου των δεδομένων στις καθημερινές τους ευθύνες³². Ενισχύοντας ένα συλλογικό αίσθημα λογοδοσίας μεταξύ όλων των εργαζομένων, οι οργανισμοί μπορούν να δημιουργήσουν ένα πιο ανθεκτικό πλαίσιο για την προστασία δεδομένων που διαπερνά κάθε επίπεδο του ιδρύματος.

Επιπλέον, οι οντότητες του δημόσιου τομέα συχνά συνεργάζονται με εξωτερικούς ενδιαφερόμενους φορείς, όπως ρυθμιστικούς φορείς, οργανώσεις της κοινωνίας των πολιτών και το ευρύ κοινό³³. Η αλληλεπίδραση με αυτούς τους ενδιαφερομένους είναι απαραίτητη για τη διατήρηση της διαφάνειας και της λογοδοσίας στα μέτρα προστασίας δεδομένων. Οι επιχειρήσεις

³⁰ Ζούνη, Α. (2024). *Η προστασία των δεδομένων υγείας στην εποχή της πανδημίας Covid-19. Η διαχείριση των δεδομένων υγείας από το δημόσιο νοσοκομείο*. <http://dspace.lib.uom.gr/handle/2159/30921>

³¹ Möller, C. (2017). *The evolution of data protection and privacy in the public security context—An institutional analysis of three eu data retention and access regimes* [Thesis, Queen Mary University of London]. <https://qmro.qmul.ac.uk/xmlui/handle/123456789/25911>

³² Greco, S., Palmieri, R., & Rigotti, E. (2016). Institutional argumentation and conflict prevention: The case of the swiss federal data protection and information commissioner. *Journal of Pragmatics*, 105, 39–53. <https://doi.org/10.1016/j.pragma.2016.09.014>

³³ Περαιτός, Α. (2023). *Προστασία δεδομένων από μεταβολές στο διαδίκτυο των πραγμάτων με χρήση της τεχνολογίας καταμεμημένου κατάστιχου(Dlt)*. <https://doi.org/10.26265/polynoe-4701>

του δημόσιου τομέα πρέπει να εκπαιδεύουν τους ενδιαφερόμενους σχετικά με τις δραστηριότητές τους επεξεργασίας δεδομένων, που περιλαμβάνουν τη συλλογή, τη χρήση και τη διάδοση προσωπικών δεδομένων. Αυτή η προορατική στρατηγική επικοινωνίας ενισχύει την εμπιστοσύνη του κοινού και δίνει τη δυνατότητα στους οργανισμούς να χειρίζονται με επιτυχία ζητήματα και κριτική.

3.2. Νομικές υποχρεώσεις για τεχνικά και οργανωτικά μέτρα

3.2.1. Νομικές απαιτήσεις για την κρυπτογράφηση και την ανωνυμοποίηση

Το Άρθρο 32 του ΓΚΠΔ αναφέρει ρητά την κρυπτογράφηση και την ανωνυμοποίηση ως παραδείγματα κατάλληλων τεχνικών μεθόδων. Η κρυπτογράφηση συνεπάγεται τη μετατροπή των προσωπικών δεδομένων σε μορφή μη προσβάσιμη σε μη εξουσιοδοτημένα άτομα, ενώ η ανωνυμοποίηση σημαίνει την μη αναστρέψιμη εξάλειψη των προσωπικών αναγνωριστικών στοιχείων από τα σύνολα δεδομένων, καθιστώντας τα δεδομένα μη προσωπικά³⁴. Αυτές οι στρατηγικές είναι απαραίτητες για τον μετριασμό του κινδύνου σε περίπτωση παραβίασης και συχνά καθορίζουν εάν ένα περιστατικό είναι ανακοινώσιμο ή μη.

Ο ελληνικός νόμος 4624/2019 ενσωματώνει και συμμορφώνεται με αυτές τις διατάξεις. Η εθνική εφαρμογή ενθαρρύνει τους δημόσιους και ιδιωτικούς φορείς, όταν είναι κατάλληλο και εφικτό, να χρησιμοποιούν κρυπτογράφηση και ψευδωνυμοποίηση για την προστασία της ασφάλειας και του απορρήτου των προσωπικών δεδομένων³⁵. Στην επεξεργασία του δημόσιου τομέα, ιδίως όσον αφορά ευαίσθητα δεδομένα όπως πληροφορίες υγείας, ποινικές ή βιομετρικές πληροφορίες, η εφαρμογή της κρυπτογράφησης δεν είναι μόνο ωφέλιμη, αλλά συχνά απαραίτητη για τη συμμόρφωση με τις αρχές της αναλογικότητας και της αναγκαιότητας, όπως ορίζονται τόσο από τον ΓΚΠΔ όσο και από τις ελληνικές συνταγματικές εγγυήσεις.

Η εφαρμογή της κρυπτογράφησης ή της ανωνυμοποίησης μπορεί να επηρεάσει τις ευθύνες των υπευθύνων επεξεργασίας σε περίπτωση παραβίασης δεδομένων. Σύμφωνα με το Άρθρο 34(3)(α) του ΓΚΠΔ, εάν τα δεδομένα που έχουν παραβιαστεί ήταν κρυπτογραφημένα και κατέστησαν ακατανόητα σε μη εξουσιοδοτημένα μέρη, ο υπεύθυνος επεξεργασίας μπορεί να απαλλαγεί από την υποχρέωση να ειδοποιήσει τα υποκείμενα των δεδομένων σχετικά με την παραβίαση³⁶. Αυτή η εξαίρεση καταδεικνύει ότι η υιοθέτηση λύσεων προηγμένης τεχνολογίας όχι μόνο ενισχύει την ασφάλεια, αλλά και μειώνει τους νομικούς κινδύνους και τους κινδύνους για τη φήμη.

Παρ' όλα αυτά, η εφαρμογή μόνο της κρυπτογράφησης ή της ανωνυμοποίησης δεν συνιστά από μόνη της συμμόρφωση. Οι υπεύθυνοι επεξεργασίας και οι επεξεργαστές πρέπει να εγγυώνται ότι αυτές οι στρατηγικές είναι ενημερωμένες, εκτελούνται σωστά και υποστηρίζονται από αποτελεσματικές οργανωτικές πρακτικές. Η ελληνική νομοθεσία υποστηρίζει αυτή τη στάση επιβάλλοντας τη συνεχή αξιολόγηση και τροποποίηση των μέτρων ασφαλείας ως αντίδραση στους μεταβαλλόμενους κινδύνους και την τεχνολογική πρόοδο.

³⁴ Art. 32 GDPR – Security of processing. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved 13 May 2025, from <https://gdpr-info.eu/art-32-gdpr/>

³⁵ Νόμος 4624/2019 (Κωδικοποιημένος)—ΦΕΚ Α 137/29.08.2019. (n.d.). Retrieved 12 May 2025, from <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>

³⁶ Art. 34 GDPR – Communication of a personal data breach to the data subject. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved 13 May 2025, from <https://gdpr-info.eu/art-34-gdpr/>

3.2.2. Υποχρεώσεις κοινοποίησης περιστατικών

Μια κρίσιμη υποχρέωση βάσει του ΓΚΠΔ, και κατά συνέπεια βάσει της ελληνικής νομοθεσίας, είναι η απαίτηση κοινοποίησης παραβιάσεων προσωπικών δεδομένων. Τα άρθρα 33 και 34 του ΓΚΠΔ ορίζουν τα κριτήρια, την έκταση και το χρονοδιάγραμμα για τις κοινοποιήσεις παραβίασης³⁷. Το άρθρο 33 απαιτεί από τους υπεύθυνους επεξεργασίας να ενημερώνουν την εποπτική αρχή — στην Ελλάδα, την Ελληνική Αρχή Προστασίας Δεδομένων (ΑΠΔΠΧ) — εντός 72 ωρών από την ανακάλυψη μιας παραβίασης, εκτός εάν η παραβίαση θεωρείται απίθανο να θίξει τα δικαιώματα και τις ελευθερίες των ατόμων.

Ο νόμος 4624/2019 αντικατοπτρίζει αυτές τις εντολές και υπογραμμίζει τις διαδικαστικές ευθύνες τόσο των δημόσιων όσο και των εμπορικών φορέων που λειτουργούν στην Ελλάδα. Στην πραγματικότητα, αυτό συνεπάγεται ότι σε περίπτωση συμβάντος, οι υπεύθυνοι επεξεργασίας πρέπει να αξιολογούν γρήγορα τη μορφή και τις επιπτώσεις της παραβίασης, να προσδιορίζουν τις κατηγορίες των επηρεαζόμενων δεδομένων, να εκτιμούν την έκταση των επιπτώσεων και να διαπιστώνουν εάν η παραβίαση ενέχει κίνδυνο για τα άτομα. Σε μια τέτοια περίπτωση, ο υπεύθυνος επεξεργασίας υποχρεούται να αποστείλει έκθεση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) στην οποία θα αναφέρεται λεπτομερώς ο τύπος της παραβίασης, οι κατηγορίες και ο αριθμός των επηρεαζόμενων υποκειμένων δεδομένων, οι πιθανές επιπτώσεις και τυχόν διορθωτικές προσπάθειες που έχουν αναληφθεί ή προβλέπεται να αναληφθούν.

Οι επεξεργαστές, αντίθετα, υποχρεούνται να ενημερώνουν τον υπεύθυνο επεξεργασίας χωρίς περιττή καθυστέρηση μόλις αντιληφθούν μια παραβίαση. Η ελληνική νομοθεσία τηρεί πιστά αυτήν την προσέγγιση, τονίζοντας την αναγκαιότητα καθιερωμένων εσωτερικών πρωτοκόλλων και σαφών καναλιών επικοινωνίας μεταξύ υπευθύνων επεξεργασίας και επεξεργαστών. Ελλείψει τέτοιων μηχανισμών, η τήρηση της προθεσμίας των 72 ωρών είναι συχνά ανέφικτη.

Σε περιπτώσεις όπου μια παραβίαση ενέχει σημαντικό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, το Άρθρο 34 του ΓΚΠΔ ορίζει ότι ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει άμεσα τα εμπλεκόμενα μέρη. Αυτή η ειδοποίηση πρέπει να είναι σαφής, απλή και κατανοητή, προσφέροντας στα εμπλεκόμενα άτομα μια περιγραφή της παραβίασης, τις πιθανές επιπτώσεις της και καθοδήγηση σχετικά με τον τρόπο μετριασμού της πιθανής ζημίας³⁸. Παρ' όλα αυτά, εάν τα δεδομένα έχουν κρυπτογραφηθεί ή έχουν καταστεί μη αναγνώσιμα με άλλο τρόπο ή εάν οι επακόλουθες ενέργειες έχουν μειώσει επαρκώς τον κίνδυνο, ο υπεύθυνος επεξεργασίας μπορεί να εξαιρεθεί από την ειδοποίηση των ατόμων, υπό την προϋπόθεση της συμφωνίας της ΑΠΔΠΧ.

Η ελληνική νομοθεσία επιβάλλει την καταγραφή όλων των παραβιάσεων, ανεξάρτητα από την ειδοποίηση, για τη διατήρηση της διαφάνειας και της ευθύνης σε τέτοιες διαδικασίες. Αυτό το αρχείο πρέπει να περιλαμβάνει τις λεπτομέρειες σχετικά με την παραβίαση, τις επιπτώσεις της και τα διορθωτικά μέτρα που εφαρμόστηκαν. Τέτοια αρχεία επιτρέπουν στην ΑΠΔΠΧ να διαπιστώνει τη συμμόρφωση και να κινεί διαδικασίες επιβολής, εάν απαιτείται.

³⁷ Art. 33 GDPR – Notification of a personal data breach to the supervisory authority. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved 13 May 2025, from <https://gdpr-info.eu/art-33-gdpr/>

³⁸ Art. 34 GDPR – Communication of a personal data breach to the data subject. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved 13 May 2025, from <https://gdpr-info.eu/art-34-gdpr/>

3.2.3. Εσωτερικοί έλεγχοι και εκτιμήσεις κινδύνου βάσει της ελληνικής νομοθεσίας

Εκτός από συγκεκριμένες διασφαλίσεις όπως η κρυπτογράφηση και οι ειδοποιήσεις παραβίασης, τόσο ο ΓΚΠΔ όσο και η ελληνική νομοθεσία επιβάλλουν μια ολοκληρωμένη υποχρέωση διενέργειας εσωτερικών ελέγχων και αξιολογήσεων κινδύνου. Το άρθρο 32(1)(δ) του ΓΚΠΔ ορίζει σαφώς τη θέσπιση μιας διαδικασίας για τον τακτικό έλεγχο, αξιολόγηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων ασφαλείας. Αυτό δεν είναι ένα μοναδικό καθήκον, αλλά μια συνεχής ευθύνη, ειδικά καθώς οι κίνδυνοι αναπτύσσονται και οι οργανωτικές πρακτικές μεταμορφώνονται.

Ο νόμος 4624/2019 υποχρεώνει τους ελληνικούς δημόσιους φορείς να εφαρμόζουν εσωτερικές πολιτικές και πλαίσια διακυβέρνησης για να διασφαλίζουν τη συμμόρφωση με τους κανονισμούς προστασίας δεδομένων³⁹. Αυτό περιλαμβάνει τακτικές αξιολογήσεις κινδύνου που εκτιμούν την πιθανότητα και τη σοβαρότητα πιθανών παραβιάσεων δεδομένων ή παράνομης επεξεργασίας. Τέτοιες αξιολογήσεις πρέπει να λαμβάνουν υπόψη τη φύση των δεδομένων που χειρίζονται, το περιβάλλον επεξεργασίας, την ευαισθησία των δεδομένων και την πιθανή βλάβη στα υποκείμενα των δεδομένων.

Στον δημόσιο τομέα, ο ορισμός ενός Υπεύθυνου Προστασίας Δεδομένων (DPO), γνωστού ως Υπουργείου Προστασίας Δεδομένων (ΥΠΔ), είναι υποχρεωτικός. Το Άρθρο 6 του Νόμου 4624/2019 ορίζει τα προσόντα και τις αρμοδιότητες του Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ), υπογραμμίζοντας τον ρόλο του στην εποπτεία των εσωτερικών ελέγχων, στη διενέργεια εκτιμήσεων επιπτώσεων και στη διασφάλιση της τήρησης των πολιτικών⁴⁰. Ο ΥΠΔ πρέπει να λειτουργεί ανεξάρτητα και δεν μπορεί να παυθεί ή να τιμωρηθεί για την εκτέλεση των καθηκόντων του, υπογραμμίζοντας την ανάγκη μέτρων εσωτερικού ελέγχου στην ελληνική νομοθεσία.

Οι Εκτιμήσεις Επιπτώσεων στην Προστασία Δεδομένων (ΕΕΠΔ) αποτελούν ουσιαστικό στοιχείο της συμμόρφωσης με βάση τον κίνδυνο. Οι ΕΕΠΔ, αν και βασίζονται στο Άρθρο 35 του ΓΚΠΔ, εφαρμόζονται στην Ελλάδα σύμφωνα τόσο με τις βασικές διατάξεις του ΓΚΠΔ όσο και με ειδικές εθνικές οδηγίες που παρέχονται από την Αρχή Προστασίας Δεδομένων. Οι Εκτιμήσεις Επιπτώσεων στην Προστασία Δεδομένων (ΕΕΠΔ) είναι ιδιαίτερα υποχρεωτικές όταν εφαρμόζονται νέες τεχνολογίες ή όταν η επεξεργασία αναμένεται να θέσει σημαντικούς κινδύνους για τα δικαιώματα και τις ελευθερίες των προσώπων. Ο Υπεύθυνος Προστασίας Δεδομένων είναι κρίσιμος στην παροχή συμβουλών και στην εποπτεία των Εκτιμήσεων Επιπτώσεων στην Προστασία Δεδομένων, διασφαλίζοντας ότι οι κίνδυνοι εντοπίζονται, καταγράφονται και αντιμετωπίζονται διεξοδικά πριν από την έναρξη της επεξεργασίας.

Οι εσωτερικοί έλεγχοι τόσο στον δημόσιο όσο και στον εμπορικό τομέα πρέπει να περιλαμβάνουν τακτικές αξιολογήσεις των πολιτικών ασφαλείας, της αποτελεσματικότητας της εκπαίδευσης του προσωπικού, των ελέγχων πρόσβασης και των μεθόδων διαχείρισης δεδομένων. Η τεκμηρίωση αυτών των ελέγχων είναι ζωτικής σημασίας για την επίδειξη λογοδοσίας και συμμόρφωσης, ιδίως κατά τη διάρκεια κανονιστικού ελέγχου ή διερεύνησης παραβιάσεων.

3.3. Κοινή χρήση δεδομένων και διαλειτουργικότητα

3.3.1. Εξισορρόπηση της κοινής χρήσης δεδομένων και της ιδιωτικής ζωής

³⁹ Νόμος 4624/2019 (Κωδικοποιημένος)—ΦΕΚ Α 137/29.08.2019. (n.d.). Retrieved 12 May 2025, from <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>

⁴⁰ Άρθρο 6—Γενικός κανονισμός για την προστασία δεδομένων—Νομιμότητα της επεξεργασίας. (2016, May 7). Lawspot. <https://www.lawspot.gr/node/67400>

Η εξισορρόπηση της κοινής χρήσης δεδομένων και του απορρήτου είναι μια κρίσιμη πρόκληση για τους οργανισμούς του δημόσιου τομέα, καθώς επιδιώκουν να χρησιμοποιήσουν δεδομένα για βελτιωμένη παροχή υπηρεσιών προστατεύοντας παράλληλα τα ατομικά δικαιώματα⁴¹. Η αυξανόμενη ζήτηση για λήψη αποφάσεων με γνώμονα τα δεδομένα, τη διαφάνεια και τη συνεργασία μεταξύ των υπηρεσιών απαιτεί αποτελεσματικά πρωτόκολλα ανταλλαγής δεδομένων. Αυτά τα προγράμματα πρέπει να τυγχάνουν σχολαστικής διαχείρισης για την αποτελεσματική διαχείριση ζητημάτων απορρήτου, αποτρέποντας πιθανή κατάχρηση προσωπικών πληροφοριών και καλλιεργώντας την εμπιστοσύνη του κοινού.

Η κοινή χρήση δεδομένων εντός του δημόσιου τομέα μπορεί να βελτιώσει την αποδοτικότητα και την αποτελεσματικότητα των υπηρεσιών επιτρέποντας στους φορείς να έχουν πρόσβαση και να αναλύουν πληροφορίες από διάφορες πηγές. Η συνεργασία μεταξύ των τμημάτων υγείας και των κοινωνικών υπηρεσιών μπορεί να οδηγήσει σε παρεμβάσεις με μεγαλύτερη ακρίβεια για τους πληθυσμούς σε κίνδυνο⁴². Ομοίως, η ανταλλαγή δεδομένων μεταξύ των οργανισμών επιβολής του νόμου μπορεί να ενισχύσει τις τακτικές πρόληψης του εγκλήματος και να ενισχύσει τη δημόσια ασφάλεια. Ωστόσο, αν και τα πλεονεκτήματα της κοινής χρήσης δεδομένων είναι σημαντικά, έχουν εγγενείς απειλές για την ιδιωτική ζωή του ατόμου. Η σύγκρουση μεταξύ των πιθανών οφελών της κοινής χρήσης δεδομένων και της αναγκαιότητας προστασίας των προσωπικών πληροφοριών απαιτεί μια πολύπλοκη στρατηγική.

Οι οργανισμοί του δημόσιου τομέα πρέπει να εφαρμόσουν ρητά πλαίσια διακυβέρνησης δεδομένων που οριοθετούν τους κανόνες και τις διαδικασίες για την ανταλλαγή δεδομένων για την επίτευξη ισορροπίας. Αυτά τα πλαίσια πρέπει να δίνουν έμφαση στη διαφάνεια, τη λογοδοσία και την ελαχιστοποίηση των δεδομένων⁴³. Η διαφάνεια συνεπάγεται τη ρητή διαβίβαση των στόχων της κοινής χρήσης δεδομένων, των κατηγοριών των δεδομένων που περιλαμβάνονται και της σκοπούμενης χρήσης των πληροφοριών. Όταν τα άτομα ενημερώνονται για τον τρόπο με τον οποίο θα διαδοθούν τα δεδομένα τους και τους λόγους που το προκαλούν, τείνουν περισσότερο να κατανοήσουν και να συναινέσουν στις διαδικασίες κοινής χρήσης δεδομένων.

Η ελαχιστοποίηση δεδομένων είναι μια βασική έννοια που βοηθά στη μείωση των κινδύνων προστασίας της ιδιωτικής ζωής. Οι οργανισμοί πρέπει να περιορίζουν την κοινή χρήση δεδομένων σε πληροφορίες απαραίτητες για καθορισμένους σκοπούς, αποτρέποντας έτσι την αποκάλυψη περιττών ή περιττών δεδομένων. Αυτή η μέθοδος ελαχιστοποιεί την πιθανή παραβίαση του ατομικού απορρήτου, ενώ βελτιστοποιεί τις διαδικασίες διαχείρισης δεδομένων για μεγαλύτερη αποτελεσματικότητα. Η εφαρμογή αυστηρών προτύπων ταξινόμησης δεδομένων μπορεί να βοηθήσει τους οργανισμούς στην αξιολόγηση της ευαισθησίας των δεδομένων και στη θέσπιση κατάλληλων ελέγχων πρόσβασης ανάλογα.

