ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Ηλεκτρονική Διακυβέρνηση

Αυτοματοποίηση διαδικασίας παραγωγής πολιτικών ιδιωτικότητας με χρήση Τεχνητής Νοημοσύνης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Απόστολου Σιάτρα

Επιβλέπουσα: Δρ. Διαμαντοπούλου Βασιλική (Μόνιμη Επίκουρος Καθηγήτρια)

Μέλη εξεταστικής επιτροπής:
Καθηγήτρια Δρ. Λίλιαν Μήτρου
Καθηγητής Δρ. Σπύρος Κοκολάκης

Μυτιλήνη, Φεβρουάριος 2026

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η ολοκλήρωση της παρούσας διπλωματικής διατριβής, η οποία εστιάζει στον κρίσιμο τομέα της αυτοματοποίησης της κανονιστικής συμμόρφωσης (RegTech) με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), αποτελεί το επιστέγασμα μιας εντατικής ερευνητικής και υλοποιητικής προσπάθειας.

Πρωτίστως, οφείλω τις βαθύτατες και ειλικρινείς ευχαριστίες μου στους γονείς μου, Αργύριο και Κωνσταντινία. Η ακλόνητη υποστήριξή τους, η διαρκής και ανιδιοτελής αγάπη τους, και η σταθερή τους πίστη στις επιλογές μου αποτέλεσαν το θεμέλιο για την επιτυχή ολοκλήρωση των σπουδών μου. Η δύναμη και οι σκέψεις τους ήταν πάντοτε μαζί μου, ακόμη και όταν οι ίδιοι αντιμετώπιζαν τις δικές τους προσωπικές προκλήσεις.

Ένα ξεχωριστό κεφάλαιο ευγνωμοσύνης ανήκει στις γιαγιάδες μου, Δήμητρα και Θεοδώρα. Τις ευχαριστώ θερμά για όλα κυρίως εξασφαλίζοντας ένα περιβάλλον σταθερότητας και φροντίδας κατά τη διάρκεια όλων των περασμένων καλοκαιριών...

Στο ακαδημαϊκό πεδίο, η ευγνωμοσύνη μου απευθύνεται σε όλα τα μέλη του Διδακτικού Προσωπικού του Μεταπτυχιακού Προγράμματος Σπουδών «Ηλεκτρονικής Διακυβέρνησης» του Πανεπιστημίου Αιγαίου και ιδιαίτερα την Δρ Βασιλική Διαμαντοπούλου η οποία έχει αναλάβει την επιμέλεια και την σωστή διεκπεραίωση/περάτωση αυτής της διπλωματικής εργασίας .

Ιδιαίτερες ευχαριστίες οφείλω στον Καθηγητή, Δρ. Χρήστο Καλλονιάτη. Η καθοδήγησή του υπήρξε κρίσιμη για την ορθή μεθοδολογία της έρευνας, ενώ η επιστημονική του οξυδέρκεια και η αδιάκοπη ενθάρρυνση καθόρισαν την ποιότητα του τελικού έργου. Τον ευχαριστώ για την ενσωμάτωσή μου στο Εργαστήριο PrivaSI του Πανεπιστημίου Αιγαίου, γεγονός που μου επέτρεψε την ενεργή συμμετοχή σε σημαντικά ερευνητικά projects, διευρύνοντας ουσιαστικά τους ορίζοντες της πρακτικής μου εμπειρίας όπως επίσης ευχαριστώ και την Δρ Αικατερίνη Μαυροειδή για την συνεχή υποστήριξή της στο περιβάλλον του εργαστηρίου. Επιπλέον, η παραχώρηση του αρχείου DPIA από την Αρχή Προστασίας Δεδομένων της Ελλάδος υπήρξε ένα κρίσιμο εργαλείο για την τεκμηρίωση και την ανάπτυξη του πυρήνα της μεθοδολογίας της παρούσας εργασίας.