Επιπλέον, οι οντότητες του δημόσιου τομέα πρέπει να δώσουν προτεραιότητα στη δημιουργία ισχυρών συμφωνιών ανταλλαγής δεδομένων που καθορίζουν σαφώς τους ρόλους και

⁴¹ Jimmy, F. (2024). Enhancing data security in financial institutions with blockchain technology. *Journal of Artificial Intelligence General Science (JAIGS)* ISSN:3006-4023, 5(1), 424–437. <https://doi.org/10.60087/jaigs.v5i1.217>

⁴² Αναστασία Κολοφωτία, Σ. (2022). *Το διαδίκτυο των πραγμάτων στο δημόσιο τομέα: η μετάβαση στην έξυπνη διακυβέρνηση, εφαρμογές και νομικές προκλήσεις* [Working Paper]. <http://repositoryesdda.ekdd.gr/jspui/handle/123456789/560>

⁴³ Κοντογεώργου, Η. (2024). *Η προστασία των προσωπικών δεδομένων εκτός ΕΕ: ΗΠΑ, Brussels effect και διασυννομιακή ροή* [Master Thesis, Πανεπιστήμιο Πειραιώς]. <https://dione.lib.unipi.gr/xmlui/handle/unipi/17427>

τις υποχρεώσεις όλων των εμπλεκόμενων φορέων. Αυτές οι συμφωνίες πρέπει να οριοθετούν τις προϋποθέσεις για την κοινή χρήση δεδομένων, που να περιλαμβάνουν μέτρα ασφαλείας, κανονισμούς διατήρησης δεδομένων και διαδικασίες πρόσβασης και χρήσης δεδομένων. Με τη θέσπιση αυτών των κατευθυντήριων γραμμών, οι οργανισμοί μπορούν να καλλιεργήσουν μια κουλτούρα λογοδοσίας και να εγγυηθούν ότι όλα τα ενδιαφερόμενα μέρη κατανοούν τις ευθύνες τους σχετικά με την προστασία δεδομένων.

Παράλληλα με τα οργανωτικά μέτρα, οι τεχνικές λύσεις είναι απαραίτητες για τον συνδυασμό της κοινής χρήσης δεδομένων με το απόρρητο. Η χρήση εξελιγμένων πρωτοκόλλων ασφαλείας, συμπεριλαμβανομένων της κρυπτογράφησης και των ελέγχων πρόσβασης, μπορεί να προστατεύσει τα κοινόχρηστα δεδομένα από μη εξουσιοδοτημένη πρόσβαση, επιτρέποντας ταυτόχρονα σε νόμιμους χρήστες να αποκτήσουν βασικές πληροφορίες. Επιπλέον, η εφαρμογή τεχνολογιών που βελτιώνουν το απόρρητο, όπως η ανωνυμοποίηση δεδομένων και η ψευδωνυμοποίηση, επιτρέπει στους οργανισμούς να χρησιμοποιούν και να διαδίδουν δεδομένα για αναλυτικούς στόχους χωρίς να τίθενται σε κίνδυνο οι ατομικές ταυτότητες. Αυτές οι τεχνολογίες επιτρέπουν πληροφορίες που βασίζονται σε δεδομένα, ενώ παράλληλα προστατεύουν το απόρρητο, επιτρέποντας έναν συμβιβασμό μεταξύ αυτών των φαινομενικά αντίθετων συμφερόντων.

Η αλληλεπίδραση με τα ενδιαφερόμενα μέρη, όπως το κοινό, οι οργανώσεις της κοινωνίας των πολιτών και οι ακτιβιστές προστασίας της ιδιωτικής ζωής, είναι απαραίτητη για την προώθηση ενός λόγου σχετικά με τις πρακτικές ανταλλαγής δεδομένων. Οι δημόσιες συζητήσεις και οι μέθοδοι ανατροφοδότησης μπορούν να δώσουν σημαντικές πληροφορίες σχετικά με τις ανησυχίες της κοινότητας σχετικά με την κοινή χρήση δεδομένων και το απόρρητο. Με τη συμμετοχή των ενδιαφερομένων στη διαδικασία λήψης αποφάσεων, οι οργανισμοί του δημόσιου τομέα μπορούν να ενισχύσουν την εμπιστοσύνη και να επιδείξουν την αφοσίωσή τους στην προστασία των προσωπικών δεδομένων ενώ προωθούν τις προσπάθειες κοινής χρήσης δεδομένων.

3.3.2. Προκλήσεις στη διαθεσμική κοινή χρήση δεδομένων

Η διαθεσμική ανταλλαγή δεδομένων θέτει πολλά εμπόδια για τους οργανισμούς του δημόσιου τομέα, εμποδίζοντας συχνά τη συλλογική χρήση δεδομένων για βελτιωμένη παροχή υπηρεσιών και διαμόρφωση πολιτικής. Καθώς οι κυβερνητικές οντότητες και οι δημόσιοι οργανισμοί αναγνωρίζουν ολοένα και περισσότερο τη σημασία των κοινών δεδομένων, οι περιπλοκές που σχετίζονται με τη διοργανική κοινή χρήση έχουν γίνει πιο εμφανείς. Τα προβλήματα μπορούν να ταξινομηθούν ως νομικοί, τεχνικοί και οργανωτικοί περιορισμοί, οι οποίοι πρέπει να επιλυθούν για να καταστεί δυνατή η επιτυχής ανταλλαγή δεδομένων.

Ένα πρωταρχικό εμπόδιο στη διαθεσμική ανταλλαγή δεδομένων είναι η διέλευση του νομικού και κανονιστικού πλαισίου. Διάφοροι φορείς λειτουργούν συχνά υπό διακριτά νομοθετικά πλαίσια που ρυθμίζουν τη χρήση και τη διάδοση δεδομένων, με αποτέλεσμα τη σύγχυση και πιθανές προκλήσεις συμμόρφωσης⁴⁴. Η νομοθεσία για την προστασία δεδομένων, η οποία αποτελεί παράδειγμα του Γενικού Κανονισμού για την Προστασία Δεδομένων στην Ευρώπη,

⁴⁴ Χατζηλιάδου, Σ. (2022). *Διαχείριση δημοσίων κατασκευαστικών έργων στην ήπειρο: Κίνδυνοι και προκλήσεις*. <https://kypseli.ouc.ac.cy/handle/11128/5316>

επιβάλλει αυστηρούς όρους σχετικά με την κοινή χρήση και την επεξεργασία προσωπικών δεδομένων. Οι δημόσιοι φορείς πρέπει να εγγυώνται ότι όλα τα έργα ανταλλαγής δεδομένων συμμορφώνονται με αυτές τις απαιτήσεις, οι οποίες ενδέχεται να περιλαμβάνουν παρατεταμένες αξιολογήσεις και συμφωνίες. Επιπλέον, οι οργανισμοί μπορεί να έχουν διαφορετικές απόψεις για τα νομικά καθήκοντα, με αποτέλεσμα να διστάζουν να κοινοποιήσουν δεδομένα λόγω ανησυχιών για μη συμμόρφωση ή πιθανές νομικές συνέπειες. Αυτή η νομική πολυπλοκότητα μπορεί να εμποδίσει τη συνεργασία, εμποδίζοντας τους οργανισμούς να χρησιμοποιήσουν πλήρως τα πιθανά πλεονεκτήματα των κοινών δεδομένων.

Τα τεχνικά ζητήματα παρουσιάζουν σημαντικά εμπόδια στη διαθεσμική ανταλλαγή δεδομένων. Οι οργανισμοί του δημόσιου τομέα χρησιμοποιούν συχνά ετερογενή συστήματα και πλατφόρμες πληροφορικής, γεγονός που περιπλέκει την ενοποίηση και τη συμβατότητα δεδομένων⁴⁵. Η απουσία τυποποίησης μεταξύ των φορέων εμποδίζει την απρόσκοπτη κοινή χρήση δεδομένων λόγω ασυμβίβαστων μορφών δεδομένων, δομών και πρωτοκόλλων. Επιπλέον, αναδύονται ανησυχίες σχετικά με την ασφάλεια και την ακεραιότητα των δεδομένων κατά τη μετάδοση ευαίσθητων πληροφοριών μεταξύ των ιδρυμάτων⁴⁶. Η εφαρμογή αυστηρών πρωτοκόλλων κυβερνοασφάλειας κατά τη μεταφορά δεδομένων είναι ζωτικής σημασίας. Ωστόσο, αυτή η διαδικασία μπορεί να απαιτεί πόρους και μπορεί να απαιτήσει τεχνολογικές δεξιότητες που ορισμένα ιδρύματα δεν διαθέτουν. Επιπλέον, η ανεπαρκής υποδομή μπορεί να περιορίσει τη δυνατότητα κοινής χρήσης δεδομένων, ιδιαίτερα σε μικρότερους οργανισμούς με περιορισμένους πόρους.

Τα οργανωτικά εμπόδια επιδεινώνουν τις προκλήσεις της διαθεσμικής ανταλλαγής δεδομένων. Οι αποκλίνουσες πολιτιστικές νόρμες μεταξύ των φορέων μπορούν να αποτελέσουν εμπόδια στην καλλιέργεια μιας ατμόσφαιρας συνεργασίας. Κάθε οργανισμός μπορεί να έχει ξεχωριστές αποστολές, προτεραιότητες και πρωτόκολλα διαχείρισης δεδομένων, με αποτέλεσμα ενδεχομένως την αντίθεση στην ανταλλαγή πληροφοριών⁴⁷. Ένας οργανισμός αφιερωμένος στην επιβολή του νόμου μπορεί να δώσει έμφαση στην ασφάλεια και το απόρρητο δεδομένων έναντι της κοινής χρήσης, ενώ ένας οργανισμός δημόσιας υγείας μπορεί να προωθήσει την αυξημένη ανταλλαγή δεδομένων για τη βελτίωση των αποτελεσμάτων της δημόσιας υγείας. Η συμφιλίωση αυτών των πολιτιστικών διαχωρισμών απαιτεί ισχυρή ηγεσία και αφοσίωση στην καλλιέργεια ενός συνεργατικού ήθους μεταξύ των ιδρυμάτων. Επιπλέον, αντικρουόμενα συμφέροντα και ατζέντες ενδέχεται να εμποδίσουν τις διθεσμικές δραστηριότητες, καθώς οι υπηρεσίες ενδέχεται να διστάζουν να αποκαλύψουν κρίσιμα δεδομένα που θα μπορούσαν να υπονομεύσουν το ανταγωνιστικό τους πλεονέκτημα ή εξουσία.

Οι οργανισμοί του δημόσιου τομέα πρέπει να έχουν μια συστηματική προσέγγιση για τη διευκόλυνση της διαθεσμικής ανταλλαγής δεδομένων προκειμένου να αντιμετωπίσουν αυτές τις δυσκολίες. Η δημιουργία ενός οριστικού πλαισίου διακυβέρνησης που οριοθετεί τους ρόλους, τα

⁴⁵ Greco, S., Palmieri, R., & Rigotti, E. (2016). Institutional argumentation and conflict prevention: The case of the swiss federal data protection and information commissioner. *Journal of Pragmatics*, 105, 39–53. <https://doi.org/10.1016/j.pragma.2016.09.014>

⁴⁶ Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4), 372–386. <https://doi.org/10.1016/j.telpol.2012.04.011>

⁴⁷ Περαιτινός, Α. (2023). Προστασία δεδομένων από μεταβολές στο διαδίκτυο των πραγμάτων με χρήση της τεχνολογίας κατανεμημένου κατάστιχου(Dlt). <https://doi.org/10.26265/polynoe-4701>

καθήκοντα και τις προσδοκίες για την κοινή χρήση δεδομένων βοηθά στη διευκόλυνση ενός συστηματικού περιβάλλοντος συνεργασίας⁴⁸. Αυτό το πλαίσιο πρέπει να περιλαμβάνει οδηγίες για την ασφάλεια των δεδομένων, τη διαφύλαξη της ιδιωτικής ζωής και την τήρηση των νομικών προτύπων. Η διαμόρφωση συμφωνιών κοινής χρήσης δεδομένων που οριοθετούν ρητά τους όρους και τις προϋποθέσεις για την ανταλλαγή δεδομένων μπορεί να μετριάσει τις νομικές ασάφειες και να ενισχύσει την εμπιστοσύνη μεταξύ των ιδρυμάτων.

Η επένδυση σε τεχνολογικές λύσεις που επιτρέπουν τη διαλειτουργικότητα δεδομένων μπορεί να βοηθήσει στην υπέρβαση τεχνικών εμποδίων⁴⁹. Η τυποποίηση μορφών και πρωτοκόλλων δεδομένων ενισχύει τη διαλειτουργικότητα του συστήματος, διευκολύνοντας την πιο αποτελεσματική ανταλλαγή δεδομένων⁵⁰. Επιπλέον, η χρήση πλατφορμών που βασίζονται σε σύννεφο μπορεί να προσφέρει ασφαλή περιβάλλοντα για αποθήκευση και μεταφορά δεδομένων, επιτρέποντας στα ιδρύματα να μοιράζονται πληροφορίες διατηρώντας παράλληλα τον έλεγχο της προστασίας δεδομένων.

Τελικά, η καλλιέργεια μιας κουλτούρας συνεργασίας και διαφάνειας στους οργανισμούς του δημόσιου τομέα είναι ζωτικής σημασίας για την αποτελεσματική διαθεσμική ανταλλαγή δεδομένων. Η συμμετοχή των ενδιαφερομένων στις διαδικασίες σχεδιασμού και λήψης αποφάσεων ενισχύει την εμπιστοσύνη και καλλιεργεί ένα συλλογικό όραμα για έργα κοινής χρήσης δεδομένων. Οι συνεπείς πρωτοβουλίες κατάρτισης και ευαισθητοποίησης μπορούν να ενισχύσουν την κατανόηση των εργαζομένων για τη σημασία της συνεργασίας και της ανταλλαγής δεδομένων, επιτρέποντας έτσι την ενεργό συμμετοχή τους σε αυτές τις προσπάθειες.

Κεφάλαιο 4: Νομικοί Κίνδυνοι και Προκλήσεις στην Προστασία Δεδομένων του Δημόσιου Τομέα

4.1. Νομική Κατηγοριοποίηση Εσωτερικών και Εξωτερικών Κινδύνων

4.1.1. Ανθρώπινο λάθος, εσωτερικές απειλές

Ένας σημαντικός κίνδυνος που συνδέεται με το ανθρώπινο λάθος αφορά τις επιθέσεις κοινωνικής μηχανικής, συμπεριλαμβανομένου του ηλεκτρονικού "ψαρέματος" (phishing). Αυτές οι παραπλανητικές στρατηγικές εκμεταλλεύονται την εμπιστοσύνη ή την άγνοια των

⁴⁸ Αναστασια Κολοφωτία, Σ. (2022). *Το διαδίκτυο των πραγμάτων στο δημόσιο τομέα: η μετάβαση στην έξυπνη διακυβέρνηση, εφαρμογές και νομικές προκλήσεις* [Working Paper]. <http://repositoryesdda.ekdd.gr/jspui/handle/123456789/560>

⁴⁹ Minkinen, M. (2015). Futures of privacy protection: A framework for creating scenarios of institutional change. *Futures*, 73, 48–60. <https://doi.org/10.1016/j.futures.2015.07.006>

⁵⁰ Jimmy, F. (2024). Enhancing data security in financial institutions with blockchain technology. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, 5(1), 424–437. <https://doi.org/10.60087/jaigs.v5i1.217>

εργαζομένων, εξαναγκάζοντάς τους να αποκαλύψουν εμπιστευτικές πληροφορίες ή να εμπλακούν σε επιβλαβείς συνδέσμους⁵¹. Οι οργανισμοί υποχρεούνται νομικά βάσει του ΓΚΠΔ να θεσπίσουν κατάλληλες τεχνολογικές και οργανωτικές δικλίδες ασφαλείας, όπως ορίζεται στο Άρθρο 32, για την προστασία των δεδομένων. Η ανεπαρκής εκπαίδευση ή προετοιμασία των εργαζομένων για τέτοιες επιθέσεις μπορεί να θεωρηθεί μη συμμόρφωση, με αποτέλεσμα η εταιρεία να υπόκειται σε κυρώσεις από τις ρυθμιστικές αρχές.

Για τον μετριασμό αυτών των απειλών, οι δημόσιοι φορείς πρέπει να δίνουν έμφαση σε συνεχείς πρωτοβουλίες εκπαίδευσης που επικεντρώνονται στις υποχρεώσεις ασφάλειας δεδομένων, την αναγνώριση ηλεκτρονικού "ψαρέματος" (phishing), την ασφαλή διαχείριση δεδομένων και τις μεθοδολογίες κρυπτογράφησης. Αυτές οι εκπαιδευτικές πρωτοβουλίες όχι μόνο μετριάζουν τα σφάλματα, αλλά και επιδεικνύουν προληπτική τήρηση των απαιτήσεων του ΓΚΠΔ⁵². Επιπλέον, η καθιέρωση φιλικών προς το χρήστη πολιτικών προστασίας δεδομένων και διαφανών μηχανισμών αναφοράς συμβάντων προωθεί την έγκαιρη αναφορά από τους εργαζόμενους, μετριάζοντας έτσι τις πιθανές νομικές επιπτώσεις των καθυστερημένων αντιδράσεων σε παραβιάσεις.

Οι οργανισμοί καλούνται να καλλιεργήσουν μια κουλτούρα που αποφεύγει την τιμωρία των εργαζομένων για γνήσια σφάλματα, προωθώντας αντ' αυτού τη διαφάνεια και την λογοδοσία. Αυτή η μέθοδος διευκολύνει τον άμεσο εντοπισμό και τη διόρθωση των τρωτών σημείων πριν από την εξέλιξή τους σε ουσιαστικές παραβιάσεις που ενδέχεται να απαιτήσουν κανονιστική εξέταση.

Οι εσωτερικές απειλές υποδηλώνουν κινδύνους που προέρχονται από άτομα εντός ενός οργανισμού — όπως υπαλλήλους, εργολάβους ή άλλο έμπιστο προσωπικό — τα οποία διαθέτουν εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα και συστήματα⁵³. Αυτές οι απειλές μπορεί να είναι είτε κακόβουλες (π.χ., σκόπιμη κλοπή ή δολιοφθορά δεδομένων) είτε απρόσεκτες (π.χ., μη συμμόρφωση με τα μέτρα ασφαλείας δεδομένων). Και οι δύο μορφές μπορεί να οδηγήσουν σε σημαντικές παραβιάσεις δεδομένων, ενεργοποιώντας τις νομικές ευθύνες σύμφωνα με τα άρθρα 32-34 του ΓΚΠΔ και τη σχετική εθνική νομοθεσία.

Η αποκλειστική πρόσβαση που κατέχουν οι εσωτερικοί παράγοντες καθιστά τις δραστηριότητές τους ιδιαίτερα επικίνδυνες, καθώς οι κακόβουλες προθέσεις μπορεί να παραμείνουν απαρατήρητες μέχρι να προκληθεί βλάβη⁵⁴. Ένας δυσαρεστημένος υπάλληλος μπορεί να αποκαλύψει εμπιστευτικές κυβερνητικές πληροφορίες ως αντίποινα, αλλά ένας εργολάβος μπορεί να διαχειριστεί ακατάλληλα ευαίσθητα δεδομένα για χρηματικό όφελος. Νομικά, οι επιχειρήσεις ενδέχεται να ευθύνονται εάν δεν θεσπίσουν επαρκείς ελέγχους πρόσβασης ή συστήματα παρακολούθησης για την αποτροπή τέτοιων παραβιάσεων.

Για την αποφυγή εσωτερικών απειλών, οι οργανισμοί του δημόσιου τομέα θα πρέπει να εφαρμόζουν την έννοια του ελάχιστου προνομίου, περιορίζοντας την πρόσβαση αποκλειστικά σε ό,τι είναι απαραίτητο για κάθε λειτουργία. Οι συνεπείς έλεγχοι πρόσβασης και η επιτήρηση της δραστηριότητας των χρηστών είναι κρίσιμοι για την ανίχνευση παρατυπιών που μπορεί να υποδηλώνουν κακόβουλη συμπεριφορά ή αμέλεια. Αυτό όχι μόνο βοηθά στην πρόληψη

⁵¹ Lampri, M. (2012). E-government and data protection in the public sector. In A. A. Lazakidou (Ed.), *Virtual Communities, Social Networks and Collaboration* (Vol. 15, pp. 135–145). Springer New York. https://doi.org/10.1007/978-1-4614-3634-8_7

⁵² Ernest, E. L., Osakwe, J., & Nhamu, I. (2023). A framework for data protection and privacy in data service centres in the public sector: A case study of a security organisation in a developing countries. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4645049>

⁵³ Ιωαννίδης, Ι. (2022). Προστασία προσωπικών δεδομένων και διαδίκτυο των πραγμάτων. <http://dspace.lib.uom.gr/handle/2159/27417>

⁵⁴ Pagallo Ugo & Bassi Eleonora. (2013). Open data protection: Challenges, perspectives, and tools for the reuse of psi. In *Digital Enlightenment Yearbook 2013*. IOS Press. <https://doi.org/10.3233/978-1-61499-295-0-179>

συμβάντων, αλλά διευκολύνει και τη συμμόρφωση παρέχοντας τεκμηρίωση των προληπτικών βημάτων, κάτι που είναι απαραίτητο σε κανονιστικές έρευνες.

Η καλλιέργεια μιας κουλτούρας που δίνει προτεραιότητα στην ασφάλεια είναι εξίσου σημαντική. Οι εργαζόμενοι πρέπει να κατανοούν τόσο τις τεχνολογικές όσο και τις ηθικές πτυχές της προστασίας δεδομένων, συμπεριλαμβανομένων των νομικών επιπτώσεων της κακοδιαχείρισης δεδομένων⁵⁵. Η προώθηση της αναφοράς ύποπτης δραστηριότητας από το προσωπικό, απαλλαγμένη από τον φόβο αντιποίνων, μπορεί να ενισχύσει την άμυνα ενός οργανισμού.

Τα προηγμένα τεχνολογικά μέσα μπορούν επίσης να επιτελέσουν μια κρίσιμη λειτουργία. Τα συστήματα Πρόληψης Απώλειας Δεδομένων (DLP), τα εργαλεία παρακολούθησης της δραστηριότητας των χρηστών και οι αναλύσεις συμπεριφοράς που βασίζονται στη μηχανική μάθηση μπορούν να εντοπίσουν ανώμαλα πρότυπα πρόσβασης δεδομένων ή παράνομες μεταφορές δεδομένων σε πραγματικό χρόνο. Αυτές οι τεχνολογίες χρησιμεύουν ως προστατευτικά μέτρα και μπορούν να μειώσουν σημαντικά την ευθύνη ενός οργανισμού, αποδεικνύοντας ότι χρησιμοποιήθηκε προληπτική παρακολούθηση, όπως επιβάλλεται από το Άρθρο 32 του ΓΚΠΔ.