© [2026]
του
Απόστολου Σιάτρα
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1 Εισαγωγή....1

1.1 Το πλαίσιο της Διπλωματικής εργασίας....1

1.2 Σκοπός της Διπλωματικής εργασίας....2

1.3 Αντικείμενο της Διπλωματικής Εργασίας....4

1.4 Δομή της διπλωματικής εργασίας....5

2 Ανάλυση Τρέχοντος Επιπέδου....7

2.1 Βασικές έννοιες και ορισμοί....7

2.1.1 Δεδομένα Προσωπικού Χαρακτήρα....7

2.1.2 Επεξεργασία (Processing)....8

2.1.3 Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA)....8

2.1.4 Ανάλυση Κενών (Gap Analysis)....9

2.1.5 Προστασία των Δεδομένων ήδη από τον Σχεδιασμό (Privacy by Design)....10

2.1.6 Λογοδοσία....10

2.2 Τρέχουσα Κατάσταση στην Ελλάδα....11

2.3 Τρέχουσα Κατάσταση στο Εξωτερικό....13

2.4 Ανασκόπηση Πεδίου....16

2.4.1 Από την Πρόβλεψη στην Παραγωγή (Predicive vs Generative AI)....16

2.4.2 Τεχνητή Νοημοσύνη στην Παραγωγή πολιτικών απορρήτου....17

2.4.3 Προκλήσεις και περιορισμοί των LLMs στη παραγωγή Νομικού κειμένου....18

2.4.4 Το Ερευνητικό Ερώτημα....19

2.5 Η χαρτογράφηση του Οργανισμού και η παραγωγή κειμένου μέσα από το Μεγάλο Γλωσσικό Μοντέλο....19

2.6 Παραγωγική Συμμόρφωση και το Ερευνητικό Ερώτημα....20

2.7 Παραγωγική Συμμόρφωση και το Ερευνητικό Ερώτημα....21

2.8 Συμπεράσματα....22

3 Μεθοδολογία....25

3.1 Στρατηγική Σχεδιασμού: Schema-Driven Development....26

3.2 Διαδικασία Υλοποίησης Υποσυστημάτων....27

3.2.1 Μηχανισμός Αξιολόγησης (Assessment Engine)....27

3.2.2 Τεχνικός Έλεγχος (Audit Module)....28

3.2.3 Μηχανή Παραγωγής Πολιτικών (Policy Engine)....28

3.3 Επαλήθευση και Έλεγχος Λογισμικού....29

3.4 Σύνδεση Μεθοδολογίας και Ερευνητικών Ερωτημάτων....30

4 Αρχιτεκτονική Συστήματος....32

4.1 Απαιτήσεις Συστήματος....32

4.1.1 Λειτουργικές Απαιτήσεις (Functional Requirements)....32

4.1.2 Σύντομη Ανάλυση και Παρατηρήσεις....33

4.1.3 Ανάλυση Μη Λειτουργικών Απαιτήσεων....35

4.2 Διαγράμματα....35

4.2.1 Διάγραμμα Περιπτώσεων Χρήσης (Use Case Diagram)....37

4.2.2 Διάγραμμα Δραστηριότητας: Παραγωγή Πολιτικής Απορρήτου με AI (Activity Diagram)....38

4.3 Διάγραμμα Κλάσεων (Class Diagram)....39

4.4 Διάγραμμα Ακολουθίας Ελέγχου Cookies (Sequence Diagram)....40

4.5 Διάγραμμα Συστατικών Στοιχείων (Component Diagram)....41

4.6 Σύνοψη Κεφαλαίου....41

5 Εργαλεία Ανάπτυξης Συστήματος....43

5.1 Οικοσύστημα Τεχνητής Νοημοσύνης....43

5.1.1 Αυστηρός Ορισμός Δομών Δεδομένων....44

5.1.2 Διαχείρηση Συστήματος Αρχείων....45

5.1.3 Πλαίσιο Ανάπτυξης Εφαρμογής : Flask cs Django....45

5.1.4 Μηχανισμός Αξιολόγησης (Assessment Engine)....46

5.2 Μηχανική Τεχνητής Νοημοσύνης: Ollama & Llama 3....47

5.2.1 Δυναμική Κατασκευή Διεπαφής (Context Processors)....47

5.3 Τεχνολογίες Διεπαφής (Frontend) και Templating....48

5.3.1 Δυναμική Σύνθεση Σελίδων (Jinja Templating)....49

5.3.2 Οπτικοποίηση Δεδομένων (Chart.js)(Ανάλυση όλων των Διαγραμμάτων)....49

5.3.3 Σχεδιαστική Συνέπεια και Προσαρμοστικότητα (CSS & Bootstrap)....49

5.4 Αποθήκευση Δεδομένων: JSON (NoSQL Approach)....50

5.4.1 Ιεραρχική Δομή και Ευελιξία Σχήματος....51

5.4.2 Σειριοποίηση και Επιδόσης (Serialization)....52

5.5 Περιβάλλον Ανάπτυξης και Διαχείριση Κώδικα....52

5.6 Σύνοψη Κεφαλαίου....52

6 Το Σύστημα....54

6.1 Επισκόπηση Ροής....55

6.1.1 Αρχιτεκτονική Πληροφορίας (Sitemap)....55

6.1.2 Μηχανισμός Αυθεντικοποίησης....56

6.1.3 Σχεδιασμός Διεπαφής....57

6.2 Κεντρικός Πίνακας Ελέγγου (Dashboard) 57
6.2.1 Δυναμικές Κάρτες Εργασιών (Task Cards) *57*
6.3 Υποσύστημα Αξιολογήσεων (DPIA & Gap Analysis) 58
6.3.1 Δυναμική Δομή και Λογική *58*
6.3.2 Μηχανισμός Επικύρωσης και Αποθήκευσης (Validation & State) *60*
6.4 Μηχανισμός Ελέγχου Ιστοσελίδας (Cookie Audit) 60
6.4.1 Μηχανισμός Αξιολόγησης (Assessment Engine) *61*
6.5 Αναλυτικά Στοιχεία και Οπτικοποίηση (Analytics) 62
6.5.1 Μηχανισμός Συσχέτισης Δεδομένων (Data Aggregation) *62*
6.6 Δομή του Πληροφοριακού συστήματος 66
6.7 Συζήτηση επί της Υλοποίησης 67
6.7.1 Αξιολόγηση της Αρχιτεκτονικής «Βάσει Σχήματος» (Schema-Driven Architecture) *67*
6.7.2 Ενσωμάτωση Τοπικής Τεχνητής Νοημοσύνης και Από *68*
6.7.3 Διαχείριση Κατάστασης Χωρίς Βάση Δεδομένων (Stateless design) *68*
6.7.4 Αυτοματοποίηση Τεχνικών Ελέγχων (Web Scraping) *68*
7 Συζήτηση 70
7.1 Αξιολόγηση της Αρχιτεκτονικής Local AI 70
7.2 Κίνδυνος της παραγωγής ψευδών πληροφοριών (Hallucinations) Στη Νομική Τεχνολογία 72
7.3 Αναγκαιότητα του “Human-in-the-loop” 73
7.4 Σύγκριση με Υπάρχουσες Λύσεις 74
7.5 Περιορισμοί της έρευνας 75
8 Συμπεράσματα της Μελέτης 77
8.1 Τα ερευνητικά ερωτήματα και απαντήσεις 77
8.1.1 Ερευνητικό ερώτημα 1 ..... *77*
8.1.2 Ερευνητικό ερώτημα 2 ..... *78*
8.1.3 Ερευνητικό ερώτημα 3 ..... *78*
8.1.4 Ερευνητικό ερώτημα 4 ..... *79*
8.1.5 Συνολική Σύνδεση με το Αρχικό Ερευνητικό Κενό *79*
8.2 Συμπεράσματα επί των αποτελεσμάτων 80
8.3 Συμπεράσματα επί της μεθοδολογίας 81
8.4 Συμπεράσματα επί των εργαλείων 83
8.5 Προοπτικές / Επόμενα βήματα 83
Βιβλιογραφία 86
Παράρτημα Ι Οδηγός Εγκατάστασης για το GDPR-Assesor (Mac/Linux/W10/W11) 91