Νομικά, τόσο το ανθρώπινο λάθος όσο και οι εσωτερικές απειλές απαιτούν μια πολύπλευρη προσέγγιση που περιλαμβάνει προληπτικές, ερευνητικές και στρατηγικές αντιμετώπισης. Ο ΓΚΠΔ ορίζει ότι οι υπεύθυνοι επεξεργασίας και οι επεξεργαστές πρέπει να υιοθετούν μέτρα ασφαλείας ανάλογα με τους κινδύνους (Άρθρο 32), να αναφέρουν παραβιάσεις στις εποπτικές αρχές εντός 72 ωρών (Άρθρο 33) και να ενημερώνουν τα επηρεαζόμενα άτομα για παραβιάσεις όταν υπάρχει σημαντικός κίνδυνος για τα δικαιώματα και τις ελευθερίες τους (Άρθρο 34).

Η ελληνική νομοθεσία περί προστασίας δεδομένων τηρεί αυτές τις αρχές και επιβάλλει περαιτέρω διοικητικές απαιτήσεις, συμπεριλαμβανομένων των εσωτερικών αξιολογήσεων κινδύνου και της αναφοράς περιστατικών⁵⁶. Οι φορείς του δημόσιου τομέα υποχρεούνται να διατηρούν αρχείο καταγραφής παραβιάσεων και να παρέχουν τεκμηρίωση των διορθωτικών μέτρων, καθώς η μη συμμόρφωση μπορεί να οδηγήσει σε ελέγχους, κυρώσεις ή βλάβη της φήμης.

4.1.2. Επιθέσεις στον κυβερνοχώρο σε δημόσια ιδρύματα

Οι κυβερνοεπιθέσεις σε κυβερνητικούς οργανισμούς έχουν γίνει μια σημαντική ανησυχία στο σύγχρονο ψηφιακό περιβάλλον. Καθώς οι οργανισμοί του δημόσιου τομέα εξαρτώνται ολοένα και περισσότερο από την τεχνολογία για την παροχή υπηρεσιών και τη διαχείριση δεδομένων, γίνονται ελκυστικοί στόχοι για εχθρικούς παράγοντες που στοχεύουν να εκμεταλλευτούν τα τρωτά σημεία για διάφορους κακόβουλους στόχους⁵⁷. Τέτοιες επιθέσεις μπορεί να οδηγήσουν σε σημαντικές επιπτώσεις, συμπεριλαμβανομένου του διακυβεύματος κρίσιμων πληροφοριών, της διακοπής των υπηρεσιών και της επιδείνωσης της εμπιστοσύνης του κοινού προς τις κυβερνητικές οντότητες. Η κατανόηση των χαρακτηριστικών και των επιπτώσεων των επιθέσεων στον κυβερνοχώρο σε δημόσιους οργανισμούς είναι ζωτικής σημασίας για τη διαμόρφωση αποτελεσματικών μέτρων για τον περιορισμό των κινδύνων και τη βελτίωση της προστασίας δεδομένων.

Το ransomware είναι ένας από τους πιο συνηθισμένους τύπους κυβερνοεπιθέσεων που στοχεύουν σε δημόσιους φορείς. Σε αυτές τις επιθέσεις, κακόβουλο λογισμικό κρυπτογραφεί τα

⁵⁵ Κουκουζέλη, Ο. Β. (2023). *Υπεύθυνος προστασίας δεδομένων(Υπδ)*. <http://dspace.lib.uom.gr/handle/2159/29706>

⁵⁶ Χατζηλιάδου, Σ. (2022). *Διαχείριση δημοσίων κατασκευαστικών έργων στην ήπειρο: Κίνδυνοι και προκλήσεις*. <https://kypseli.ouc.ac.cy/handle/11128/5316>

⁵⁷ Κουκουζέλη, Ο. Β. (2023). *Υπεύθυνος προστασίας δεδομένων(Υπδ)*. <http://dspace.lib.uom.gr/handle/2159/29706>

δεδομένα ενός οργανισμού, καθιστώντας τα απρόσιτα έως ότου επιστραφούν λύτρα στους δράστες. Οι επιθέσεις ransomware μπορούν να προκαλέσουν σοβαρή ζημιά σε δημόσιους οργανισμούς, με αποτέλεσμα συχνά σημαντικές διακοπές λειτουργίας και λειτουργικές διακοπές. Για παράδειγμα, όταν τα διοικητικά συστήματα μιας πόλης αδυνατούν από μια επίθεση ransomware, κρίσιμες λειτουργίες όπως η επιβολή του νόμου, η απόκριση έκτακτης ανάγκης και η δημόσια υγεία μπορεί να επηρεαστούν σημαντικά. Πέρα από τις άμεσες λειτουργικές δυσκολίες, αυτά τα ατυχήματα μπορούν να οδηγήσουν σε μόνιμες οικονομικές επιπτώσεις, καθώς οι οργανισμοί ενδέχεται να υποστούν δαπάνες ανάκτησης, πιθανές κυρώσεις και μειωμένη χρηματοδότηση λόγω βλάβης της φήμης.

Οι επιθέσεις phishing αντιπροσωπεύουν έναν διαδεδομένο κίνδυνο στον κυβερνοχώρο που αντιμετωπίζουν οι δημόσιοι φορείς. Αυτές οι επιθέσεις γενικά συνεπάγονται την παραπλάνηση των εργαζομένων στην αποκάλυψη εμπιστευτικών πληροφοριών, όπως κωδικούς πρόσβασης ή οικονομικά δεδομένα, πλαστοπροσωπώντας αξιόπιστες οντότητες. Οι εγκληματίες του κυβερνοχώρου συνθέτουν συχνά μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνονται αυθεντικά, παρασύροντας τους παραλήπτες να κάνουν κλικ σε επιζήμιους συνδέσμους ή να κατεβάσουν καταστροφικά συνημμένα⁵⁸. Οι υπάλληλοι του δημόσιου τομέα, ιδιαίτερα εκείνοι που δεν έχουν τακτική εκπαίδευση στις βέλτιστες πρακτικές ασφάλειας στον κυβερνοχώρο, είναι ιδιαίτερα ευαίσθητοι σε τέτοιες προσεγγίσεις. Μια επιτυχημένη απόπειρα phishing μπορεί να παρέχει στους εισβολείς πρόσβαση σε βασικά συστήματα, επιτρέποντάς τους να διεισδύουν δεδομένα, να υπονομεύουν τις διαδικασίες ασφαλείας ή να ξεκινούν άλλες επιθέσεις⁵⁹.

Οι επιθέσεις άρνησης υπηρεσίας (DoS) αποτελούν σημαντική απειλή για τους δημόσιους οργανισμούς. Σε αυτές τις επιθέσεις, οι εγκληματίες του κυβερνοχώρου κατακλύζουν ένα δίκτυο ή μια υπηρεσία με υπερβολική κίνηση, καθιστώντας το ανίκανο. Τέτοιες επιθέσεις μπορεί να εμποδίσουν την εύρυθμη λειτουργία των δημόσιων υπηρεσιών, με αποτέλεσμα την ενόχληση και τη δυσαρέσκεια για τα άτομα που εξαρτώνται από αυτές τις υπηρεσίες⁶⁰. Οι επιπτώσεις των επιθέσεων DoS μπορεί να είναι ιδιαίτερα σημαντικές κατά τη διάρκεια καταστάσεων έκτακτης ανάγκης ή σημαντικών γεγονότων όταν η άμεση πρόσβαση στις δημόσιες υπηρεσίες είναι απαραίτητη. Οι δημόσιοι θεσμοί πρέπει να είναι εξοπλισμένοι για να ανταποκρίνονται άμεσα σε αυτές τις απειλές για τον μετριασμό των διαταραχών σε βασικές υπηρεσίες.

Η εμφάνιση κυβερνοεπιθέσεων που χρηματοδοτούνται από το κράτος εισάγει ένα πρόσθετο στοιχείο περιπλοκής για τους δημόσιους θεσμούς. Σε έναν πιο δικτυωμένο κόσμο, τα έθνη-κράτη μπορεί να συμμετέχουν σε κυβερνοπόλεμο ή κατασκοπεία, με στόχο τους οργανισμούς του δημόσιου τομέα να αποκτήσουν πληροφορίες ή να διαβρώσουν την εμπιστοσύνη στην κυβέρνηση. Αυτές οι επιθέσεις μπορεί να είναι εξαιρετικά περίπλοκες και μπορεί να παραμείνουν απαρατήρητες για παρατεταμένες διάρκειες, επιτρέποντας στους εισβολείς να διεισδύουν στα συστήματα και να συλλέξουν σημαντικές πληροφορίες χωρίς έγκαιρη

⁵⁸ Ernest, E., Osakwe, J., & Nhamu, I. (2023). *A framework for data protection and privacy in data service centres in the public sector: A case study of a security organisation in a developing countries* (SSRN Scholarly Paper 4645049). <https://doi.org/10.2139/ssrn.4645049>

⁵⁹ Χατζηλιάδου, Σ. (2022). *Διαχείριση δημοσίων κατασκευαστικών έργων στην ήπειρο: Κίνδυνοι και προκλήσεις*. <https://kypseli.ouc.ac.cy/handle/11128/5316>

⁶⁰ Ιωαννίδης, Ι. (2022). *Προστασία προσωπικών δεδομένων και διαδίκτυο των πραγμάτων*. <http://dspace.lib.uom.gr/handle/2159/27417>

ενημέρωση. Κατά συνέπεια, οι δημόσιοι οργανισμοί πρέπει να διατηρούν επαγρύπνηση για τον εντοπισμό πιθανών κινδύνων και την εκτέλεση προηγμένων πρωτοκόλλων ασφαλείας για προστασία από τέτοιες περίπλοκες επιθέσεις.

Οι οργανισμοί του δημόσιου τομέα πρέπει να δώσουν προτεραιότητα στην ασφάλεια στον κυβερνοχώρο ως ουσιαστικό στοιχείο των δραστηριοτήτων τους για την αντιμετώπιση της αυξανόμενης επικράτησης των επιθέσεων στον κυβερνοχώρο⁶¹. Η διαμόρφωση μιας ολοκληρωμένης στρατηγικής κυβερνοασφάλειας που περιλαμβάνει αξιολόγηση κινδύνου, σχεδιασμό αντιμετώπισης περιστατικών και συνεχή εκπαίδευση των εργαζομένων είναι ζωτικής σημασίας. Η συνεχής ενημέρωση λογισμικού και συστημάτων, η θέσπιση αυστηρών περιορισμών πρόσβασης και η επένδυση σε εξελιγμένη τεχνολογία ανίχνευσης απειλών μπορούν να ενισχύσουν την άμυνα έναντι των απειλών στον κυβερνοχώρο.

Επιπλέον, η συνεργασία και η ανταλλαγή πληροφοριών μεταξύ των δημόσιων φορέων είναι απαραίτητες για τη βελτίωση της συνολικής ανθεκτικότητας στην ασφάλεια στον κυβερνοχώρο. Η δημιουργία συμμαχιών με άλλους κυβερνητικούς φορείς, υπηρεσίες επιβολής του νόμου και οργανισμούς κυβερνοασφάλειας μπορεί να ενισχύσει την ανταλλαγή πληροφοριών σχετικά με τις απειλές και τις βέλτιστες πρακτικές. Μέσω της προώθησης μιας στρατηγικής συνεργασίας, οι δημόσιοι φορείς μπορούν να προβλέψουν πιο αποτελεσματικά τους πιθανούς κινδύνους και να ανταποκριθούν σε περιστατικά.

4.2. Συμμόρφωση και νομικές προκλήσεις

4.2.1. Διασφάλιση της συμμόρφωσης με τον GDPR και τις κανονιστικές διατάξεις

Η τήρηση του Γενικού Κανονισμού Προστασίας Δεδομένων και άλλων νομοθετικών πλαισίων αποτελεί ουσιαστική υποχρέωση για τους οργανισμούς του δημόσιου τομέα. Ο GDPR, που τέθηκε σε ισχύ τον Μάιο του 2018, δημιούργησε ένα ολοκληρωμένο πλαίσιο για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση (ΕΕ) και επηρεάζει κάθε οργανισμό που διαχειρίζεται τα δεδομένα των ατόμων της ΕΕ, ανεξάρτητα από την τοποθεσία του. Για τους δημόσιους οργανισμούς, η συμμόρφωση με τον GDPR αποτελεί ταυτόχρονα νομική απαίτηση και ουσιαστικό στοιχείο για τη διατήρηση της εμπιστοσύνης του κοινού και την προστασία των δικαιωμάτων των πολιτών⁶².

Οι οργανισμοί του δημόσιου τομέα πρέπει αρχικά να πραγματοποιήσουν έναν ολοκληρωμένο έλεγχο δεδομένων για να διασφαλίσουν τη συμμόρφωση με τον GDPR. Αυτή η διαδικασία περιλαμβάνει την οριοθέτηση της τροχιάς των προσωπικών δεδομένων εντός του οργανισμού, την εξακρίβωση των τύπων των δεδομένων που συλλέγονται, τις τοποθεσίες αποθήκευσης, τις μεθόδους επεξεργασίας και τα άτομα που έχουν πρόσβαση σε αυτά⁶³. Η κατανόηση του κύκλου ζωής των δεδομένων είναι ζωτικής σημασίας για την αξιολόγηση της

⁶¹ Lampri, M. (2012). E-government and data protection in the public sector. In A. A. Lazakidou (Ed.), *Virtual Communities, Social Networks and Collaboration* (pp. 135–145). Springer. https://doi.org/10.1007/978-1-4614-3634-8_7

⁶² Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, 21(5), 510–524. <https://doi.org/10.1108/DPRG-05-2019-0039>

⁶³ Lampri, M. (2012). E-government and data protection in the public sector. In A. A. Lazakidou (Ed.), *Virtual Communities, Social Networks and Collaboration* (pp. 135–145). Springer. https://doi.org/10.1007/978-1-4614-3634-8_7

θέσης συμμόρφωσης του οργανισμού και τον εντοπισμό περιοχών που απαιτούν βελτίωση. Οι οργανισμοί πρέπει να διασφαλίζουν έγκυρες νομικές βάσεις για την επεξεργασία δεδομένων, συμπεριλαμβανομένης της συγκατάθεσης, της συμβατικής αναγκαιότητας ή του έννομου συμφέροντος, ενώ υποστηρίζουν τα δικαιώματα των ατόμων σχετικά με τα προσωπικά τους δεδομένα, όπως τα δικαιώματα πρόσβασης, διόρθωσης, διαγραφής και φορητότητας δεδομένων.

Με την ολοκλήρωση του ελέγχου δεδομένων, οι δημόσιοι φορείς πρέπει να διαμορφώσουν ρητές πολιτικές και διαδικασίες για την ασφάλεια των δεδομένων. Αυτοί οι κανόνες πρέπει να συμμορφώνονται με τις αρχές που καθορίζονται στον GDPR, συμπεριλαμβανομένης της ελαχιστοποίησης δεδομένων, του περιορισμού σκοπού και του περιορισμού αποθήκευσης⁶⁴. Οι οργανισμοί πρέπει να διασφαλίζουν ότι αποκτούν και διατηρούν μόνο τα ελάχιστα απαραίτητα προσωπικά δεδομένα για τις δραστηριότητές τους και ότι τα δεδομένα αυτά διατηρούνται αποκλειστικά για τη διάρκεια που εκπληρώνουν τον επιδιωκόμενο σκοπό τους. Επιπλέον, η διαφάνεια είναι βασικό στοιχείο συμμόρφωσης με τον GDPR. Οι οργανισμοί του δημόσιου τομέα πρέπει να παρέχουν στα άτομα ρητές πληροφορίες σχετικά με τη χρήση, την αποθήκευση και τη διάδοση των δεδομένων τους. Αυτό συνεπάγεται την ανάπτυξη προσβάσιμων δηλώσεων απορρήτου και τη θέσπιση διαδικασιών για την απόκτηση συναίνεσης όταν απαιτείται.

Η εκπαίδευση και η ευαισθητοποίηση είναι απαραίτητες για τη διασφάλιση της συμμόρφωσης με τον GDPR σε οργανισμούς του δημόσιου τομέα. Οι εργαζόμενοι αποτελούν αναπόσπαστο κομμάτι της προστασίας δεδομένων και η συχνή εκπαίδευση μπορεί να τους εξοπλίσει ώστε να κατανοούν τις υποχρεώσεις τους και να εντοπίζουν πιθανές απειλές για την προστασία των δεδομένων. Αυτή η εκπαίδευση πρέπει να περιλαμβάνει τα βασικά στοιχεία του GDPR, τους συγκεκριμένους κανόνες και διαδικασίες του οργανισμού και τις βέλτιστες πρακτικές για τη διαχείριση δεδομένων⁶⁵. Καλλιεργώντας μια κουλτούρα ευαισθητοποίησης για την προστασία των δεδομένων, οι οργανισμοί μπορούν να μειώσουν την πιθανότητα ακούσιων παραβιάσεων και να βελτιώσουν τις συνολικές πρωτοβουλίες συμμόρφωσης.

Οι οργανισμοί του δημόσιου τομέα πρέπει να εφαρμόζουν διαδικασίες για την παρακολούθηση και τον έλεγχο της συμμόρφωσης με τον GDPR και άλλες νομικές υποχρεώσεις, εκτός από τις εσωτερικές διασφαλίσεις. Οι τακτικές αξιολογήσεις των πολιτικών προστασίας δεδομένων μπορούν να βοηθήσουν στον εντοπισμό τυχόν ελλείψεων ή τρωτών σημείων στις πρωτοβουλίες συμμόρφωσης⁶⁶. Η διεξαγωγή αξιολογήσεων επιπτώσεων στην προστασία δεδομένων (ΕΑΠΔ) είναι μια αποτελεσματική μέθοδος για τη διασφάλιση της συμμόρφωσης, ειδικά κατά την έναρξη νέων έργων ή τεχνολογιών που συνεπάγονται την επεξεργασία προσωπικών δεδομένων. Οι Εκτιμήσεις Επιπτώσεων Προστασίας Δεδομένων (ΕΑΠΔ) επιτρέπουν στους οργανισμούς να αξιολογούν τους κινδύνους που συνδέονται με τις λειτουργίες

⁶⁴ Παπαδόπουλος, Α. (2020). *The implementation of the General Data Protection Regulation (Gdpr) in the EU and Greece: Procedures, risks, challenges and impacts in the context of good governance*. <http://dspace.lib.uom.gr/handle/2159/24326>

⁶⁵ Ernest, E., Osakwe, J., & Nhamu, I. (2023). *A framework for data protection and privacy in data service centres in the public sector: A case study of a security organisation in a developing countries* (SSRN Scholarly Paper 4645049). <https://doi.org/10.2139/ssrn.4645049>

⁶⁶ Panjwani, M., & Jäntti, M. (2017). Data protection & security challenges in digital & it services: A case study. *2017 International Conference on Computer and Applications (ICCA)*, 379–383. <https://doi.org/10.1109/COMAPP.2017.8079790>

επεξεργασίας δεδομένων και να υιοθετούν κατάλληλες ενέργειες για την άμβλυνση τέτοιων κινδύνων.

Επιπλέον, ο ορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO) μπορεί να ενισχύσει σημαντικά τις πρωτοβουλίες συμμόρφωσης. Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) είναι επιφορτισμένος με την επίβλεψη της πολιτικής προστασίας δεδομένων του οργανισμού και τη διασφάλιση της συμμόρφωσης με τις εντολές GDPR⁶⁷. Αυτή η θέση συνεπάγεται την επίβλεψη της συμμόρφωσης, την παροχή συμβουλών σε θέματα προστασίας δεδομένων και την υπηρεσία ως σύνδεσμος για τα υποκείμενα των δεδομένων και τους ρυθμιστικούς φορείς. Ένας επαγγελματίας Υπεύθυνος Προστασίας Δεδομένων (DPO) μπορεί να βοηθήσει τους οργανισμούς του δημόσιου τομέα στη διαχείριση των περιπλοκών του GDPR και να επιβεβαιώσει την αφοσίωσή τους στη διαφύλαξη των προσωπικών δεδομένων.

Οι δημόσιοι φορείς πρέπει να είναι εξοπλισμένοι για να ανταποκρίνονται αποτελεσματικά σε παραβιάσεις δεδομένων. Ο GDPR απαιτεί από τους οργανισμούς να ειδοποιούν την αρμόδια εποπτική αρχή για συγκεκριμένες παραβιάσεις δεδομένων εντός 72 ωρών από την ενημέρωση για το συμβάν. Αυτό απαιτεί οι οργανισμοί του δημόσιου τομέα να καταρτίσουν ολοκληρωμένα σχέδια αντιμετώπισης συμβάντων που περιγράφουν λεπτομερώς μεθόδους αναγνώρισης, διαχείρισης και αναφοράς παραβιάσεων. Η εφαρμογή σαφών μηχανισμών επικοινωνίας για την ενημέρωση των επηρεαζόμενων ατόμων είναι ζωτικής σημασίας, καθώς η διαφάνεια κατά τη διάρκεια μιας παραβίασης συμβάλλει στη διατήρηση της εμπιστοσύνης του κοινού και στη μείωση της βλάβης της φήμης.

4.2.2. Ζητήματα διακρατικού χειρισμού δεδομένων

Οι διακρατικές προκλήσεις διαχείρισης δεδομένων έχουν αποκτήσει σημασία καθώς η παγκοσμιοποίηση και η ψηφιοποίηση μεταμορφώνουν τη συλλογή, την επεξεργασία και τη διάδοση προσωπικών δεδομένων πέρα από τα σύνορα⁶⁸. Οι οργανισμοί του δημόσιου τομέα αντιμετωπίζουν ξεχωριστά ζητήματα στη διαχείριση των περιπλοκών των διακρατικών διαβιβάσεων δεδομένων, που απαιτούν την τήρηση των κανονισμών προστασίας δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων και άλλα σχετικά διεθνή πλαίσια.