Λίστα Σχημάτων

Εικόνα 1: Αρχιτεκτονική Συστήματος και Ροή Δεδομένων 36
Εικόνα 2 : Διάγραμμα Περιπτώσεων Χρήσης 37
Εικόνα 3: Απεικόνιση Δραστηριότητας Διαδικασίας Παραγωγής Πολιτικής [1/3] 38
Εικόνα 4: Απεικόνηση Δραστηριότητας διαδικασίας παραγωγής Πολιτικής [2/3] 38
Εικόνα 5: Απεικόνιση Δραστηριότητας διαδικασίας παραγωγής Πολιτικής [3/3] 38
Εικόνα 6: Δραστηριότητας διαδικασίας παραγωγής [ολοκληρωμένο] 38
Εικόνα 7: Δομή Assesment Engine [1/2] 39
Εικόνα 8: Δομή Assesment Engine [2/2] 39
Εικόνα 9: Δομή Assesment Engine [ολοκληρωμένο] 39
Εικόνα 10: Δομή Cookie Audit 40
Εικόνα 11: Διάγραμμα Συστατικών Στοιχείων 41
Εικόνα 12: Διάγραμμα Επικοινωνίας Ollama-Llama με το σύστημα 44
Εικόνα 13: Διαγραμμα προτύπων των ερωτήσεων 44
Εικόνα 14: Διαχείριση αρχείων Συστήματος 45
Εικόνα 15: Συγκριτική Ανάλυση Αρχιτεκτονικής (Παράδειγμα Flask) 46
Εικόνα 16: Συγκριτική Ανάλυση Αρχιτεκτονικής (Παράδειγμα Django) 46
Εικόνα 17: Λογική Context proccesors 48
Εικόνα 18: Διαδρομή σύνθεσης σελίδας 49
Εικόνα 19: Διαδρομή δεδομένων πριν τη σύνθεση της σελίδας 49
Εικόνα 20: Διάγραμμα Προσαρμοστικότητας σύνθεσης της σελίδας 50
Εικόνα 21: Σύγκριση Μοντέλων Δεδομένων json/sql 51
Εικόνα 22: Ροή Εγγραφής Δεδομένων 52
Εικόνα 23: Ροή διεργασιών στο Επιχειρησιακό Περιβάλλον 54
Εικόνα 24: Ροή Ενεργειών Χρήστη (User Action Flow) 55
Εικόνα 25: Διάγραμμα διαμοιρασμού πληροφοριών προς τον χρήστη 56
Εικόνα 26: Οθόνη Αυθεντικοποίησης 56
Εικόνα 27: Δομή Σελίδας Εισόδου 57
Εικόνα 28: Dashboard Πληροφοριακού Συστήματος 58
Εικόνα 29: Οθόνη χρήσης για αξιολόγηση βάση DPIA 59
Εικόνα 30:Ροή Δημιουργίας Ερωτηματολογίου 59
Εικόνα 31: Διαδικασία Υποβολής και Ελέγχου 60
Εικόνα 32: Cookie Audit landing Page 61
Εικόνα 33: Ροή Εκτέλεσης Σάρωσης (cookie audit) 62
Εικόνα 34: Ροή Ενοποίησης Δεδομένων 63
Εικόνα 35: Radar/Risk Matrix 64

Εικόνα 36: Radar / Coverage per Article 64
Εικόνα 37: Correlation Matrix 65
Εικόνα 38: Gap List 66
Εικόνα 39: Οθόνη Παραγωγής Πολιτικής 67

Λίστα Πινάκων

Πίνακας1: Συγκριτικός Πίνακας μεταξύ πλατφορμών Διακυβέρνησης Δεδομένων.....23
Πίνακας 2: Λειτουργικές απαιτήσεις 32
Πίνακας 3: Μη Λειτουργικές απαιτήσεις.....34

Ακρωνύμια

AI	Τεχνητή Νοημοσύνη (Artificial Intelligence)
AI Act	Κανονισμός της ΕΕ για την Τεχνητή Νοημοσύνη (EU Artificial Intelligence Act)
API	Διεπαφή Προγραμματισμού Εφαρμογών (Application Programming Interface)
AWS	Υπηρεσίες Ιστού της Amazon (Amazon Web Services)
CMP	Πλατφόρμα Διαχείρισης Συγκατάθεσης (Consent Management Platform)
DPIA	Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (Data Protection Impact Assessment)
DPO	Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer)
DSAR	Αίτημα Άσκησης Δικαιωμάτων Υποκειμένου (Data Subject Access Request)
DSARs	Αιτήματα Άσκησης Δικαιωμάτων Υποκειμένου (Data Subject Access Requests)
ERP	Σύστημα Επιχειρησιακού Σχεδιασμού Πόρων (Enterprise Resource Planning)
EU	Ευρωπαϊκή Ένωση (European Union)
GAP	Ανάλυση Κενού
GDPR	Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation)
GPT	Γενετικά Προεκπαιδευμένος Μετασχηματιστής (Generative Pre-trained Transformer)
GPT-4	Γενετικά Προεκπαιδευμένος Μετασχηματιστής (Generative Pre-trained Transformer, version 4)
GRC	Διακυβέρνηση, Κίνδυνος και Συμμόρφωση (Governance, Risk & Compliance)
HITL	Άνθρωπος-στον-Βρόχο (Human-in-the-Loop)
HR	Ανθρώπινο Δυναμικό (Human Resources)
HTML	Γλώσσα Σήμανσης Υπερκειμένου (HyperText Markup Language)
HTTP	Πρωτόκολλο Μεταφοράς Υπερκειμένου (Hypertext Transfer Protocol)
IEC	Διεθνής Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission)
ISO	Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization)
ISO/IEC 27001	Πρότυπο Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISO/IEC 27001 ISMS standard)
JSON	Μορφότυπος JSON για δομημένα δεδομένα (JavaScript Object Notation)
LLM	Μεγάλο Γλωσσικό Μοντέλο (Large Language Model)
LLMs	Μεγάλα Γλωσσικά Μοντέλα (Large Language Models)
NLP	Επεξεργασία Φυσικής Γλώσσας (Natural Language Processing)