Μια βασική πρόκληση της διεθνούς διαχείρισης δεδομένων είναι τα διαφορετικά πρότυπα προστασίας δεδομένων μεταξύ των διαφόρων κυβερνήσεων. Ο GDPR δημιουργεί μια ισχυρή βάση για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση, αν και τα κράτη εκτός ΕΕ ενδέχεται να έχουν διαφορετικούς κανόνες, ορισμένοι από τους οποίους μπορεί να μην έχουν ισοδύναμα επίπεδα προστασίας⁶⁹. Αυτή η αναντιστοιχία δημιουργεί ζητήματα για οργανισμούς του δημόσιου τομέα που απαιτούν τη μεταφορά προσωπικών δεδομένων σε χώρες εκτός ΕΕ για σκοπούς όπως η διεθνής συνεργασία, η συμμετοχή σε ερευνητικά έργα ή η χρήση υπηρεσιών cloud. Οι δημόσιοι οργανισμοί πρέπει να εφαρμόζουν επαρκή προστασία για την

⁶⁷ Νοτοπούλου, Φ. (2022). *Σύγχρονα ζητήματα γύρω από την προστασία δεδομένων προσωπικού χαρακτήρα* [Master Thesis, Πανεπιστήμιο Πειραιώς]. https://doi.org/10.26267/unipi_dione/2472

⁶⁸ Gonçalves, M. E. (2017). The EU data protection reform and the challenges of big data: Remaining uncertainties and ways forward. *Information & Communications Technology Law*, 26(2), 90–115. <https://doi.org/10.1080/13600834.2017.1295838>

⁶⁹ Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, 21(5), 510–524. <https://doi.org/10.1108/DPRG-05-2019-0039>

προστασία των δικαιωμάτων ιδιωτικής ζωής των ατόμων κατά τη διάρκεια διεθνών διαβιβάσεων δεδομένων, όπως απαιτείται από τον GDPR.

Ο GDPR οριοθετεί πολλές τεχνικές που μπορούν να χρησιμοποιήσουν οι οργανισμοί για να εξασφαλίσουν συμβατές μεταφορές δεδομένων. Οι Τυπικές Συμβατικές Ρήτρες (SCC) αναγνωρίζονται ευρέως ως νομικά δεσμευτικές συμφωνίες μεταξύ μερών σε διαφορετικές δικαιοδοσίες. Αυτές οι διατάξεις εγγυώνται ότι παρέχεται στα μεταφερόμενα δεδομένα ένα επίπεδο προστασίας σύμφωνα με τους κανόνες GDPR. Η εφαρμογή των SCCs είναι δύσκολη, καθώς απαιτεί από τους οργανισμούς να πραγματοποιούν ολοκληρωμένες αξιολογήσεις των κανονισμών προστασίας δεδομένων και του ρυθμιστικού πλαισίου της χώρας υποδοχής. Επιπλέον, ορισμένοι οργανισμοί ενδέχεται να αντιμετωπίσουν δυσκολίες στη διατήρηση της συνεχούς συμμόρφωσης με τα SCC, ειδικά σε περίπτωση αλλαγών στο ρυθμιστικό περιβάλλον ή στην πολιτική κατάσταση στο αποδέκτη κράτος.

Μια αξιοσημείωτη ανησυχία για τη διεθνή διαχείριση δεδομένων είναι ο αυξανόμενος αντίκτυπος της νομοθεσίας για την προστασία δεδομένων των ΗΠΑ, ιδίως λαμβάνοντας υπόψη τις πρόσφατες κανονιστικές αλλαγές που επηρεάζουν τις διατλαντικές ροές δεδομένων. Η ακύρωση του πλαισίου Privacy Shield το 2020 από το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) έχει δημιουργήσει ανησυχίες για οντότητες που στο παρελθόν εξαρτιόταν από αυτόν τον μηχανισμό για τη μεταφορά δεδομένων μεταξύ της ΕΕ και των ΗΠΑ. Μετά από αυτήν την ετυμηγορία, οι οργανισμοί του δημόσιου τομέα απαιτείται αυξημένη προσοχή και διεξαγωγή ενδελεχών αξιολογήσεων κινδύνου πριν από τη διαβίβαση δεδομένων σε εταιρείες των ΗΠΑ, λαμβάνοντας υπόψη πιθανές ελλείψεις στους κανονισμούς προστασίας δεδομένων⁷⁰. Αυτή η επίμονη ασάφεια απαιτεί επαναξιολόγηση των συμφωνιών μεταφοράς δεδομένων και διερεύνηση εναλλακτικών μεθόδων για τη διασφάλιση της συμμόρφωσης.

Επιπλέον, οι οντότητες του δημόσιου τομέα πρέπει να αναγνωρίσουν τις συνέπειες της κυβερνητικής επιτήρησης και της πρόσβασης σε προσωπικές πληροφορίες στο κράτος υποδοχής. Ανησυχίες σχετικά με τη νομοθεσία για την εθνική ασφάλεια που επιτρέπει την κυβερνητική πρόσβαση ή την παρακολούθηση δεδομένων ενδέχεται να θέσει σε κίνδυνο τις διασφαλίσεις που παρέχονται από τον GDPR⁷¹. Κατά συνέπεια, οι οργανισμοί πρέπει να επιδείξουν τη δέουσα επιμέλεια για να κατανοήσουν το νομικό πλαίσιο που διέπει τις μεταφορές δεδομένων και να αξιολογήσουν τους κινδύνους που συνδέονται με την ενδεχόμενη κυβερνητική πρόσβαση. Οι οργανισμοί μπορεί να χρειαστεί να θεσπίσουν συμπληρωματικές συμβατικές προστασίες ή τεχνικά μέτρα για να αποτρέψουν τα προσωπικά δεδομένα από μη εξουσιοδοτημένη πρόσβαση.

Οι συνέπειες των διακρατικών προκλήσεων διαχείρισης δεδομένων είναι ιδιαίτερα εμφανείς στο πεδίο της διεθνούς συνεργασίας και συμμαχιών. Οι οργανισμοί του δημόσιου τομέα συμμετέχουν συχνά σε διασυνοριακά έργα, έρευνες και πρωτοβουλίες ανταλλαγής δεδομένων που απαιτούν την ανταλλαγή προσωπικών δεδομένων. Για να ενεργοποιηθούν αυτές οι συνεργασίες,

⁷⁰ Νοτοπούλου, Φ. (2022). *Σύγχρονα ζητήματα γύρω από την προστασία δεδομένων προσωπικού χαρακτήρα* [Master Thesis, Πανεπιστήμιο Πειραιώς]. https://doi.org/10.26267/unipi_dione/2472

⁷¹ Παπαδόπουλος, Α. (2020). *The implementation of the General Data Protection Regulation (Gdpr) in the EU and Greece: Procedures, risks, challenges and impacts in the context of good governance*. <http://dspace.lib.uom.gr/handle/2159/24326>

ενώ τηρούν τους κανονισμούς προστασίας δεδομένων, οι οργανισμοί πρέπει να συνάψουν ρητές συμφωνίες κοινής χρήσης δεδομένων που να καθορίζουν τα καθήκοντα κάθε συμμετέχοντα όσον αφορά την προστασία δεδομένων⁷². Αυτές οι συμφωνίες πρέπει να προσδιορίζουν τις μεθόδους χειρισμού, επεξεργασίας και προστασίας δεδομένων, καθώς και τα δικαιώματα των ατόμων των οποίων τα δεδομένα κοινοποιούνται.

Η εκπαίδευση και η ευαισθητοποίηση είναι βασικά στοιχεία για την αντιμετώπιση παγκόσμιων προκλήσεων διαχείρισης δεδομένων. Οι υπάλληλοι του δημόσιου τομέα που ασχολούνται με δραστηριότητες μεταφοράς δεδομένων πρέπει να ενημερώνονται για τις νομικές υποχρεώσεις και τις βέλτιστες πρακτικές που σχετίζονται με τις διεθνείς διαβιβάσεις δεδομένων. Αυτό περιλαμβάνει την κατανόηση των επιπτώσεων των διαφορετικών προτύπων προστασίας δεδομένων, τον εντοπισμό πιθανών κινδύνων και την ικανότητα αξιολόγησης της συμμόρφωσης κατά τη συνεργασία με διεθνείς εταίρους. Μια κουλτούρα συμμόρφωσης σε οργανισμούς του δημόσιου τομέα μπορεί να μειώσει τους κινδύνους που συνδέονται με τη διεθνή διαχείριση δεδομένων.

4.3. Δημόσια αντίληψη και εμπιστοσύνη

4.3.1. Εμπιστοσύνη του κοινού στην προστασία των δεδομένων

Η εμπιστοσύνη του κοινού στην προστασία δεδομένων είναι απαραίτητη για την αποτελεσματική λειτουργία των οργανισμών του δημόσιου τομέα. Η διαχείριση των προσωπικών δεδομένων επηρεάζει άμεσα το απόρρητο και την ασφάλεια των ατόμων⁷³. Ως εκ τούτου, η εμπιστοσύνη στη διαχείριση θεσμικών δεδομένων είναι απαραίτητη. Όταν οι πολίτες βλέπουν ότι τα προσωπικά τους στοιχεία προστατεύονται επαρκώς, τείνουν περισσότερο να χρησιμοποιούν τις δημόσιες υπηρεσίες και να αποκαλύπτουν οικειοθελώς τα δεδομένα τους. Η έλλειψη εμπιστοσύνης σχετικά με τα μέτρα προστασίας δεδομένων μπορεί να έχει ως αποτέλεσμα τη διστακτικότητα της συνεργασίας με δημόσιους θεσμούς, εμποδίζοντας την αποτελεσματική παροχή υπηρεσιών και διαβρώνοντας την πίστη του κοινού στην κυβέρνηση.

Η διαφάνεια των οργανισμών του δημόσιου τομέα είναι βασικός παράγοντας που επηρεάζει την εμπιστοσύνη του κοινού στην προστασία των δεδομένων. Οι πολίτες τείνουν περισσότερο να εμπιστεύονται τα ιδρύματα που μεταφέρουν με διαφάνεια τις πολιτικές, τις πρακτικές προστασίας δεδομένων και τυχόν περιστατικά παραβίασης δεδομένων. Η διαφάνεια συνεπάγεται την παροχή ρητών πληροφοριών σχετικά με τα δεδομένα που αποκτήθηκαν, τη χρήση τους και τις διασφαλίσεις που εφαρμόζονται για την προστασία τους⁷⁴. Οι οργανισμοί που επιδεικνύουν ευθύνη αναφέροντας με συνέπεια τις διαδικασίες και τα περιστατικά προστασίας δεδομένων τους καλλιεργούν την εμπιστοσύνη και την ασφάλεια του κοινού. Αυτή η διαφάνεια είναι ιδιαίτερα σημαντική σε μια εποχή που τα άτομα είναι πιο ανήσυχα σχετικά με το απόρρητο των δεδομένων και την πιθανή εκμετάλλευση των πληροφοριών τους.

⁷² Gonçalves, M. E. (2017). The EU data protection reform and the challenges of big data: Remaining uncertainties and ways forward. *Information & Communications Technology Law*, 26(2), 90–115. <https://doi.org/10.1080/13600834.2017.1295838>

⁷³ Panjwani, M., & Jäntti, M. (2017). Data protection & security challenges in digital & it services: A case study. *2017 International Conference on Computer and Applications (ICCA)*, 379–383. <https://doi.org/10.1109/COMAPP.2017.8079790>

⁷⁴ Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, 21(5), 510–524. <https://doi.org/10.1108/DPRG-05-2019-0039>

Επιπλέον, η εμπιστοσύνη του κοινού στην προστασία δεδομένων επηρεάζεται σημαντικά από την αντιληπτή αποτελεσματικότητα της ρυθμιστικής δομής που επιβλέπει τις πρακτικές διαχείρισης δεδομένων. Κανονισμοί όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων παρέχουν ένα πλαίσιο για τον καθορισμό προτύπων στην προστασία των δεδομένων και τη λογοδοσία. Όταν οι πολίτες αναγνωρίζουν την ύπαρξη ισχυρών νομοθετικών πλαισίων που έχουν σχεδιαστεί για την προστασία των δικαιωμάτων τους στα δεδομένα, τείνουν περισσότερο να εμπιστεύονται ότι η διαχείριση των προσωπικών τους δεδομένων θα γίνεται με υπευθυνότητα. Αυτή η άποψη ενισχύεται όταν οι δημόσιοι φορείς τηρούν επιμελώς τη νομοθεσία και επιδεικνύουν δέσμευση στις πρακτικές δεοντολογικών δεδομένων.

Οι οργανισμοί του δημόσιου τομέα πρέπει επίσης να αναγνωρίσουν τη σημασία της επικοινωνίας για την ενίσχυση της εμπιστοσύνης⁷⁵. Συνεπείς πρωτοβουλίες προβολής που ενημερώνουν τους πολίτες σχετικά με την προστασία δεδομένων, τα δικαιώματα απορρήτου και τις διαδικασίες διαχείρισης δεδομένων του οργανισμού μπορούν να ενισχύσουν σημαντικά την εμπιστοσύνη του κοινού. Αυτό περιλαμβάνει όχι μόνο την εκπαίδευση των πολιτών σχετικά με τη χρήση των δεδομένων τους, αλλά και τη συμπερίληψή τους σε διαλόγους σχετικά με το απόρρητο και την ασφάλεια των δεδομένων. Με την προώθηση του λόγου για την προστασία των δεδομένων, οι δημόσιοι οργανισμοί μπορούν να επιτρέψουν στους πολίτες να συμμετέχουν ενεργά στη διαφύλαξη των πληροφοριών τους. Αυτή η προορατική στρατηγική μπορεί να διευκολύνει τη σύνδεση μεταξύ των δημόσιων οργανισμών και των ανθρώπων που εξυπηρετούν, ενισχύοντας την αμοιβαία αφοσίωση στο απόρρητο των δεδομένων.

Η διαχείριση των παραβιάσεων δεδομένων επηρεάζει σημαντικά την εμπιστοσύνη του κοινού στην προστασία των δεδομένων⁷⁶. Ο τρόπος με τον οποίο οι οργανισμοί αντιδρούν σε περιστατικά μπορεί είτε να ενισχύσει είτε να διαβρώσει την εμπιστοσύνη. Η έγκαιρη και σαφής ειδοποίηση για παραβιάσεις, σε συνδυασμό με αποτελεσματικές στρατηγικές αποκατάστασης, είναι ζωτικής σημασίας για τη διατήρηση της εμπιστοσύνης του κοινού. Όταν οι πολίτες παρατηρούν ότι ένας οργανισμός αναγνωρίζει τα λάθη του και προσπαθεί επιμελώς να αποτρέψει επαναλαμβανόμενα περιστατικά, είναι πιο διατεθειμένοι να διατηρήσουν την εμπιστοσύνη σε αυτόν τον θεσμό. Αντίθετα, η αναποτελεσματική επικοινωνία κατά τη διάρκεια παραβίασης ή οι ανεπαρκείς απαντήσεις μπορεί να επιδεινώσουν τον σκεπτικισμό και το άγχος σχετικά με την ασφάλεια των δεδομένων.

Οι πολιτισμικές μεταβλητές επηρεάζουν σημαντικά την εμπιστοσύνη του κοινού στην προστασία των δεδομένων. Άτομα από διαφορετική προέλευση μπορεί να έχουν διαφορετικές προοπτικές προστασίας της ιδιωτικής ζωής και των δεδομένων που επηρεάζονται από τις εμπειρίες και τα κοινωνικά τους πρότυπα. Οι οργανισμοί του δημόσιου τομέα πρέπει να προσπαθούν να έχουν πολιτιστική επίγνωση και να λαμβάνουν υπόψη αυτές τις διαφορές κατά τη διαμόρφωση των πρακτικών προστασίας δεδομένων τους. Αναγνωρίζοντας και αντιμετωπίζοντας διαφορετικές

⁷⁵ Νοτοπούλου, Φ. (2022). *Σύγχρονα ζητήματα γύρω από την προστασία δεδομένων προσωπικού χαρακτήρα* [Master Thesis, Πανεπιστήμιο Πειραιώς]. https://doi.org/10.26267/unipi_dione/2472

⁷⁶ Παπαδόπουλος, Α. (2020). *The implementation of the General Data Protection Regulation (Gdpr) in the EU and Greece: Procedures, risks, challenges and impacts in the context of good governance*. <http://dspace.lib.uom.gr/handle/2159/24326>

απόψεις σχετικά με το απόρρητο των δεδομένων, οι οργανισμοί μπορούν να προσαρμόσουν τις στρατηγικές τους για να ενισχύσουν την εμπιστοσύνη μεταξύ των διαφορετικών κοινοτήτων.

4.3.2. Διαφάνεια και λογοδοσία

Η διαφάνεια και η λογοδοσία είναι βασικά χαρακτηριστικά που υποστηρίζουν καλές πολιτικές προστασίας δεδομένων στον δημόσιο τομέα. Δεδομένου ότι οι δημόσιοι οργανισμοί χειρίζονται εκτεταμένα προσωπικά δεδομένα, η καλλιέργεια μιας ατμόσφαιρας διαφάνειας και λογοδοσίας είναι απαραίτητη για την εδραίωση της εμπιστοσύνης του κοινού και την τήρηση των απαιτήσεων προστασίας δεδομένων. Η διαφάνεια περιλαμβάνει τη ρητή επικοινωνία σχετικά με τις πρακτικές δεδομένων και την αφοσίωση στο άνοιγμα όσον αφορά τη συλλογή, την επεξεργασία και τη διαφύλαξη δεδομένων. Αυτή η διαφάνεια είναι απαραίτητη για τη διασφάλιση των πολιτών ότι η διαχείριση των προσωπικών τους δεδομένων γίνεται με επιμέλεια και ακεραιότητα.

Οι οργανισμοί του δημόσιου τομέα μπορούν να επιδείξουν διαφάνεια προσφέροντας προσβάσιμες και σαφείς πληροφορίες σχετικά με τις πολιτικές διαχείρισης δεδομένων τους. Αυτό περιλαμβάνει τη διάδοση ειδοποιήσεων απορρήτου που περιγράφουν λεπτομερώς τα είδη των προσωπικών δεδομένων που συλλέγονται, τους στόχους χρήσης των δεδομένων, τις μεθόδους αποθήκευσης και κοινής χρήσης και τα δικαιώματα των προσώπων στα δεδομένα τους. Παρέχοντας αυτές τις πληροφορίες με δυνατότητα πρόσβασης, οι οργανισμοί μπορούν να επιτρέψουν στους πολίτες να κατανοήσουν τα δικαιώματά τους και να κάνουν μορφωμένες επιλογές σχετικά με τα δεδομένα τους. Επιπλέον, οι οργανισμοί του δημόσιου τομέα μπορούν να πραγματοποιούν τακτικές αναφορές και ελέγχους των διαδικασιών προστασίας δεδομένων τους, επιτρέποντας στους ενδιαφερόμενους να αξιολογήσουν την αποτελεσματικότητα αυτών των διασφαλίσεων και να θέσουν τον οργανισμό υπεύθυνο.

Η λογοδοσία αφορά το καθήκον των οργανισμών του δημόσιου τομέα να αναλαμβάνουν τη λογοδοσία για τις μεθόδους και τις επιλογές τους για την προστασία των δεδομένων. Αυτό συνεπάγεται όχι μόνο τη συμμόρφωση με τους ισχύοντες κανόνες και κανονισμούς προστασίας δεδομένων, αλλά και την προληπτική ανάπτυξη εσωτερικών πολιτικών και διαδικασιών που προωθούν την ηθική διαχείριση δεδομένων⁷⁷. Οι οργανισμοί πρέπει να καθορίσουν σαφείς γραμμές λογοδοσίας για την προστασία δεδομένων, που συνήθως επιτυγχάνονται με τον ορισμό εξειδικευμένων Υπεύθυνων Προστασίας Δεδομένων (DPO) που επιβλέπουν τις πρωτοβουλίες συμμόρφωσης και εγγυώνται τη συμμόρφωση με τις βέλτιστες πρακτικές εντός του ιδρύματος. Η καθιέρωση μιας κουλτούρας ευθύνης δίνει τη δυνατότητα στους οργανισμούς του δημόσιου τομέα να επιβεβαιώσουν την αφοσίωσή τους στη διαφύλαξη των προσωπικών δεδομένων και των ατομικών δικαιωμάτων.

Η σύνδεση μεταξύ διαφάνειας και λογοδοσίας ενισχύεται αμοιβαία. Η διαφάνεια προάγει τη λογοδοσία καθιστώντας τις πρακτικές δεδομένων ορατές στο κοινό, διευκολύνοντας έτσι την εξέταση της οργανωτικής συμπεριφοράς από τα ενδιαφερόμενα μέρη⁷⁸. Όταν οι πολίτες μπορούν

⁷⁷ Gonçalves, M. E. (2017). The EU data protection reform and the challenges of big data: Remaining uncertainties and ways forward. *Information & Communications Technology Law*, 26(2), 90–115. <https://doi.org/10.1080/13600834.2017.1295838>

⁷⁸ Panjwani, M., & Jäntti, M. (2017). Data protection & security challenges in digital & it services: A case study. *2017 International Conference on Computer and Applications (ICCA)*, 379–383. <https://doi.org/10.1109/COMAPP.2017.8079790>

να λάβουν πληροφορίες σχετικά με τη διαχείριση των δεδομένων τους, είναι πιο διατεθειμένοι να ζητούν από τους δημόσιους οργανισμούς υπεύθυνους για τη συμπεριφορά τους. Αυτή η λογοδοσία ενισχύεται με μέτρα που περιλαμβάνουν δημόσιες διαβουλεύσεις, βρόχους ανατροφοδότησης και προσβάσιμους διαύλους για την αναφορά ανησυχιών ή παραπόνων σχετικά με το απόρρητο δεδομένων. Ενισχύοντας τη συμμετοχή των πολιτών, οι οργανισμοί του δημόσιου τομέα μπορούν να αυξήσουν την ανταπόκρισή τους σε δημόσια ζητήματα και να βελτιώνουν διαρκώς τα πρωτόκολλα προστασίας δεδομένων τους.

Επιπλέον, η σημασία της διαφάνειας και της λογοδοσίας σχετίζεται με την αντιμετώπιση περιστατικών και τη διαχείριση παραβάσεων⁷⁹. Οι οργανισμοί υποχρεούνται να ειδοποιούν άμεσα τα επηρεαζόμενα άτομα και τις αρμόδιες εποπτικές αρχές σε περίπτωση παραβίασης δεδομένων. Η σαφήνεια στην επικοινωνία είναι απαραίτητη για τη διατήρηση της εμπιστοσύνης του κοινού, καθώς καταδεικνύει τη σοβαρότητα του οργανισμού σχετικά με την παραβίαση και την αφοσίωσή του στην επίλυση του ζητήματος. Επιπλέον, οι εκτενείς αξιολογήσεις μετά το περιστατικό και η διάδοση των ευρημάτων μπορούν να αυξήσουν τη λογοδοσία παρουσιάζοντας τον τρόπο με τον οποίο οι γνώσεις που αποκτήθηκαν από την παραβίαση θα χρησιμοποιηθούν για την αποφυγή μελλοντικών συμβάντων.

Η έννοια της λογοδοσίας περιλαμβάνει την ανάγκη για τους οργανισμούς του δημόσιου τομέα να διενεργούν συχνούς ελέγχους και αξιολογήσεις των διαδικασιών προστασίας δεδομένων τους. Οι ανεξάρτητες αξιολογήσεις μπορούν να δώσουν σημαντικές πληροφορίες σχετικά με την αποτελεσματικότητα των πρακτικών διαχείρισης δεδομένων, να εντοπίσουν τομείς που απαιτούν βελτίωση και να εγγυηθούν την τήρηση των νομικών υποχρεώσεων. Επιδιώκοντας προληπτικά εξωτερικές αξιολογήσεις και αποκαλύπτοντας με διαφάνεια τα αποτελέσματα, οι οργανισμοί μπορούν να επιδείξουν την αφοσίωσή τους στη συνεχή βελτίωση και να καλλιεργήσουν αυξημένη εμπιστοσύνη του κοινού.

⁷⁹ Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, 21(5), 510–524. <https://doi.org/10.1108/DPRG-05-2019-0039>

Κεφάλαιο 5: Βέλτιστες πρακτικές, συστάσεις και μελλοντικές κατευθύνσεις

5.1. Βέλτιστες πρακτικές για την προστασία των δεδομένων στον δημόσιο τομέα

5.1.1. Εφαρμογή ισχυρών πλαισίων διακυβέρνησης

Η θέσπιση ισχυρών πλαισίων διακυβέρνησης για την προστασία δεδομένων είναι ζωτικής σημασίας για τους οργανισμούς του δημόσιου τομέα να χειρίζονται αποτελεσματικά και να διασφαλίζουν τα προσωπικά δεδομένα⁸⁰. Ένα ολοκληρωμένο πλαίσιο διακυβέρνησης δημιουργεί τις βασικές δομές, κανόνες και διαδικασίες που εγγυώνται την τήρηση της νομοθεσίας για την προστασία των δεδομένων, προάγοντας παράλληλα μια κουλτούρα ευθύνης και διαφάνειας. Ένα πλαίσιο διακυβέρνησης στοχεύει ουσιαστικά στη θέσπιση ρόλων και καθηκόντων, να σκιαγραφεί τις διαδικασίες διαχείρισης δεδομένων και να προσφέρει μια οριστική διαδικασία για τη λήψη αποφάσεων σχετικά με θέματα προστασίας δεδομένων.

Ένα θεμελιώδες συστατικό ενός αποτελεσματικού συστήματος διακυβέρνησης είναι η δημιουργία ρητών μηχανισμών ηγεσίας και λογοδοσίας. Οι οργανισμοί του δημόσιου τομέα πρέπει να διορίζουν Υπεύθυνους Προστασίας Δεδομένων (DPO) ή ισοδύναμες θέσεις για να επιβλέπουν τη συμμόρφωση με την προστασία δεδομένων και να εγγυώνται τη συμμόρφωση με τους σχετικούς κανόνες, συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Αυτό το προσωπικό είναι απαραίτητο για την καθοδήγηση των σχεδίων προστασίας δεδομένων, τη διενέργεια αξιολογήσεων κινδύνου και τη δράση ως σύνδεσμοι για εσωτερικούς ενδιαφερόμενους φορείς και εξωτερικές ρυθμιστικές οντότητες⁸¹. Ορίζοντας ορισμένα άτομα υπεύθυνα για την προστασία δεδομένων, οι οργανισμοί μπορούν να θεσπίσουν μια κεντρική στρατηγική που ενισχύει την εποπτεία και προάγει μια κουλτούρα συμμόρφωσης.

Ένα ισχυρό σύστημα διακυβέρνησης θα πρέπει να περιλαμβάνει διαλειτουργικές ομάδες εκπροσώπων από διάφορα τμήματα, συμπεριλαμβανομένων των IT, των νομικών, των ανθρώπινων πόρων και της συμμόρφωσης, παράλληλα με τις ηγετικές ευθύνες⁸². Αυτή η διεπιστημονική προσέγγιση εγγυάται την ενσωμάτωση θεμάτων προστασίας δεδομένων σε κάθε πτυχή των λειτουργιών του οργανισμού, περιλαμβάνοντας το σχεδιασμό συστημάτων και διαδικασιών καθώς και τη διαχείριση προσωπικών δεδομένων σε καθημερινές δραστηριότητες. Αυτή η συνεργασία επιτρέπει στους οργανισμούς να αντιμετωπίζουν ολοκληρωμένα τα ζητήματα προστασίας δεδομένων, μειώνοντας την πιθανότητα σιλό που μπορεί να οδηγήσει σε αποτυχίες συμμόρφωσης ή ασυνεπείς πολιτικές.

⁸⁰ Φράγκου, Α. (2018). *Οι προοπτικές της διοικητικής μεταρρύθμισης στην Ελλάδα: ο ρόλος της συγκριτικής αξιολόγησης (Benchmarking) με βάση την εργαλειοθήκη του ΟΟΣΑ και τις βέλτιστες πρακτικές της Ε. Ε.* <http://dspace.lib.uom.gr/handle/2159/23062>

⁸¹ Panjwani, M., & Jäntti, M. (2017). Data protection & security challenges in digital & it services: A case study. *2017 International Conference on Computer and Applications (ICCA)*, 379–383. <https://doi.org/10.1109/COMAPP.2017.8079790>

⁸² Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, 34(4), 157–170. <https://doi.org/10.1016/j.tele.2017.01.008>

Επιπλέον, οι αποτελεσματικές πολιτικές και διαδικασίες αποτελούν βασικά στοιχεία ενός ισχυρού συστήματος διακυβέρνησης. Αυτές οι συμφωνίες πρέπει να οριοθετούν την αφοσίωση του οργανισμού στην προστασία δεδομένων, περιλαμβάνοντας ρητά πρωτόκολλα για τη συλλογή, την αποθήκευση, την επεξεργασία, την κοινή χρήση και τη διατήρηση δεδομένων⁸³. Οι πολιτικές πρέπει να προσδιορίζουν τη διαχείριση των παραβιάσεων δεδομένων, διασφαλίζοντας ότι όλο το προσωπικό είναι ενημερωμένο για τις μεθόδους αναφοράς περιστατικών και ταχείας απόκρισης. Η συνεπής αξιολόγηση και αναθεώρηση αυτών των κανόνων είναι ζωτικής σημασίας για την προσαρμογή των μεταβαλλόμενων νομοθετικών εντολών και της τεχνολογικής προόδου. Οι οργανισμοί πρέπει να διασφαλίσουν ότι οι εργαζόμενοι εκπαιδεύονται σχετικά με αυτές τις πολιτικές και κατανοούν τις ευθύνες τους όσον αφορά την προστασία των προσωπικών δεδομένων.

Οι πρωτοβουλίες κατάρτισης και ευαισθητοποίησης είναι απαραίτητες για την ενθάρρυνση μιας κουλτούρας προστασίας δεδομένων εντός του οργανισμού. Όλοι οι εργαζόμενοι πρέπει να εκπαιδεύονται τακτικά στις αρχές προστασίας δεδομένων, δίνοντας έμφαση στην ανάγκη διασφάλισης προσωπικών δεδομένων και κατανόησης των ατομικών δικαιωμάτων βάσει της νομοθεσίας περί προστασίας δεδομένων. Αυτή η εκπαίδευση όχι μόνο παρέχει στο προσωπικό τις απαραίτητες πληροφορίες για την εκτέλεση των καθηκόντων του, αλλά επίσης ενισχύει την αφοσίωση του οργανισμού στην προστασία δεδομένων ως συλλογική υποχρέωση. Η συμμετοχή των εργαζομένων σε συνομιλίες σχετικά με την προστασία δεδομένων μπορεί να ενισχύσει μια προορατική στάση για τον εντοπισμό κινδύνου και τη βελτίωση της πρακτικής, με αποτέλεσμα ένα πιο ασφαλές περιβάλλον δεδομένων.

Ζωτική συνιστώσα της θέσπισης ενός ισχυρού συστήματος διακυβέρνησης είναι η δημιουργία διαδικασιών για την παρακολούθηση και τον έλεγχο της συμμόρφωσης. Οι τακτικοί έλεγχοι επιτρέπουν στους οργανισμούς να αξιολογούν την αποτελεσματικότητα των μέτρων προστασίας δεδομένων τους, να εντοπίζουν πιθανούς κινδύνους και να επιβεβαιώνουν τη συνεπή τήρηση της πολιτικής. Αυτές οι αξιολογήσεις θα πρέπει να εκτελούνται από εσωτερικές ομάδες ή ανεξάρτητους τρίτους για να διασφαλιστεί η αμερόληπτη επανεξέταση των πρωτοβουλιών συμμόρφωσης του οργανισμού. Μέσω της τακτικής εποπτείας των πολιτικών προστασίας δεδομένων, οι οργανισμοί μπορούν να κάνουν τεκμηριωμένες κρίσεις σχετικά με ουσιαστικές βελτιώσεις και τροποποιήσεις στο πλαίσιο διακυβέρνησής τους.

Σε τελική ανάλυση, η συμπερίληψη των ενδιαφερομένων, όπως οι κάτοικοι και οι κοινοτικές οργανώσεις, αποτελεί κρίσιμο συστατικό μιας αποτελεσματικής δομής διακυβέρνησης. Οι οργανισμοί του δημόσιου τομέα θα πρέπει να συμμετέχουν σε διαφανή επικοινωνία με το κοινό σχετικά με τις διαδικασίες προστασίας των δεδομένων τους και να ζητούν προληπτικά σχόλια για βελτίωση. Αυτή η συμμετοχή μπορεί να καλλιεργήσει εμπιστοσύνη και συνεργασία, καθώς οι κάτοικοι αντιλαμβάνονται ότι τα ζητήματά τους αναγνωρίζονται και αντιμετωπίζονται. Επιπλέον, η εμπλοκή των ενδιαφερομένων σε διαλόγους για το απόρρητο των δεδομένων μπορεί να

⁸³ Ανατολίτης, Θ. (2024). *Μέτρηση του βαθμού ευαισθητοποίησης των εργαζομένων στο δημόσιο τομέα της Ελλάδας σε θέματα ασφάλειας πληροφοριακών συστημάτων*. <https://doi.org/10.26265/polynoe-6713>

αποφέρει σημαντικές γνώσεις που οδηγούν στη διαμόρφωση πολιτικής και βελτιώνουν τις συνολικές πρακτικές.

5.1.2. Προγράμματα κατάρτισης και ευαισθητοποίησης

Οι πρωτοβουλίες κατάρτισης και ευαισθητοποίησης αποτελούν βασικά στοιχεία μιας αποτελεσματικής πολιτικής προστασίας δεδομένων στον δημόσιο τομέα⁸⁴. Καθώς οι οργανισμοί εξαρτώνται όλο και περισσότερο από τις ψηφιακές τεχνολογίες για τη διαχείριση προσωπικών δεδομένων, η ανάγκη για εκτεταμένα προγράμματα κατάρτισης καθίσταται απαραίτητη⁸⁵. Αυτά τα εργαστήρια επιδιώκουν να παρέχουν στους εργαζόμενους σε όλα τα επίπεδα τις απαραίτητες γνώσεις και δεξιότητες για την κατανόηση των ευθυνών τους στην προστασία δεδομένων και για την πλοήγηση στις περιπλοκές της νομοθεσίας περί απορρήτου και των οργανωτικών κανόνων. Καλλιεργώντας μια κουλτούρα ευαισθητοποίησης και υπευθυνότητας, τα προγράμματα κατάρτισης μπορούν να βελτιώσουν σημαντικά την ικανότητα ενός οργανισμού να προστατεύει τις προσωπικές πληροφορίες και να μειώνει τους κινδύνους που συνδέονται με παραβιάσεις δεδομένων.

Ο κύριος στόχος των προγραμμάτων εκπαίδευσης και ευαισθητοποίησης είναι η ενημέρωση των εργαζομένων σχετικά με τις αρχές προστασίας δεδομένων, τονίζοντας τη σημασία της προστασίας των προσωπικών δεδομένων, την κατανόηση των ατομικών δικαιωμάτων και τον εντοπισμό πιθανών ανησυχιών για την ασφάλεια των δεδομένων. Οι εργαζόμενοι πρέπει να κατανοούν τα νομικά πλαίσια που διέπουν την προστασία δεδομένων, συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), και τις επιπτώσεις αυτών των κανονισμών στις καθημερινές τους ευθύνες. Η παροχή ρητών και συνοπτικών πληροφοριών σχετικά με αυτές τις απαιτήσεις αποσαφηνίζει τις περιπλοκές της προστασίας δεδομένων και παρακινεί τους εργαζόμενους να αναλάβουν την ευθύνη για τις πολιτικές διαχείρισης δεδομένων τους.

Επιπλέον, τα προγράμματα κατάρτισης πρέπει να προσαρμόζονται για να ανταποκρίνονται στις ξεχωριστές απαιτήσεις διαφορετικών ρόλων εντός του οργανισμού. Διαφορετικό προσωπικό μπορεί να εμπλακεί με προσωπικά δεδομένα με διάφορους τρόπους και η εκπαίδευσή του θα πρέπει να ανταποκρίνεται αντίστοιχα σε αυτές τις διακρίσεις⁸⁶. Για παράδειγμα, όσοι διαχειρίζονται ευαίσθητες πληροφορίες, όπως αρχεία υγειονομικής περίθαλψης ή οικονομικά δεδομένα, ενδέχεται να απαιτούν πιο εξειδικευμένη εκπαίδευση από εκείνους που βρίσκονται σε διοικητικές θέσεις. Δημιουργώντας εξειδικευμένο εκπαιδευτικό υλικό που εστιάζεται στα ξεχωριστά καθήκοντα κάθε θέσης, οι οργανισμοί μπορούν να εγγυηθούν ότι όλοι οι εργαζόμενοι κατανοούν τα καθήκοντά τους και είναι έτοιμοι να τηρήσουν τις βέλτιστες πρακτικές.

Για να ενισχυθεί η αποτελεσματικότητα των πρωτοβουλιών κατάρτισης και ευαισθητοποίησης, οι οργανισμοί του δημόσιου τομέα θα πρέπει να εφαρμόζουν ποικίλους τρόπους κατάρτισης. Αυτό περιλαμβάνει προσωπικά σεμινάρια, διαδικτυακά μαθήματα και

⁸⁴ Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, 34(4), 157–170. <https://doi.org/10.1016/j.tele.2017.01.008>

⁸⁵ Ανατολίτης, Θ. (2024). *Μέτρηση του βαθμού ευαισθητοποίησης των εργαζομένων στο δημόσιο τομέα της Ελλάδας σε θέματα ασφάλειας πληροφοριακών συστημάτων*. <https://doi.org/10.26265/polynoe-6713>

⁸⁶ Wong, J., Henderson, T., & Ball, K. (2022). Data protection for the common good: Developing a framework for a data protection-focused data commons. *Data & Policy*, 4, e3. <https://doi.org/10.1017/dap.2021.40>

διαδραστικά διαδικτυακά σεμινάρια, τα οποία καλύπτουν διαφορετικές μαθησιακές προτιμήσεις και είναι διαθέσιμα πολλές φορές. Η ενσωμάτωση πραγματικών καταστάσεων και περιπτώσιολογικών περιπτώσεων σε εκπαιδευτικές συνεδρίες βοηθά τους υπαλλήλους να κατανοήσουν τις πρακτικές συνέπειες των κανόνων απορρήτου δεδομένων και τις πιθανές επιπτώσεις της μη συμμόρφωσης⁸⁷. Η συμμετοχή του προσωπικού σε διαδραστικές δραστηριότητες και συζητήσεις μπορεί να βελτιώσει τη διατήρηση πληροφοριών και να προωθήσει μια συλλογική προσέγγιση για την προστασία των δεδομένων.

Η συνεχής αναθεώρηση του εκπαιδευτικού υλικού είναι κρίσιμη συνιστώσα των καλών πρωτοβουλιών κατάρτισης και ευαισθητοποίησης. Καθώς τα πρότυπα προστασίας δεδομένων προχωρούν και ανακύπτουν νέοι κίνδυνοι, είναι επιτακτική ανάγκη για τους οργανισμούς να διατηρήσουν το νόμισμα του εκπαιδευτικού τους περιεχομένου. Αυτό συνεπάγεται την ενοποίηση πληροφοριών σχετικά με πρόσφατες παραβιάσεις δεδομένων, τεχνικές καινοτομίες και τροποποιήσεις σε νομικές εντολές. Οι οργανισμοί μπορούν να εγγυηθούν ότι οι εργαζόμενοι εκπαιδεύονται για τις πιο πρόσφατες εξελίξεις στην προστασία δεδομένων και είναι εξοπλισμένοι για να ανταποκρίνονται αποτελεσματικά σε οποιουσδήποτε κινδύνους προσφέροντας συνεχή εκπαίδευση και ανανέωση.

Επιπλέον, οι οργανισμοί πρέπει να καλλιεργήσουν μια κουλτούρα διαρκούς μάθησης και διαφάνειας σχετικά με την προστασία δεδομένων. Η διευκόλυνση των συζητήσεων του προσωπικού για θέματα προστασίας δεδομένων, η ανταλλαγή πληροφοριών και η έκφραση ανησυχιών καλλιεργεί μια ατμόσφαιρα συνεργασίας που δίνει προτεραιότητα στην ασφάλεια των δεδομένων. Αυτό θα μπορούσε να επιτευχθεί μέσω συχνών συναντήσεων ομάδας, ενημερωτικών δελτίων ή εξειδικευμένων φόρουμ όπου το προσωπικό μπορεί να μοιραστεί ιδέες και εμπειρίες σχετικά με την προστασία δεδομένων⁸⁸. Η καλλιέργεια μιας κουλτούρας λογοδοσίας και υποστήριξης ενθαρρύνει τους υπαλλήλους να προστατεύουν προληπτικά τα προσωπικά δεδομένα και ενισχύει τη δέσμευση του οργανισμού για κοινή ευθύνη στην ασφάλεια των δεδομένων.

Η αξιολόγηση και η κριτική είναι ουσιαστικά στοιχεία οποιασδήποτε πρωτοβουλίας κατάρτισης και ευαισθητοποίησης. Οι οργανισμοί θα πρέπει να αξιολογούν την αποτελεσματικότητα των εκπαιδευτικών προγραμμάτων τους μέσω ερωτηματολογίων, κουίζ και αξιολογήσεων απόδοσης. Οι οργανισμοί μπορούν να βελτιώσουν τα προγράμματά τους ζητώντας ανατροφοδότηση από τους εργαζόμενους σχετικά με το περιεχόμενο και την παράδοση της εκπαίδευσης, εντοπίζοντας έτσι τομείς προς βελτίωση⁸⁹. Επιπλέον, η παρακολούθηση των μετρήσεων συμμόρφωσης και των αναφορών συμβάντων βοηθά στην αξιολόγηση της αποτελεσματικότητας των εκπαιδευτικών πρωτοβουλιών για τον μετριασμό των παραβιάσεων δεδομένων και τη βελτίωση της συνολικής ασφάλειας δεδομένων.

5.1.3. Τεχνολογικές καινοτομίες για την ασφάλεια των δημόσιων δεδομένων

⁸⁷ Panjwani, M., & Jäntti, M. (2017). Data protection & security challenges in digital & it services: A case study. *2017 International Conference on Computer and Applications (ICCA)*, 379–383. <https://doi.org/10.1109/COMAPP.2017.8079790>

⁸⁸ Φράγκου, Α. (2018). *Οι προοπτικές της διοικητικής μεταρρύθμισης στην Ελλάδα: ο ρόλος της συγκριτικής αξιολόγησης (Benchmarking) με βάση την εργαλειοθήκη του οοσα και τις βέλτιστες πρακτικές της ε. Ε.* <http://dspace.lib.uom.gr/handle/2159/23062>

⁸⁹ Wong, J., Henderson, T., & Ball, K. (2022). Data protection for the common good: Developing a framework for a data protection-focused data commons. *Data & Policy*, 4, e3. <https://doi.org/10.1017/dap.2021.40>

Οι τεχνολογικές εξελίξεις είναι απαραίτητες για τη βελτίωση της ασφάλειας των δημόσιων δεδομένων, τον εξοπλισμό των οργανισμών με τα μέσα για την προστασία ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις και διάφορους κινδύνους για την ασφάλεια στον κυβερνοχώρο⁹⁰. Καθώς οι οργανισμοί του δημόσιου τομέα εξαρτώνται όλο και περισσότερο από ψηφιακά συστήματα για αποθήκευση και επεξεργασία δεδομένων, η χρήση σύγχρονων τεχνολογιών έχει καταστεί ζωτικής σημασίας για τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των προσωπικών πληροφοριών. Χρησιμοποιώντας νέες λύσεις, τα δημόσια ιδρύματα μπορούν να ενισχύσουν τις πρωτοβουλίες τους για την προστασία των δεδομένων και να αντιμετωπίσουν με επιτυχία το μεταβαλλόμενο τοπίο των απειλών στον κυβερνοχώρο.

Μια σημαντική τεχνολογική πρόοδος στη διαφύλαξη των δημόσιων δεδομένων είναι η εφαρμογή της κρυπτογράφησης. Η κρυπτογράφηση μετατρέπει ευαίσθητες πληροφορίες σε κωδικοποιημένη μορφή, προσβάσιμη αποκλειστικά σε εξουσιοδοτημένο προσωπικό που διαθέτει τα κατάλληλα κλειδιά αποκρυπτογράφησης⁹¹. Αυτή η διαδικασία μειώνει σημαντικά την πιθανότητα παραβίασης δεδομένων, καθώς μη εξουσιοδοτημένα άτομα, ακόμη και αν λάβουν κρυπτογραφημένες πληροφορίες, δεν μπορούν να τις αποκρυπτογραφήσουν χωρίς τα απαραίτητα κλειδιά. Οι οργανισμοί του δημόσιου τομέα μπορούν να χρησιμοποιούν κρυπτογράφηση σε πολλαπλές φάσεις διαχείρισης δεδομένων, που περιλαμβάνουν τόσο τη μεταφορά δεδομένων όσο και την αποθήκευση δεδομένων σε βάσεις δεδομένων. Τα ιδρύματα μπορούν να ενισχύσουν την ασφάλεια των στοιχείων του ενεργητικού τους και να διασφαλίσουν την τήρηση των κανόνων προστασίας δεδομένων κρυπτογραφώντας τις προσωπικές πληροφορίες.