PDF	Μορφότυπος Φορητού Εγγράφου (Portable Document Format)
RAG	Παραγωγή με Ενίσχυση Ανάκτησης (Retrieval-Augmented Generation)
RegTech	Κανονιστική Τεχνολογία (Regulatory Technology)
ROPA	Αρχείο Δραστηριοτήτων Επεξεργασίας (Record of Processing Activities)
SaaS	Λογισμικό ως Υπηρεσία (Software as a Service)
SOC 2	Πλαίσιο Ελέγχου Ασφάλειας τύπου audit (SOC 2)
SVM	Μηχανή Διανυσμάτων Υποστήριξης (Support Vector Machine)
SVMs	Μηχανές Διανυσμάτων Υποστήριξης (Support Vector Machines)
TOM	Τεχνικά και Οργανωτικά Μέτρα (Technical and Organisational Measures)
TOMs	Τεχνικά και Οργανωτικά Μέτρα (Technical and Organisational Measures)
URL	Ενιαίος Εντοπιστής Πόρου (Uniform Resource Locator)
ΕΕ	Ευρωπαϊκή Ένωση (European Union)
ΜΜΕ	Μικρομεσαίες Επιχειρήσεις (SMEs: Small and Medium-sized Enterprises)
ΜμΕ	Μικρομεσαίες Επιχειρήσεις (SMEs: Small and Medium-sized Enterprises)
ΤΝ	Τεχνητή Νοημοσύνη (Artificial Intelligence)

Περίληψη

Η παρούσα διπλωματική εργασία πραγματεύεται τον σχεδιασμό και την ανάπτυξη ενός ολοκληρωμένου πληροφοριακού συστήματος υποβοήθησης της παραγωγής πολιτικών ιδιωτικότητας, αξιοποιώντας σύγχρονες τεχνολογίες Τεχνητής Νοημοσύνης (AI). Σκοπός της έρευνας είναι η αυτοματοποίηση χρονοβόρων διαδικασιών, όπως η Εκτίμηση Αντικτύπου (DPIA) και η συγγραφή νομικών κειμένων πολιτικής απορρήτου, μέσω της χρήσης Μεγάλων Γλωσσικών Μοντέλων (LLMs).

Η μεθοδολογία που ακολουθήθηκε βασίστηκε στις αρχές της Έρευνας Σχεδιασμού (Design Science Research) για την ανάπτυξη λογισμικού. Αναπτύχθηκε μια διαδικτυακή εφαρμογή (web application) σε περιβάλλον Python/Flask, η οποία ενσωματώνει εργαλεία για τη διενέργεια ελέγχων Gap Analysis και DPIA, καθώς και μηχανισμό αυτόματης σάρωσης ιστοσελίδων (Cookie Audit). Η καινοτομία της προσέγγισης έγκειται στη διασύνδεση των δομημένων δεδομένων των ερωτηματολογίων με τοπικά γλωσσικά μοντέλα (Llama 3 μέσω Ollama), επιτρέποντας την παραγωγή φυσικής γλώσσας για τη σύνταξη τελικών αναφορών και πολιτικών απορρήτου, προσαρμοσμένων στο προφίλ του εκάστοτε οργανισμού.

Τα αποτελέσματα της υλοποίησης καταδεικνύουν ότι η χρήση εξειδικευμένων prompts σε συνδυασμό με δομημένα δεδομένα εισόδου μπορεί να παράγει κείμενα υψηλής ακρίβειας και συνοχής, μειώνοντας δραστικά τον χρόνο που απαιτείται από τους υπευθύνους προστασίας δεδομένων (DPOs). Συμπερασματικά, η εργασία αναδεικνύει ότι τα εργαλεία AI, όταν λειτουργούν υπό ανθρώπινη επίβλεψη, μπορούν να αποτελέσουν κρίσιμο αρωγό στη κανονιστική συμμόρφωση, προσφέροντας λύσεις που είναι ταυτόχρονα τεχνικά άρτιες και νομικά συνεκτικές.