Μια σημαντική πρόοδος είναι η εφαρμογή της τεχνητής νοημοσύνης (AI) και της τεχνολογίας μηχανικής μάθησης για τη βελτίωση των δυνατοτήτων ανίχνευσης και απόκρισης απειλών. Αυτές οι τεχνολογίες μπορούν να επεξεργάζονται εκτεταμένα δεδομένα σε πραγματικό χρόνο, εντοπίζοντας μοτίβα και ανωμαλίες που μπορεί να υποδηλώνουν πιθανές παραβιάσεις της ασφάλειας. Μέσω της χρήσης λύσεων που βασίζονται στην τεχνητή νοημοσύνη, οι οργανισμοί του δημόσιου τομέα μπορούν να επιτηρούν ενεργά τα συστήματά τους για ανώμαλες συμπεριφορές, επιτρέποντας άμεσες απαντήσεις σε αναδυόμενους κινδύνους. Οι αλγόριθμοι τεχνητής νοημοσύνης μπορούν να εκπαιδευτούν ώστε να αναγνωρίζουν την τυπική συμπεριφορά των χρηστών και να ειδοποιούν τυχόν ανωμαλίες, όπως απόπειρες μη εξουσιοδοτημένης πρόσβασης ή άτυπες μεταφορές δεδομένων. Αυτή η προληπτική στρατηγική στον τομέα της κυβερνοασφάλειας μπορεί να μειώσει σημαντικά τους κινδύνους που συνδέονται με παραβιάσεις δεδομένων και να βελτιώσει τη συνολική στάση ασφάλειας.

Επιπλέον, η καθιέρωση ασφαλών ελέγχων πρόσβασης είναι απαραίτητη για την προστασία των δημόσιων δεδομένων. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) είναι μια εφεύρεση που ενισχύει την ασφάλεια απαιτώντας από τους χρήστες να παρουσιάζουν διάφορα

⁹⁰ Ανατολίτης, Θ. (2024). *Μέτρηση του βαθμού ευαισθητοποίησης των εργαζομένων στο δημόσιο τομέα της Ελλάδας σε θέματα ασφάλειας πληροφοριακών συστημάτων*. <https://doi.org/10.26265/polynoe-6713>

⁹¹ Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, 34(4), 157–170. <https://doi.org/10.1016/j.tele.2017.01.008>

είδη επαλήθευσης πριν από την πρόσβαση σε ευαίσθητες πληροφορίες. Αυτό μπορεί να περιλαμβάνει έναν συνδυασμό κωδικών πρόσβασης, βιομετρικών δεδομένων ή κωδικών μίας χρήσης που μεταδίδονται σε μια κινητή συσκευή. Η εφαρμογή ΜΧΣ επιτρέπει στους οργανισμούς του δημόσιου τομέα να μειώνουν σημαντικά την πιθανότητα μη εξουσιοδοτημένης πρόσβασης, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να εμπλακούν με προσωπικά δεδομένα. Οι ισχυροί έλεγχοι πρόσβασης, μαζί με τις άδειες που βασίζονται σε ρόλους, επιτρέπουν στους οργανισμούς να περιορίζουν την πρόσβαση σε δεδομένα σε εξουσιοδοτημένα άτομα, μειώνοντας έτσι τον κίνδυνο εσωτερικών απειλών και ανθρώπινου λάθους.

Οι τεχνολογίες πρόληψης απώλειας δεδομένων (DLP) είναι ζωτικής σημασίας για τη διαφύλαξη των δημόσιων δεδομένων. Οι λύσεις DLP επιβλέπουν τα δεδομένα κατά τη μετάδοση και την αποθήκευση, εντοπίζοντας και αποτρέποντας οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση ή διάδοση ευαίσθητων πληροφοριών. Αυτές οι μέθοδοι μπορούν να μετριάσουν τις παραβιάσεις δεδομένων που προκύπτουν από ακούσια κοινή χρήση, ακατάλληλα διαμορφωμένα συστήματα ή κακόβουλες εσωτερικές δραστηριότητες. Μέσω της χρήσης λύσεων DLP, οι φορείς του δημόσιου τομέα μπορούν να επιβάλλουν αποτελεσματικότερα τους κανονισμούς προστασίας δεδομένων, διασφαλίζοντας έτσι την ασφάλεια και τη συμμόρφωση με τους κανονισμούς των προσωπικών πληροφοριών.

Επιπλέον, η εφαρμογή της τεχνολογίας blockchain προσφέρει μια επαναστατική μέθοδο για την ενίσχυση της ασφάλειας δεδομένων στον δημόσιο τομέα. Το Blockchain προσφέρει ένα αποκεντρωμένο και αμετάβλητο καθολικό για την καταγραφή συναλλαγών, καθιστώντας το εγγενώς ασφαλές έναντι μη εξουσιοδοτημένων αλλαγών. Αυτή η τεχνολογία είναι εφαρμόσιμη σε πολλούς τομείς του δημόσιου τομέα, όπως τα μητρώα ιδιοκτησίας, τα συστήματα διαχείρισης ταυτότητας και τα δημόσια αρχεία. Οι οργανισμοί μπορούν να ενισχύσουν την ακεραιότητα των δεδομένων και τη λογοδοσία χρησιμοποιώντας το blockchain, διασφαλίζοντας ότι τα προσωπικά στοιχεία προστατεύονται και επαληθεύονται.

Οι συνεργασίες με εταιρείες κυβερνοασφάλειας και η χρήση λύσεων υπολογιστικού νέφους μπορούν να βελτιώσουν τις πρωτοβουλίες προστασίας δεδομένων. Οι οργανισμοί του δημόσιου τομέα μπορούν να συνεργάζονται με εξειδικευμένες εταιρείες κυβερνοασφάλειας για την ανάπτυξη προηγμένων πρωτοκόλλων ασφαλείας και την πραγματοποίηση αξιολογήσεων ρουτίνας ασφαλείας. Επιπλέον, οι πάροχοι υπηρεσιών cloud παρέχουν συχνά εξελιγμένες δυνατότητες ασφαλείας, όπως αυτόματες αναβαθμίσεις, λύσεις δημιουργίας αντιγράφων ασφαλείας και ενσωματωμένα εργαλεία συμμόρφωσης, τα οποία μπορούν να ενισχύσουν σημαντικά την ασφάλεια δεδομένων για τους δημόσιους οργανισμούς⁹². Οι οργανισμοί μπορούν να χρησιμοποιήσουν την τεχνολογία cloud για να αποκτήσουν επεκτάσιμες και ευέλικτες λύσεις που προσαρμόζονται στις εξελισσόμενες απαιτήσεις προστασίας δεδομένων τους.

Σε τελική ανάλυση, τα συστήματα συνεχούς επιτήρησης και αντιμετώπισης συμβάντων είναι απαραίτητα για τη διασφάλιση της ασφάλειας των δεδομένων στον δημόσιο τομέα. Οι οργανισμοί θα πρέπει να εφαρμόζουν συστήματα πληροφοριών ασφαλείας και διαχείρισης

⁹² Wong, J., Henderson, T., & Ball, K. (2022). Data protection for the common good: Developing a framework for a data protection-focused data commons. *Data & Policy*, 4, e3. <https://doi.org/10.1017/dap.2021.40>

συμβάντων (SIEM) που παρέχουν παρακολούθηση και ανάλυση σε πραγματικό χρόνο των συναγερμών ασφαλείας που παράγονται από υλικό και εφαρμογές. Μέσω της εφαρμογής των συστημάτων SIEM, οι οργανισμοί του δημόσιου τομέα μπορούν να επιτύχουν εκτεταμένη ορατότητα στο τοπίο ασφαλείας τους, επιτρέποντας την έγκαιρη απόκριση συμβάντων και τον μετριασμό των ζημιών.

5.2. Συστάσεις πολιτικής

5.2.1. Βελτίωση των κανονιστικών πλαισίων

Η ενίσχυση των ρυθμιστικών πλαισίων είναι ζωτικής σημασίας για την ενίσχυση της αποτελεσματικότητας της προστασίας δεδομένων στον δημόσιο τομέα. Καθώς ο όγκος και η πολυπλοκότητα της διαχείρισης προσωπικών δεδομένων αυξάνεται, τα νομοθετικά πλαίσια πρέπει να προσαρμοστούν για την αντιμετώπιση νέων ζητημάτων, τεχνολογιών και απειλών που σχετίζονται με το απόρρητο των δεδομένων⁹³. Τα ισχυρά ρυθμιστικά πλαίσια όχι μόνο θεσπίζουν ρητές οδηγίες για τις οντότητες του δημόσιου τομέα, αλλά καλλιεργούν επίσης μια ατμόσφαιρα που προάγει τη συμμόρφωση, τη λογοδοσία και την εμπιστοσύνη του κοινού.

Ένα ουσιαστικό στοιχείο της ενίσχυσης των ρυθμιστικών πλαισίων είναι η εγγύηση της προσαρμοστικότητας και της ανταπόκρισής τους στην ταχεία πρόοδο της τεχνολογικής καινοτομίας. Ο ψηφιακός κόσμος αλλάζει συνεχώς, με αναδυόμενες τεχνολογίες όπως η τεχνητή νοημοσύνη, η μηχανική μάθηση και η ανάλυση μεγάλων δεδομένων που μεταμορφώνουν τις μεθόδους συλλογής, επεξεργασίας και αποθήκευσης προσωπικών δεδομένων. Κατά συνέπεια, οι ρυθμιστικές αρχές πρέπει να συνεργάζονται με τους ενδιαφερόμενους του κλάδου, τους τεχνολόγους και τους επαγγελματίες νομικούς για να διασφαλίσουν ότι η νομοθεσία ευθυγραμμίζεται με τις σύγχρονες πρακτικές και την τεχνική πραγματικότητα. Αυτή η συνεργατική μέθοδος θα διευκολύνει την ανάπτυξη νομοθεσίας που είναι ταυτόχρονα ρεαλιστική και αποτελεσματική, ενισχύοντας την ισορροπία μεταξύ της καινοτομίας και της διαφύλαξης των προσωπικών δεδομένων.

Επιπλέον, τα ρυθμιστικά συστήματα θα πρέπει να δίνουν έμφαση στη σαφήνεια και την προσβασιμότητα. Οι ρητές ρυθμίσεις βοηθούν τους οργανισμούς του δημόσιου τομέα να κατανοήσουν τις ευθύνες τους, μειώνοντας έτσι την πιθανότητα μη συμμόρφωσης λόγω ασάφειας⁹⁴. Οι οντότητες του δημόσιου τομέα, ανεξάρτητα από το μέγεθος και τους πόρους τους, θα πρέπει να έχουν πρόσβαση σε εμπειριστατωμένες πληροφορίες σχετικά με τις υποχρεώσεις προστασίας δεδομένων. Αυτό μπορεί να περιλαμβάνει εργαλειαθήκες, εγχειρίδια βέλτιστων πρακτικών και μελέτες περιπτώσεων που αποτελούν παράδειγμα της συμμόρφωσης στην πράξη. Ενισχύοντας την προσβασιμότητα των κανόνων, οι οργανισμοί μπορούν να εφαρμόσουν αποτελεσματικότερα μέτρα προστασίας δεδομένων και να καλλιεργήσουν μια κουλτούρα συμμόρφωσης στις δραστηριότητές τους.

⁹³ Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, 34(2), 234–243. <https://doi.org/10.1016/j.clsr.2017.09.001>

⁹⁴ Ανατολίτης, Θ. (2024). *Μέτρηση του βαθμού ευαισθητοποίησης των εργαζομένων στο δημόσιο τομέα της Ελλάδας σε θέματα ασφάλειας πληροφοριακών συστημάτων*. <https://doi.org/10.26265/polynoe-6713>

Ένας κρίσιμος τομέας για βελτίωση είναι η ευθυγράμμιση των ρυθμιστικών πλαισίων τόσο σε εθνικό όσο και σε διεθνές επίπεδο. Η διακρατική διακίνηση δεδομένων, σε συνδυασμό με ποικίλους κανονισμούς, μπορεί να προκαλέσει σύγχυση και να εμποδίσει τις πρωτοβουλίες συμμόρφωσης. Οι οργανισμοί του δημόσιου τομέα λειτουργούν συχνά σε ένα παγκόσμιο πλαίσιο, απαιτώντας μια συνεκτική στρατηγική για την προστασία των δεδομένων. Η εφαρμογή ενιαίων προτύπων σε όλες τις δικαιοδοσίες μπορεί να εξορθολογίσει τη συμμόρφωση για τους οργανισμούς, επιτρέποντάς τους να υιοθετήσουν ένα συνεκτικό σύνολο πρακτικών αντί να διαχειρίζονται μια κατακερματισμένη σειρά απαιτήσεων. Πρωτοβουλίες όπως ο GDPR της ΕΕ έχουν δημιουργήσει τα θεμέλια για την εναρμόνιση. Ωστόσο, απαιτούνται πρόσθετες προσπάθειες για να εξασφαλιστεί ότι τα έθνη συνεργάζονται για την ανάπτυξη κατάλληλων κανόνων προστασίας δεδομένων που υποστηρίζουν τα δικαιώματα της ιδιωτικής ζωής προάγοντας παράλληλα τη διεθνή συνεργασία.

Επιπλέον, η ενίσχυση των διαδικασιών επιβολής εντός των κανονιστικών πλαισίων είναι απαραίτητη για τη διασφάλιση της συμμόρφωσης και την πρόληψη των παραβιάσεων. Οι ρυθμιστικοί φορείς πρέπει να διαθέτουν την απαιτούμενη εξουσία και πόρους για τη διερεύνηση των παραβιάσεων και την επιβολή κατάλληλων κυρώσεων για μη συμμόρφωση. Αυτό μπορεί να περιλαμβάνει όχι μόνο κυρώσεις αλλά και διορθωτικά μέτρα που απαιτούν από τους οργανισμούς να διορθώσουν τις ελλείψεις προστασίας δεδομένων. Μέσω της επίδειξης μιας σταθερής δέσμευσης για αυστηρή επιβολή, οι ρυθμιστικοί φορείς μπορούν να καλλιεργήσουν μια κουλτούρα ευθύνης, ωθώντας τους οργανισμούς του δημόσιου τομέα να αντιμετωπίζουν με σοβαρότητα την προστασία δεδομένων και να δίνουν προτεραιότητα στη συμμόρφωση.

Η δημόσια αλληλεπίδραση είναι ουσιαστικό στοιχείο για την ενίσχυση των ρυθμιστικών καθεστώτων. Οι ρυθμιστικές αρχές θα πρέπει να ζητούν σχόλια από πολίτες, οργανώσεις συνηγορίας και εκπροσώπους του κλάδου κατά τη διαμόρφωση ή την τροποποίηση των κανονισμών⁹⁵. Αυτή η περιεκτική μεθοδολογία εγγυάται την εξέταση πολλών προοπτικών, καταλήγοντας τελικά σε νομοθεσία που ενσωματώνει με μεγαλύτερη ακρίβεια τις δημόσιες αξίες και προσδοκίες σχετικά με την προστασία δεδομένων. Η συμμετοχή του κοινού σε διαλόγους για το απόρρητο δεδομένων ενισχύει τη διαφάνεια και καλλιεργεί την εμπιστοσύνη στις ρυθμιστικές διαδικασίες και αποτελέσματα.

Τέλος, τα προγράμματα κατάρτισης και ανάπτυξης ικανοτήτων για ρυθμιστικούς φορείς είναι ζωτικής σημασίας για τη βελτίωση της αποτελεσματικότητας των κανόνων προστασίας δεδομένων. Οι ρυθμιστικές αρχές πρέπει να παραμένουν ενημερωμένες για τις νεότερες τάσεις, την τεχνολογία και τις βέλτιστες πρακτικές στον τομέα της προστασίας δεδομένων για την αποτελεσματική παρακολούθηση της συμμόρφωσης. Αυτό μπορεί να συνεπάγεται επένδυση στη συνεχή επαγγελματική ανάπτυξη του ρυθμιστικού προσωπικού, παρέχοντάς τους τις απαραίτητες δεξιότητες και γνώσεις για να διαχειρίζονται κατάλληλα τις περιπλοκές του απορρήτου των δεδομένων. Οι οργανισμοί μπορούν να ενισχύσουν τη συνολική αποτελεσματικότητα των

⁹⁵ Lnenicka, M., Kysela, T., & Horák, O. (2025). Building security and resilience: A guide to implementing effective cybersecurity and data protection measures in smart cities. *Smart and Sustainable Built Environment, ahead-of-print*(ahead-of-print). <https://doi.org/10.1108/SASBE-09-2024-0363>

συστημάτων προστασίας δεδομένων στον δημόσιο τομέα διασφαλίζοντας ότι οι ρυθμιστικές αρχές είναι επαρκώς εξοπλισμένες για την αντιμετώπιση αναδυόμενων ανησυχιών.

5.2.2. Ενθάρρυνση συμπράξεων δημόσιου και ιδιωτικού τομέα

Η προώθηση των συμπράξεων δημόσιου και ιδιωτικού τομέα (ΣΔΙΤ) είναι μια στρατηγική μέθοδος για τη βελτίωση του απορρήτου των δεδομένων στον δημόσιο τομέα. Αυτές οι συνεργασίες αξιοποιούν τις δεξιότητες και τις γνώσεις και των δύο τομέων για την επιτυχή αντιμετώπιση των προβλημάτων ασφάλειας δεδομένων και απορρήτου. Καθώς τα θέματα προστασίας δεδομένων γίνονται πιο περίπλοκα λόγω της τεχνολογικής προόδου και των αναδυόμενων κινδύνων, οι Συμπράξεις Δημόσιου και Ιδιωτικού Τομέα (ΣΔΙΤ) παρέχουν ένα πλαίσιο συνεργασίας που προωθεί την καινοτομία, την κοινή χρήση πόρων και την ενισχυμένη συμμόρφωση.

Ένα θεμελιώδες πλεονέκτημα της συνεργασίας δημόσιου-ιδιωτικού τομέα στην προστασία δεδομένων είναι η συγκέντρωση πόρων και εμπειρογνομosύνης. Οι οργανισμοί του δημόσιου τομέα αντιμετωπίζουν συχνά περιορισμούς όσον αφορά τους οικονομικούς πόρους και την τεχνολογική επάρκεια⁹⁶. Αντίθετα, οι εταιρείες του ιδιωτικού τομέα, ιδιαίτερα εκείνες που επικεντρώνονται στην ασφάλεια στον κυβερνοχώρο και την προστασία δεδομένων, περιέχουν εξελιγμένες τεχνολογίες, ικανά άτομα και σημαντική εμπειρία στον μετριασμό των ανησυχιών για την ασφάλεια των δεδομένων. Η συνεργασία με αυτούς τους οργανισμούς επιτρέπει στα δημόσια ιδρύματα να χρησιμοποιούν προηγμένες τεχνολογίες και διαδικασίες, βελτιώνοντας έτσι ουσιαστικά τις διαδικασίες προστασίας δεδομένων τους. Αυτή η συνεργασία μπορεί να εκδηλωθεί σε πολλαπλές μορφές, συμπεριλαμβανομένων των προσπαθειών συνεργασίας, των ερευνητικών συνεργασιών, της ανταλλαγής τεχνολογίας και των προγραμμάτων κατάρτισης.

Επιπλέον, οι συνεργασίες δημόσιου και ιδιωτικού τομέα μπορούν να τονώσουν την καινοτομία στις μεθοδολογίες προστασίας δεδομένων⁹⁷. Ο ιδιωτικός τομέας είναι γενικά πιο ευκίνητος και ανταποκρίνεται στα εξελισσόμενα τεχνολογικά περιβάλλοντα, πρωτοπορώντας συχνά στην ανάπτυξη καινοτόμων λύσεων για τις αυξανόμενες προκλήσεις ασφάλειας δεδομένων. Οι οργανισμοί του δημόσιου τομέα μπορούν να αξιοποιήσουν τις ΣΔΙΤ για την εφαρμογή καινοτόμων τεχνολογιών και πρακτικών που βελτιώνουν τις πρωτοβουλίες τους για την προστασία δεδομένων. Οι συνεργασίες μπορεί να επικεντρωθούν στη δημιουργία εξελιγμένων τεχνικών κρυπτογράφησης, ανθεκτικών συστημάτων ελέγχου ταυτότητας ή αυτοματοποιημένων οργάνων ανίχνευσης απειλών προσαρμοσμένων για τις συγκεκριμένες απαιτήσεις των δημόσιων ιδρυμάτων. Αυτή η συνεχής ανταλλαγή εννοιών και τεχνολογιών μπορεί τελικά να οδηγήσει σε πιο ισχυρές λύσεις προστασίας δεδομένων.

Οι συνεργασίες δημόσιου και ιδιωτικού τομέα μπορούν να ενισχύσουν τις τεχνολογικές ικανότητες ενώ παράλληλα διευκολύνουν τη μεταφορά πληροφοριών και τη διάδοση των βέλτιστων πρακτικών. Ο δημόσιος τομέας μπορεί να αντλήσει γνώσεις από τις εμπειρίες ιδιωτικών οργανισμών που έχουν αντιμετωπίσει ανάλογα ζητήματα στην προστασία των δεδομένων και της

⁹⁶ Φράγκου, Α. (2018). *Οι προοπτικές της διοικητικής μεταρρύθμισης στην Ελλάδα: ο ρόλος της συγκριτικής αξιολόγησης (Benchmarking) με βάση την εργαλειοθήκη του ΟΟΣΑ και τις βέλτιστες πρακτικές της Ε. Ε.* <http://dspace.lib.uom.gr/handle/2159/23062>

⁹⁷ Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, 34(2), 234–243. <https://doi.org/10.1016/j.clsr.2017.09.001>

ιδιωτικής ζωής⁹⁸. Μέσω συνεργατικών φόρουμ, εργαστηρίων και εκπαιδευτικών συνεδριών, και οι δύο τομείς μπορούν να ανταλλάξουν γνώσεις, στρατηγικές και διδάγματα που αποκτήθηκαν. Αυτή η ανταλλαγή γνώσεων βοηθά τους δημόσιους φορείς να κατανοήσουν τις τάσεις του κλάδου, τις νομοθετικές εξελίξεις και τους μελλοντικούς κινδύνους, επιτρέποντάς τους έτσι να εφαρμόσουν προληπτικές ενέργειες για την προστασία των προσωπικών δεδομένων. Επιπλέον, η καλλιέργεια μιας κουλτούρας συνεργασίας μπορεί να ενισχύσει τη δικτύωση μεταξύ των εργαζομένων και των δύο τομέων, ενισχύοντας τις σχέσεις και προωθώντας τη συνεχή συζήτηση για θέματα προστασίας δεδομένων.

Η κανονιστική συμμόρφωση αντιπροσωπεύει έναν άλλο τομέα στον οποίο οι συμπράξεις δημόσιου και ιδιωτικού τομέα μπορούν να ασκήσουν σημαντική επιρροή. Μέσω της συνεργασίας με εταιρείες του ιδιωτικού τομέα, οι δημόσιοι οργανισμοί μπορούν να διαμορφώσουν πλήρεις στρατηγικές συμμόρφωσης που συμμορφώνονται με τις υπάρχουσες απαιτήσεις, συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων και άλλων νόμων περί προστασίας δεδομένων. Οι ιδιωτικές επιχειρήσεις μπορούν να προσφέρουν εξειδικευμένες γνώσεις για τη διέλευση του ρυθμιστικού πλαισίου, βοηθώντας τους δημόσιους φορείς να κατανοήσουν τις ευθύνες τους και να εφαρμόσουν αποτελεσματικές στρατηγικές συμμόρφωσης. Αυτή η στρατηγική συνεργασίας μπορεί να μετριάσει τον κίνδυνο μη συμμόρφωσης και τις σχετικές κυρώσεις, προωθώντας έτσι ένα πιο ασφαλές πλαίσιο προστασίας δεδομένων.

Οι συνεργασίες δημόσιου και ιδιωτικού τομέα μπορούν να ενισχύσουν περαιτέρω την εμπιστοσύνη του κοινού στις πρωτοβουλίες προστασίας δεδομένων. Όταν οι πολίτες γίνονται μάρτυρες εταιρικών σχέσεων μεταξύ της κυβέρνησής τους και αξιολογών εμπορικών επιχειρήσεων, συμβάλλει στην ενίσχυση της διασφάλισης ότι η διαχείριση των προσωπικών τους δεδομένων γίνεται με υπευθυνότητα και ασφάλεια. Η διαφάνεια σε αυτές τις εταιρικές σχέσεις είναι απαραίτητη. Οι οργανισμοί του δημόσιου τομέα πρέπει να μεταφέρουν τους στόχους, τις δραστηριότητες και τα αποτελέσματα αυτών των συνεργασιών στο κοινό. Αυτή η διαφάνεια ενισχύει την εμπιστοσύνη και προωθεί τη συμμετοχή των πολιτών στους διαλόγους για την προστασία των δεδομένων, επιτρέποντας στο κοινό να εκφράσει τις ανησυχίες και τις προσδοκίες του σχετικά με την ιδιωτική ζωή.

Η δημιουργία αποτελεσματικών συμπράξεων δημόσιου και ιδιωτικού τομέα απαιτεί μια σχολαστική προσέγγιση στη διακυβέρνηση και τη λογοδοσία. Πρέπει να δημιουργηθούν ξεκάθαρα πλαίσια για να οριοθετούν τους ρόλους, τις ευθύνες και τις προσδοκίες για όλους τους εμπλεκόμενους φορείς⁹⁹. Οι συμφωνίες προστασίας δεδομένων πρέπει να οριοθετούν τις παραμέτρους της συνεργασίας, διασφαλίζοντας ότι οι εμπορικές επιχειρήσεις συμμορφώνονται με τα ίδια πρότυπα προστασίας δεδομένων που επιβάλλονται για τους δημόσιους οργανισμούς. Επιπλέον, τα συστήματα παρακολούθησης και αξιολόγησης της αποτελεσματικότητας των εταιρικών σχέσεων είναι ζωτικής σημασίας για τη διασφάλιση της επίτευξης των στόχων

⁹⁸ Καβαλλιέρου, Α. (2024). *Διαχείριση ανθρώπινου δυναμικού στο δημόσιο τομέα κατά την περίοδο κρίσεων*. <https://doi.org/10.26265/polynoe-7818>

⁹⁹ Φράγκου, Α. (2018). *Οι προοπτικές της διοικητικής μεταρρύθμισης στην Ελλάδα: ο ρόλος της συγκριτικής αξιολόγησης (Benchmarking) με βάση την εργαλειοθήκη του oosa και τις βέλτιστες πρακτικές της ε. Ε.* <http://dspace.lib.uom.gr/handle/2159/23062>

προστασίας δεδομένων. Οι συχνές αξιολογήσεις μπορούν να εντοπίσουν ευκαιρίες για βελτίωση και να ενισχύσουν την αφοσίωση και των δύο τομέων στην ασφάλεια δεδομένων.

5.3. Μελλοντικές προκλήσεις και ευκαιρίες

5.3.1. Το μέλλον της προστασίας των δεδομένων στην ψηφιακή κοινωνία

Το μέλλον της προστασίας δεδομένων σε έναν ψηφιακό κόσμο αναμένεται να δει ουσιαστικές αλλαγές, επηρεαζόμενες από την τεχνολογική πρόοδο, τις μεταβαλλόμενες προσδοκίες του κοινού και τα ολοένα πιο περίπλοκα νομοθετικά πλαίσια. Καθώς οι ψηφιακές αλληλεπιδράσεις πολλαπλασιάζονται σε πολυάριθμες πτυχές της ζωής —συμπεριλαμβανομένων των κρατικών υπηρεσιών, της υγειονομικής περίθαλψης και της εκπαίδευσης— η σημασία των περιεκτικών μεθόδων προστασίας δεδομένων είναι πρωταρχικής σημασίας¹⁰⁰. Μια προληπτική και προοδευτική στρατηγική για την προστασία των δεδομένων θα είναι ζωτικής σημασίας για την αντιμετώπιση των επερχόμενων προβλημάτων και ευκαιριών.

Μια σημαντική τάση που διαμορφώνει το μέλλον της προστασίας δεδομένων είναι η ταχεία πρόοδος των αναδυόμενων τεχνολογιών, συμπεριλαμβανομένης της τεχνητής νοημοσύνης (AI), της μηχανικής μάθησης και του Διαδικτύου των Πραγμάτων (IoT). Αν και αυτές οι τεχνολογίες παρουσιάζουν σημαντικές ευκαιρίες για την ενίσχυση της αποτελεσματικότητας και της δημιουργικότητας, δημιουργούν επίσης νέες επιπλοκές στη διαχείριση των προσωπικών δεδομένων. Τα συστήματα τεχνητής νοημοσύνης συχνά απαιτούν εκτεταμένα σύνολα δεδομένων για αποτελεσματική εκπαίδευση και λειτουργία, προκαλώντας ανησυχίες σχετικά με την ελαχιστοποίηση των δεδομένων και την πιθανή εκμετάλλευση ευαίσθητων πληροφοριών. Καθώς οι οργανισμοί εξαρτώνται όλο και περισσότερο από την τεχνητή νοημοσύνη για τον έλεγχο των προσωπικών δεδομένων, θα υπάρξει επείγουσα ανάγκη για ηθικούς κανόνες και πλαίσια που να εγγυώνται ότι αυτές οι τεχνολογίες χρησιμοποιούνται με υπευθυνότητα και διαφάνεια. Ο στόχος είναι να αξιοποιηθούν τα πλεονεκτήματα της τεχνητής νοημοσύνης με ταυτόχρονη επιβολή αυστηρών πρωτοκόλλων προστασίας δεδομένων που διασφαλίζουν τη διασφάλιση των δικαιωμάτων απορρήτου των ατόμων.

Επιπλέον, η εμφάνιση συσκευών IoT έχει επιδεινώσει τις προκλήσεις προστασίας δεδομένων. Αυτά τα αλληλένδετα gadget συλλέγουν και αναμεταδίδουν συνεχώς δεδομένα, συχνά χωρίς την επίγνωση ή την επίβλεψη των χρηστών. Με την αυξανόμενη ενσωμάτωση των συσκευών στην καθημερινή ζωή, η ποσότητα και η ποικιλία των προσωπικών δεδομένων που παράγονται θα αυξηθεί, απαιτώντας ολοκληρωμένες λύσεις προστασίας δεδομένων. Οι οργανισμοί πρέπει να εφαρμόζουν διαδικασίες ασφαλείας που καλύπτουν ολόκληρη τη διάρκεια ζωής των δεδομένων που παράγονται από συσκευές IoT, συμπεριλαμβανομένης της συλλογής, αποθήκευσης, κοινής χρήσης και καταστροφής. Αυτό απαιτεί συνεργασία μεταξύ κατασκευαστών, παρόχων υπηρεσιών και ρυθμιστικών φορέων για τη θέσπιση ενδεδειγμένων προτύπων και μεθόδων ασφαλείας για το χειρισμό δεδομένων IoT.

¹⁰⁰ Lnenicka, M., Kysela, T., & Horák, O. (2025). Building security and resilience: A guide to implementing effective cybersecurity and data protection measures in smart cities. *Smart and Sustainable Built Environment, ahead-of-print*(ahead-of-print). <https://doi.org/10.1108/SASBE-09-2024-0363>

Καθώς κλιμακώνεται η κοινωνική ευαισθητοποίηση σχετικά με τα ζητήματα απορρήτου, οι προσδοκίες για διαφάνεια και υπευθυνότητα στις διαδικασίες διαχείρισης δεδομένων θα ενταθούν¹⁰¹. Τα άτομα αποκτούν μεγαλύτερη γνώση των δικαιωμάτων τους σχετικά με τα προσωπικά δεδομένα και τείνουν όλο και περισσότερο να θεωρούν τους οργανισμούς υπεύθυνους για παραβιάσεις και κακή χρήση. Αυτή η αλλαγή στην κοινή γνώμη αναμένεται να επηρεάσει τις ρυθμιστικές εξελίξεις, με αποτέλεσμα πιο αυστηρούς κανόνες και στρατηγικές επιβολής που δίνουν έμφαση στην προστασία των καταναλωτών¹⁰². Οι οργανισμοί πρέπει να δώσουν προτεραιότητα στη διαφάνεια στις πρακτικές δεδομένων τους, αναφέροντας ρητά τον τρόπο με τον οποίο συλλέγονται, χρησιμοποιούνται και διαδίδονται προσωπικά δεδομένα. Καλλιεργώντας μια ατμόσφαιρα εμπιστοσύνης και υπευθυνότητας, οι οργανισμοί μπορούν να βελτιώσουν τη φήμη τους και να ενισχύσουν τις σχέσεις με τους ενδιαφερόμενους.

Η πρόοδος της προστασίας δεδομένων θα διαμορφωθεί από την παγκόσμια δυναμική, καθώς τα έθνη επιμένουν να αντιμετωπίζουν τα ζητήματα που παρουσιάζουν οι διακρατικές ροές δεδομένων. Η αλληλεξάρτηση της ψηφιακής οικονομίας απαιτεί από τους οργανισμούς να ελίσσονται μέσα από ένα περίπλοκο δίκτυο νόμων και κανονισμών για την προστασία δεδομένων σε διάφορες δικαιοδοσίες. Καθώς η προστασία των δεδομένων γίνεται ολοένα και πιο ουσιαστική στο διεθνές εμπόριο και τη διπλωματία, θα υπάρξει συντονισμένη προσπάθεια για την εναρμόνιση των κανονισμών ώστε να καταστεί δυνατή η διασυνοριακή μεταφορά δεδομένων διασφαλίζοντας παράλληλα τη διατήρηση των δικαιωμάτων ιδιωτικής ζωής. Πρωτοβουλίες όπως ο GDPR της Ευρωπαϊκής Ένωσης έχουν δημιουργήσει προηγούμενο για την εναρμόνιση. Ωστόσο, η συνεχής επικοινωνία και συνεργασία μεταξύ των εθνών θα είναι ζωτικής σημασίας για τη δημιουργία ενιαίων πλαισίων που συμβιβάζουν την καινοτομία με την προστασία.

Επιπλέον, καθώς οι απειλές στον κυβερνοχώρο προχωρούν, οι οργανισμοί θα αντιμετωπίσουν αυξημένη ζήτηση για ενίσχυση των πρωτοκόλλων ασφάλειας στον κυβερνοχώρο. Η αύξηση των προηγμένων επιθέσεων στον κυβερνοχώρο που απευθύνονται σε οργανισμούς του δημόσιου και του ιδιωτικού τομέα έχει υπογραμμίσει τις αδυναμίες στα πρωτόκολλα προστασίας δεδομένων. Οι μελλοντικές μέθοδοι προστασίας δεδομένων πρέπει να ενσωματώνουν εξελιγμένες τεχνικές κυβερνοασφάλειας, που θα περιλαμβάνουν την ανίχνευση απειλών, τον σχεδιασμό αντιμετώπισης περιστατικών και τη συνεχή παρακολούθηση¹⁰³. Η χρήση της τεχνητής νοημοσύνης και της μηχανικής μάθησης στην ασφάλεια του κυβερνοχώρου θα βελτιώσει την ικανότητα ανίχνευσης και αντιμετώπισης επιθέσεων σε πραγματικό χρόνο, δημιουργώντας ένα πιο ισχυρό σύστημα προστασίας δεδομένων. Οι οργανισμοί πρέπει να δώσουν προτεραιότητα σε πρωτοβουλίες εκπαίδευσης και ευαισθητοποίησης του προσωπικού για τον μετριασμό των ανθρώπινων παραγόντων που οδηγούν σε παραβιάσεις της ασφάλειας.

¹⁰¹ Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, 34(2), 234–243. <https://doi.org/10.1016/j.clsr.2017.09.001>

¹⁰² Καβαλλιέρου, Α. (2024). *Διαχείριση ανθρώπινου δυναμικού στο δημόσιο τομέα κατά την περίοδο κρίσεων*. <https://doi.org/10.26265/polynoe-7818>

¹⁰³ Φράγκου, Α. (2018). *Οι προοπτικές της διοικητικής μεταρρύθμισης στην Ελλάδα: ο ρόλος της συγκριτικής αξιολόγησης (Benchmarking) με βάση την εργαλειοθήκη του οοσα και τις βέλτιστες πρακτικές της ε. Ε.* <http://dspace.lib.uom.gr/handle/2159/23062>

Δεδομένων αυτών των τάσεων, η σημασία των υπευθύνων προστασίας δεδομένων (DPO) και των ομάδων συμμόρφωσης θα κλιμακωθεί σημαντικά. Αυτοί οι επαγγελματίες πρέπει να παραμένουν ενημερωμένοι σχετικά με την αλλαγή των κανονισμών, τις τεχνικές καινοτομίες και τις βέλτιστες πρακτικές για να εγγυηθούν ότι οι οργανισμοί παραμένουν συμμορφωμένοι και προορατικοί στις πρωτοβουλίες τους για την προστασία δεδομένων. Καθώς οι κανονισμοί προστασίας δεδομένων γίνονται όλο και πιο περίπλοκοι, η επάρκεια των Υπευθύνων Προστασίας Δεδομένων θα είναι απαραίτητη για τη διαχείριση των περιπλοκών συμμόρφωσης και την προώθηση μιας κουλτούρας απορρήτου δεδομένων εντός των οργανισμών.

5.3.2. Αντιμετώπιση αναδυόμενων ζητημάτων προστασίας της ιδιωτικής ζωής

Η αντιμετώπιση των αυξανόμενων ανησυχιών για το απόρρητο είναι απαραίτητη για τους οργανισμούς που λειτουργούν στο τρέχον δυναμικό ψηφιακό περιβάλλον. Καθώς η τεχνολογία εξελίσσεται, οι αναδυόμενες ανησυχίες σχετικά με την προστασία των προσωπικών δεδομένων απαιτούν προληπτικές και ευέλικτες στρατηγικές για τη διασφάλιση των ατομικών δικαιωμάτων απορρήτου. Οι αναδυόμενες προκλήσεις απορρήτου επηρεάζονται από πολλούς λόγους, όπως η πρόοδος της ανάλυσης δεδομένων, η αύξηση των συνδεδεμένων συσκευών και η αυξανόμενη πολυπλοκότητα των απειλών στον κυβερνοχώρο. Οι οργανισμοί πρέπει να δώσουν προτεραιότητα στη συμμόρφωση με τις τρέχουσες απαιτήσεις, ενώ παράλληλα προβλέπουν μελλοντικές αλλαγές στο τοπίο της ιδιωτικής ζωής για να αντιμετωπίσουν σωστά αυτές τις ανησυχίες.

Μια σημαντική αναπτυσσόμενη ανησυχία για το απόρρητο είναι η απόκτηση και η χρήση προσωπικών δεδομένων από συστήματα τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης. Αν και αυτές οι τεχνολογίες παρέχουν σημαντικά οφέλη για την ενίσχυση της αποτελεσματικότητας και της λήψης αποφάσεων, συχνά εξαρτώνται από εκτεταμένα σύνολα δεδομένων, τα οποία μπορεί να περιλαμβάνουν ευαίσθητες προσωπικές πληροφορίες¹⁰⁴. Οι αλγόριθμοι που οδηγούν τα συστήματα τεχνητής νοημοσύνης ενδέχεται να προσθέτουν αθέλητα προκατάληψη, με αποτέλεσμα μεροληπτικά αποτελέσματα που επηρεάζουν τα άτομα με βάση τα δεδομένα τους. Οι οργανισμοί πρέπει να εφαρμόζουν ηθικούς κανόνες για την ανάπτυξη και την ανάπτυξη της τεχνητής νοημοσύνης για να εγγυηθούν ότι οι διαδικασίες συλλογής δεδομένων είναι διαφανείς και δίκαιες. Η εφαρμογή μεθόδων όπως οι αλγοριθμικοί έλεγχοι και οι εκτιμήσεις επιπτώσεων μπορούν να βοηθήσουν στον εντοπισμό πιθανών μεροληψιών και στον μετριασμό των κινδύνων που σχετίζονται με αποφάσεις που βασίζονται στην τεχνητή νοημοσύνη.

Μια αυξανόμενη ανησυχία για το απόρρητο είναι η κλιμακούμενη προβολή των τεχνολογιών παρακολούθησης και επιτήρησης δεδομένων. Η ικανότητα παρακολούθησης των δραστηριοτήτων των ατόμων έχει αυξηθεί δραματικά, περιλαμβάνοντας τα cookies, την παρακολούθηση μέσω κινητού τηλεφώνου, την αναγνώριση προσώπου και τις υπηρεσίες γεωγραφικού εντοπισμού. Αν και αυτές οι τεχνολογίες μπορούν να αυξήσουν τις εμπειρίες των χρηστών και την καλύτερη παροχή υπηρεσιών, δημιουργούν επίσης σημαντικά προβλήματα απορρήτου. Τα άτομα συχνά δεν έχουν επίγνωση σχετικά με το μέγεθος της συλλογής και της χρήσης δεδομένων, με αποτέλεσμα την παραβίαση της εμπιστοσύνης μεταξύ των οργανισμών και

¹⁰⁴ Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. L., Tirta, R., & Schiffner, S. (2015). *Privacy and Data Protection by Design—From policy to engineering* (arXiv:1501.03726). arXiv. <https://doi.org/10.48550/arXiv.1501.03726>

των χρηστών τους. Οι οργανισμοί θα πρέπει να δώσουν προτεραιότητα στο άνοιγμα συζητώντας ρητά τις διαδικασίες συλλογής δεδομένων τους και παρέχοντας στα άτομα ουσιαστικό έλεγχο επί των δεδομένων τους¹⁰⁵. Η καθιέρωση διαισθητικών ρυθμίσεων απορρήτου και η δυνατότητα απόρριψης της παρακολούθησης στους χρήστες μπορεί να επιτρέψει στους καταναλωτές να λαμβάνουν ενημερωμένες αποφάσεις σχετικά με τα δεδομένα τους.

Η επέκταση του Διαδικτύου των Πραγμάτων (IoT) εισάγει μια πρόσθετη διάσταση περιπλοκών σχετικά με τα ζητήματα απορρήτου¹⁰⁶. Ο πολλαπλασιασμός δικτυωμένων συσκευών που συλλέγουν και αποστέλλουν δεδομένα σε πραγματικό χρόνο αυξάνει σημαντικά τον κίνδυνο παραβίασης δεδομένων και μη εξουσιοδοτημένης πρόσβασης. Πολλές συσκευές IoT εμφανίζουν ανεπαρκή πρωτόκολλα ασφαλείας, γεγονός που τις καθιστά ευάλωτες σε απατεώνες. Ο μετριασμός αυτών των κινδύνων απορρήτου απαιτεί μια ολοκληρωμένη στρατηγική που περιλαμβάνει ασφάλεια συσκευών, κρυπτογράφηση δεδομένων και εκπαίδευση των χρηστών. Οι κατασκευαστές πρέπει να δώσουν προτεραιότητα στη δημιουργία ασφαλών προϊόντων που ενσωματώνουν το απόρρητο με αρχές σχεδιασμού. Επιπλέον, οι οργανισμοί πρέπει να ενημερώνουν τους καταναλωτές για τους πιθανούς κινδύνους που συνδέονται με τις συσκευές IoT και να προωθούν την υιοθέτηση βέλτιστων μεθόδων για την προστασία των προσωπικών τους πληροφοριών.

Οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο αποτελούν σημαντική πρόκληση για τη διατήρηση της ιδιωτικής ζωής στην ψηφιακή εποχή. Καθώς οι επιθέσεις στον κυβερνοχώρο γίνονται όλο και πιο εξελιγμένες και διαδεδομένες, οι οργανισμοί πρέπει να ενισχύσουν την άμυνά τους ενάντια σε παραβιάσεις δεδομένων και μη εξουσιοδοτημένη πρόσβαση. Το ransomware, το ηλεκτρονικό ψάρεμα και άλλες κακόβουλες ενέργειες μπορούν να θέσουν σε κίνδυνο εκτεταμένα προσωπικά δεδομένα, με αποτέλεσμα σημαντικές συνέπειες τόσο για άτομα όσο και για οργανισμούς. Οι οργανισμοί πρέπει να επενδύσουν σε ολοκληρωμένα σχέδια κυβερνοασφάλειας που να περιλαμβάνουν ισχυρή ανίχνευση απειλών, σχεδιασμό αντιμετώπισης περιστατικών και εκπαίδευση εργαζομένων για να μετριάσουν με επιτυχία αυτούς τους κινδύνους. Οι τακτικές αξιολογήσεις ασφαλείας και οι ενημερώσεις λογισμικού/συστήματος μπορούν να εντοπίσουν αδυναμίες και να ενισχύσουν την άμυνα έναντι πιθανών επιθέσεων.

Τα αναδυόμενα ζητήματα απορρήτου εκτείνονται πέρα από τις τεχνολογικές προκλήσεις και περιλαμβάνουν νομικές και ρυθμιστικές επιπτώσεις. Καθώς η νομοθεσία για την προστασία της ιδιωτικής ζωής προχωρά παράλληλα με τις τεχνολογικές βελτιώσεις, οι οργανισμοί πρέπει να κινούνται μέσω ενός περίπλοκου δικτύου περιορισμών που μπορεί να διαφέρουν ανά χώρα. Αυτό μπορεί να δημιουργήσει δυσκολίες στη διατήρηση της συμμόρφωσης, ειδικά για οργανισμούς που λειτουργούν διεθνώς¹⁰⁷. Οι οργανισμοί θα πρέπει να εφαρμόσουν μια διεξοδική δομή συμμόρφωσης που να περιλαμβάνει τις υπάρχουσες απαιτήσεις και να προβλέπει μελλοντικές

¹⁰⁵ Lnenicka, M., Kysela, T., & Horák, O. (2025). Building security and resilience: A guide to implementing effective cybersecurity and data protection measures in smart cities. *Smart and Sustainable Built Environment, ahead-of-print*(ahead-of-print). <https://doi.org/10.1108/SASBE-09-2024-0363>

¹⁰⁶ Καβαλλιέρου, Α. (2024). Διαχείριση ανθρώπινου δυναμικού στο δημόσιο τομέα κατά την περίοδο κρίσεων. <https://doi.org/10.26265/polynoe-7818>

¹⁰⁷ Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). *Privacy and Data Protection by Design—From policy to engineering* (arXiv:1501.03726). arXiv. <https://doi.org/10.48550/arXiv.1501.03726>

αλλαγές στη νομοθεσία περί απορρήτου. Η διαβούλευση με επαγγελματίες νομικούς και ενώσεις του κλάδου μπορεί να δώσει σημαντικές γνώσεις σχετικά με τις εξελισσόμενες νομικές τάσεις και τις βέλτιστες πρακτικές, διασφαλίζοντας ότι οι οργανισμοί διατηρούν προληπτική στάση στις πρωτοβουλίες τους για την προστασία της ιδιωτικής ζωής.

Η σημασία του δημόσιου λόγου για τον επηρεασμό των πρακτικών απορρήτου είναι υψίστης σημασίας. Καθώς η κοινωνική συνείδηση των ζητημάτων απορρήτου αυξάνεται, τα άτομα διατυπώνουν ολοένα και περισσότερο τις ανησυχίες και τις προσδοκίες τους σχετικά με την προστασία των δεδομένων. Οι οργανισμοί πρέπει να δώσουν προσοχή σε αυτά τα ζητήματα και να είναι έτοιμοι να τροποποιήσουν τις διαδικασίες τους ανάλογα. Η αλληλεπίδραση με ενδιαφερόμενα μέρη, όπως πελάτες, οργανώσεις υπεράσπισης και ρυθμιστικές υπηρεσίες, μπορεί να δώσει σημαντικές γνώσεις για τη διάθεση του κοινού και να βοηθήσει τους οργανισμούς να ευθυγραμμίσουν τη στρατηγική τους για την προστασία της ιδιωτικής ζωής με τις προσδοκίες της κοινωνίας.

Κεφάλαιο 6: Συμπεράσματα

Η διερεύνηση της προστασίας των προσωπικών δεδομένων στον δημόσιο τομέα αποκαλύπτει ένα πολύπλευρο περιβάλλον επηρεασμένο από ρυθμιστικές δομές, τεχνολογική πρόοδο και νέες ανησυχίες. Καθώς η ψηφιακή κοινωνία προχωρά, αυξάνεται επίσης η ανάγκη για ισχυρά συστήματα για την προστασία των δικαιωμάτων απορρήτου των ατόμων, ενώ παράλληλα διευκολύνεται η αποτελεσματική διακυβέρνηση και η παροχή υπηρεσιών. Η παρούσα διατριβή υπογραμμίζει την ουσιαστική σημασία της προστασίας δεδομένων, υποστηρίζοντας ότι δεν αποτελεί απλώς νομική ανάγκη αλλά και ζωτικό στοιχείο της δημόσιας εμπιστοσύνης και της κοινωνικής ευημερίας.

Στα προηγούμενα κεφάλαια μελετήσαμε τα νομικά και κανονιστικά πλαίσια που αφορούν την προστασία δεδομένων, δίνοντας έμφαση στον Γενικό Κανονισμό για την Προστασία Δεδομένων και τις επιπτώσεις του στον δημόσιο τομέα. Παρατηρήσαμε ότι παρόλο που ο GDPR θεσπίζει έναν αυστηρό κανόνα για την προστασία των δεδομένων, η επιτυχής εκτέλεσή του απαιτεί συνεχή αφοσίωση από τους δημόσιους φορείς. Η εξέταση των εθνικών κανόνων και των ειδικών κατευθυντήριων γραμμών ανά τομέα αποκάλυψε τις ποικίλες μεθόδους μεταξύ των δικαιοδοσιών, καταδεικνύοντας τις δυσκολίες που αντιμετωπίζουν οι δημόσιοι οργανισμοί στους ελιγμούς μέσω αυτού του πολύπλοκου δικτύου νομικών απαιτήσεων.

Οι θεσμικές και τεχνολογικές διαστάσεις της προστασίας δεδομένων έχουν γίνει κρίσιμα στοιχεία στην αναζήτηση κατάλληλων μέτρων προστασίας της ιδιωτικής ζωής. Εξετάσαμε τη σημασία της δημιουργίας ισχυρών οργανωτικών πλαισίων και του καθορισμού σαφών ρόλων και ευθυνών για την προστασία δεδομένων εντός των δημοσίων οργανισμών. Οι τεχνολογικές εξελίξεις, συμπεριλαμβανομένης της κρυπτογράφησης, των πρωτοκόλλων κυβερνοασφάλειας και των πλαισίων διακυβέρνησης δεδομένων, αποτελούν ουσιαστικά μέσα για τον μετριασμό των απειλών και την προστασία των προσωπικών δεδομένων. Οι οργανισμοί πρέπει να είναι προσεκτικοί στην ανταπόκριση στις νέες τεχνολογίες και στους αναδυόμενους κινδύνους που επαναπροσδιορίζουν διαρκώς το τοπίο προστασίας δεδομένων.

Τα προβλήματα και οι κίνδυνοι που αναγνωρίζονται στον δημόσιο τομέα, που περιλαμβάνουν εσωτερικές ευπάθειες, εξωτερικές απειλές στον κυβερνοχώρο και ζητήματα συμμόρφωσης, υπογραμμίζουν την ανάγκη για μια προορατική στρατηγική για την προστασία δεδομένων. Ο μετριασμός του ανθρώπινου λάθους και των εσωτερικών απειλών είναι απαραίτητος, καθώς μπορούν να θέτουν σημαντικούς κινδύνους για την ακεραιότητα των δεδομένων. Η αυξανόμενη συχνότητα και η πολυπλοκότητα των επιθέσεων στον κυβερνοχώρο υπογραμμίζει την επιτακτική ανάγκη για τους δημόσιους φορείς να ενισχύσουν τα πλαίσια κυβερνοασφάλειάς τους και να διατηρήσουν την ανθεκτικότητά τους έναντι των αναδυόμενων απειλών.

Οι προσεχείς συστάσεις για βέλτιστες πρακτικές και μελλοντικούς προσανατολισμούς υπογραμμίζουν την ανάγκη καλλιέργειας μιας κουλτούρας προστασίας δεδομένων που δίνει έμφαση στη διαφάνεια, την υπευθυνότητα και τη συνεργασία. Η προώθηση των συμπράξεων δημόσιου και ιδιωτικού τομέα μπορεί να ενισχύσει την καινοτομία και την κατανομή πόρων, επιτρέποντας στους δημόσιους φορείς να αξιοποιήσουν την εμπειρία και τις τεχνολογίες που

καλλιεργούνται στον ιδιωτικό τομέα.Επιπλέον, οι πρωτοβουλίες κατάρτισης και ευαισθητοποίησης είναι ζωτικής σημασίας για την παροχή στο προσωπικό των πληροφοριών και των δεξιοτήτων που απαιτούνται για τη διαχείριση των περιπλοκών της προστασίας δεδομένων σε ένα ψηφιακό περιβάλλον.

Βιβλιογραφία

- Abed, Y., & Chavan, M. (2019). The challenges of institutional distance: Data privacy issues in cloud computing. *Science, Technology and Society*, 24(1), 161–181.
<https://doi.org/10.1177/0971721818806088>
- Ahl, A., Goto, M., Yarime, M., Tanaka, K., & Sagawa, D. (2022). Challenges and opportunities of blockchain energy applications: Interrelatedness among technological, economic, social, environmental, and institutional dimensions. *Renewable and Sustainable Energy Reviews*, 166, 112623. <https://doi.org/10.1016/j.rser.2022.112623>
- Art. 32 GDPR – Security of processing. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved 13 May 2025, from <https://gdpr-info.eu/art-32-gdpr/>
- Art. 33 GDPR – Notification of a personal data breach to the supervisory authority. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved 13 May 2025, from <https://gdpr-info.eu/art-33-gdpr/>
- Art. 34 GDPR – Communication of a personal data breach to the data subject. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved 13 May 2025, from <https://gdpr-info.eu/art-34-gdpr/>
- Caruana, M. M. (2019). The reform of the EU data protection framework in the context of the police and criminal justice sector: Harmonisation, scope, oversight and enforcement. *International Review of Law, Computers & Technology*, 33(3), 249–270.
<https://doi.org/10.1080/13600869.2017.1370224>
- Chua, H. N., Herbrand, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, 34(4), 157–170. <https://doi.org/10.1016/j.tele.2017.01.008>
- Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, 34(2), 234–243. <https://doi.org/10.1016/j.clsr.2017.09.001>
- Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). *Privacy and Data Protection by Design—From policy to engineering* (arXiv:1501.03726). arXiv. <https://doi.org/10.48550/arXiv.1501.03726>
- de Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194. <https://doi.org/10.1016/j.clsr.2016.02.006>
- Dove, E. S. (2018). The eu general data protection regulation: Implications for international scientific research in the digital era. *Journal of Law, Medicine & Ethics*, 46(4), 1013–1030.
<https://doi.org/10.1177/1073110518822003>
- Dove, E. S. (2018). The eu general data protection regulation: Implications for international scientific research in the digital era. *Journal of Law, Medicine & Ethics*, 46(4), 1013–1030.
<https://doi.org/10.1177/1073110518822003>
- Ernest, E., Osakwe, J., & Nhamu, I. (2023). *A framework for data protection and privacy in data service centres in the public sector: A case study of a security organisation in a developing countries* (SSRN Scholarly Paper 4645049). <https://doi.org/10.2139/ssrn.4645049>

- Goddard, M. (2017). The eu general data protection regulation (Gdpr): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703–705.
<https://doi.org/10.2501/IJMR-2017-050>
- Gonçalves, M. E. (2017). The EU data protection reform and the challenges of big data: Remaining uncertainties and ways forward. *Information & Communications Technology Law*, 26(2), 90–115. <https://doi.org/10.1080/13600834.2017.1295838>
- Greco, S., Palmieri, R., & Rigotti, E. (2016). Institutional argumentation and conflict prevention: The case of the swiss federal data protection and information commissioner. *Journal of Pragmatics*, 105, 39–53. <https://doi.org/10.1016/j.pragma.2016.09.014>
- Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), 65–98. <https://doi.org/10.1080/13600834.2019.1573501>
- Jimmy, F. (2024). Enhancing data security in financial institutions with blockchain technology. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, 5(1), 424–437.
<https://doi.org/10.60087/jaigs.v5i1.217>
- Kiesow Cortez, E. (2021). Data protection around the world: An introduction. In E. Kiesow Cortez (Ed.), *Data Protection Around the World: Privacy Laws in Action* (pp. 1–6). T.M.C. Asser Press.
https://doi.org/10.1007/978-94-6265-407-5_1
- Kloza, D., Van Dijk, N., Gellert, R. M., Borocz, I. M., Tanas, A., Mantovani, E., & Quinn, P. (2017). Data protection impact assessments in the European Union: Complementing the new legal framework towards a more robust protection of individuals. *POLICY BRIEF D.PIA.LAB*, 1, 1–4.
<https://doi.org/10.31228/osf.io/b68em>
- Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4), 372–386.
<https://doi.org/10.1016/j.telpol.2012.04.011>
- Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25(4), 307–317. <https://doi.org/10.1016/j.clsr.2009.05.001>
- Lampri, M. (2012). E-government and data protection in the public sector. In A. A. Lazakidou (Ed.), *Virtual Communities, Social Networks and Collaboration* (pp. 135–145). Springer.
https://doi.org/10.1007/978-1-4614-3634-8_7
- Lnenicka, M., Kysela, T., & Horák, O. (2025). Building security and resilience: A guide to implementing effective cybersecurity and data protection measures in smart cities. *Smart and Sustainable Built Environment, ahead-of-print*(ahead-of-print). <https://doi.org/10.1108/SASBE-09-2024-0363>
- Mantelero, A. (2017). Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review*, 33(5), 584–602.
<https://doi.org/10.1016/j.clsr.2017.05.011>
- Minkkinen, M. (2015). Futures of privacy protection: A framework for creating scenarios of institutional change. *Futures*, 73, 48–60. <https://doi.org/10.1016/j.futures.2015.07.006>

- Mitrou, L. (2017). The general data protection regulation: A law for the digital age? In T.-E. Synodinou, P. Jougleux, C. Markou, & T. Prastitou (Eds.), *EU Internet Law: Regulation and Enforcement* (pp. 19–57). Springer International Publishing. https://doi.org/10.1007/978-3-319-64955-9_2
- Möller, C. (2017). *The evolution of data protection and privacy in the public security context—An institutional analysis of three eu data retention and access regimes* [Thesis, Queen Mary University of London]. <https://qmro.qmul.ac.uk/xmlui/handle/123456789/25911>
- Pagallo, U., & Bassi, E. (2013). Open data protection: Challenges, perspectives, and tools for the reuse of psi. In *Digital Enlightenment Yearbook 2013* (pp. 179–189). IOS Press. <https://doi.org/10.3233/978-1-61499-295-0-179>
- Panjwani, M., & Jäntti, M. (2017). Data protection & security challenges in digital & it services: A case study. *2017 International Conference on Computer and Applications (ICCA)*, 379–383. <https://doi.org/10.1109/COMAPP.2017.8079790>
- Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, 21(5), 510–524. <https://doi.org/10.1108/DPRG-05-2019-0039>
- Schaar, P. (2010). Privacy by design. *Identity in the Information Society*, 3(2), 267–274. <https://doi.org/10.1007/s12394-010-0055-x>
- Stepenko, V., Dreval, L., Chernov, S., & Shestak, V. (2022). Eu personal data protection standards and regulatory framework. *Journal of Applied Security Research*, 17(2), 190–207. <https://doi.org/10.1080/19361610.2020.1868928>
- Vollmer, N. (2023, April 4). *Άρθρο 37 ee γενικός κανονισμός για την προστασία δεδομένων* [Text]. <https://www.privacy-regulation.eu/el/37.htm>
- Wong, J., Henderson, T., & Ball, K. (2022). Data protection for the common good: Developing a framework for a data protection-focused data commons. *Data & Policy*, 4, e3. <https://doi.org/10.1017/dap.2021.40>
- Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, 16(1), 137–155. <https://doi.org/10.1111/rego.12401>
- Αναστασια Κολοφωτια, Σ. (2022). *Το διαδίκτυο των πραγμάτων στο δημόσιο τομέα: η μετάβαση στην έξυπνη διακυβέρνηση, εφαρμογές και νομικές προκλήσεις* [Working Paper]. <http://repositoryesdda.ekdd.gr/jspui/handle/123456789/560>
- Ανατολίτης, Θ. (2024). *Μέτρηση του βαθμού ευαισθητοποίησης των εργαζομένων στο δημόσιο τομέα της Ελλάδας σε θέματα ασφάλειας πληροφοριακών συστημάτων*. <https://doi.org/10.26265/polynoe-6713>
- Άρθρο 33—Γενικός κανονισμός για την προστασία δεδομένων—Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή. (2016, May 7). Lawspot. <https://www.lawspot.gr/node/67427>

- Άρθρο 5—Γενικός κανονισμός για την προστασία δεδομένων—Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. (2016, May 7). Lawspot. <https://www.lawspot.gr/node/67399>
- Άρθρο 6—Γενικός κανονισμός για την προστασία δεδομένων—Νομιμότητα της επεξεργασίας. (2016, May 7). Lawspot. <https://www.lawspot.gr/node/67400>
- Ζούνη, Α. (2024). *Η προστασία των δεδομένων υγείας στην εποχή της πανδημίας Covid-19. Η διαχείριση των δεδομένων υγείας από το δημόσιο νοσοκομείο*. <http://dspace.lib.uom.gr/handle/2159/30921>
- Ιγγλεζάκης, Ι. (Διπλωματική εργασία). (2020). *Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων (Κανονισμός 2016/679) και ο εφαρμοστικός νόμος (Ν. 4624/2019)*. Interactive Books.
- Ιωαννίδης, Ι. (2022). *Προστασία προσωπικών δεδομένων και διαδίκτυο των πραγμάτων*. <http://dspace.lib.uom.gr/handle/2159/27417>
- Καβαλλιέρου, Α. (2024). *Διαχείριση ανθρώπινου δυναμικού στο δημόσιο τομέα κατά την περίοδο κρίσεων*. <https://doi.org/10.26265/polynoe-7818>
- Κοντογεώργου, Η. (2024). *Η προστασία των προσωπικών δεδομένων εκτός ΕΕ: ΗΠΑ, Brussels effect και διασυννοριακή ροή* [Master Thesis, Πανεπιστήμιο Πειραιώς]. <https://dione.lib.unipi.gr/xmlui/handle/unipi/17427>
- Κουκουζέλη, Ο. Β. (2023). *Υπεύθυνος προστασίας δεδομένων (Υπδ)*. <http://dspace.lib.uom.gr/handle/2159/29706>
- Λαζαρίδου, Κ. Ν. (Διπλωματική εργασία). (2024). *Ο γενικός κανονισμός προστασίας δεδομένων και η εφαρμογή του στους εργαζόμενους στον δημόσιο τομέα*.
- Λεπίδα, Π. (2022). *Εκτίμηση αντικτύπου ως προς την προστασία δεδομένων—Μελέτη περίπτωσης στο δημόσιο τομέα*. <https://kypseli.ouc.ac.cy/handle/11128/5098>
- Λούντου, Μ. (2021). *Η προστασία των προσωπικών δεδομένων των εργαζομένων στον δημόσιο και ιδιωτικό τομέα υπό το πρίσμα των πρόσφατων νομοθετικών εξελίξεων (Σύγκριση—Αντιπαραβολή και προοπτικές εξέλιξης)*. <https://doi.org/10.26265/polynoe-597>
- Νομοθεσία προσωπικών δεδομένων. (n.d.). dpa.gr. Retrieved 4 February 2025, from http://www.dpa.gr/el/enimerwtiko/nomothesia/proswpika/nomothesia_prwsopikwn
- Νόμος 4624/2019 (Κωδικοποιημένος)—ΦΕΚ Α 137/29.08.2019. (n.d.). Retrieved 12 May 2025, from <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>
- Νόμος 4624/2019. (2019, August 31). Lawspot. <https://www.lawspot.gr/node/265098>
- Νοτοπούλου, Φ. (2022). *Σύγχρονα ζητήματα γύρω από την προστασία δεδομένων προσωπικού χαρακτήρα* [Master Thesis, Πανεπιστήμιο Πειραιώς]. https://doi.org/10.26267/unipi_dione/2472
- Παπαδόπουλος, Α. (2020). *The implementation of the General Data Protection Regulation in the EU and Greece: Procedures, risks, challenges and impacts in the context of good governance*. <http://dspace.lib.uom.gr/handle/2159/24326>
- Περατινός, Α. (2023). *Προστασία δεδομένων από μεταβολές στο διαδίκτυο των πραγμάτων με χρήση της τεχνολογίας καταναμημένου κατάστιχου (Dlt)*. <https://doi.org/10.26265/polynoe-4701>
- Ράμια, Κ. Σ. (2022). *Η τεχνολογία blockchain και η συμβατότητάς της με τον γενικό κανονισμό προστασίας δεδομένων*. <http://dspace.lib.uom.gr/handle/2159/26464>

- Ρίζου, Α. Σ. (Διπλωματική εργασία). (2023). *Η συμβολή του γενικού κανονισμού προστασίας δεδομένων στην καταπολέμηση του εργασιακού εκφοβισμού και την προστασία των whistleblowers στον δημόσιο τομέα.*
- Φράγκου, Α. (2018). *Οι προοπτικές της διοικητικής μεταρρύθμισης στην Ελλάδα: ο ρόλος της συγκριτικής αξιολόγησης (Benchmarking) με βάση την εργαλειοθήκη του ΟΟΣΑ και τις βέλτιστες πρακτικές της Ε. Ε.* <http://dspace.lib.uom.gr/handle/2159/23062>
- Χατζηλιάδου, Σ. (2022). *Διαχείριση δημοσίων κατασκευαστικών έργων στην ήπειρο: Κίνδυνοι και προκλήσεις.* <https://kypseli.ouc.ac.cy/handle/11128/5316>