Λέξεις Κλειδιά: GDPR, Τεχνητή Νοημοσύνη, Large Language Models, Gap analysis, DPIA, Αυτοματοποίηση Συμμόρφωσης, Privacy Engineering, πολιτική ιδιωτικότητας

Abstract

This thesis addresses the design and development of an integrated information system to assist in the production of Privacy Policies Regulation by leveraging modern Artificial Intelligence (AI) technologies. The aim of the research is to automate time-consuming procedures, such as Data Protection Impact Assessments (DPIA) and the drafting of privacy policy texts, through the use of Large Language Models (LLMs).

The methodology adopted followed the principles of Design Science Research for software development. A web application was developed using the Python/Flask framework, incorporating tools for conducting Gap Analysis and DPIA, as well as an automated website scanning mechanism (Cookie Audit). The innovation of this approach lies in integrating structured questionnaire data with local language models (Llama 3 via Ollama), enabling the generation of natural language for the synthesis of final reports and privacy policies tailored to the profile of each organization.

The implementation results demonstrate that using specialized prompts combined with structured input data can produce high-accuracy and coherent texts, drastically reducing the time required by Data Protection Officers (DPOs). In conclusion, the thesis highlights that AI tools, when operating under human oversight, can be a critical aid in regulatory compliance, offering solutions that are both technically sound and legally consistent.

Keywords: GDPR, Artificial Intelligence, Large Language Models, DPIA, Gap analysis, Compliance Automation, Privacy Engineering, Privacy Policy.

1 *Εισαγωγή*

1.1 Το πλαίσιο της Διπλωματικής εργασίας

Η σύγχρονη ψηφιακή εποχή χαρακτηρίζεται από τον ολοένα αυξανόμενο ρυθμό παραγωγής και επεξεργασίας δεδομένων, φαινόμενο που συχνά περιγράφεται ως "Big Data revolution". Η ραγδαία ψηφιοποίηση των υπηρεσιών, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, σε συνδυασμό με την εκθετική αύξηση του όγκου των δεδομένων που συλλέγουν οι οργανισμοί, έχουν αναγάγει την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων σε μία από τις σημαντικότερες κοινωνικές, νομικές και τεχνολογικές προκλήσεις του 21ου αιώνα. Σε αυτό το πλαίσιο, η ασφάλεια των πληροφοριών παύει να αποτελεί ένα αμιγώς τεχνικό ζήτημα και μετατρέπεται σε θεμελιώδη πυλώνα της εταιρικής διακυβέρνησης και της εμπιστοσύνης των καταναλωτών.

Η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR – General Data Protection Regulation) [1] από την Ευρωπαϊκή Ένωση τον Μάιο του 2018, αποτέλεσε ορόσημο για την παγκόσμια νομοθεσία περί απορρήτου. Ο Κανονισμός έθεσε ένα αυστηρό και ομοιόμορφο κανονιστικό πλαίσιο για όλα τα κράτη-μέλη, με στόχο την ενίσχυση των δικαιωμάτων των πολιτών και την ελεύθερη κυκλοφορία των δεδομένων εντός της Ενιαίας Ψηφιακής Αγοράς. Παρόλο που η αναγκαιότητα του Κανονισμού για την προάσπιση των θεμελιωδών ελευθεριών είναι αδιαμφισβήτητη, η πρακτική εφαρμογή του δημιούργησε έναν δυσανάλογο διοικητικό, τεχνικό και οικονομικό φόρτο για τις επιχειρήσεις.

Η διαδικασία συμμόρφωσης αποδεικνύεται μια πολυδιάστατη άσκηση που απαιτεί τη συνέργεια εξειδικευμένης νομικής γνώσης, τεχνικής εμπειρογνωμοσύνης στην ασφάλεια πληροφοριών και συνεχούς οργανωτικής επαγρύπνησης. Αυτή η πολυπλοκότητα καθιστά τη συμμόρφωση ιδιαίτερα δαπανηρή και δυσχερή, ειδικά για τις μικρομεσαίες επιχειρήσεις (ΜμΕ), οι οποίες συχνά στερούνται των πόρων για την πρόσληψη εξειδικευμένων συμβούλων ή Υπευθύνων Προστασίας Δεδομένων (DPOs). Το πρόβλημα επιτείνεται από τον κίνδυνο επιβολής εξοντωτικών διοικητικών κυρώσεων, καθώς τα πρόστιμα συμμόρφωσης συνεχίζουν να αυξάνονται, με τις ρυθμιστικές αρχές να επιβάλλουν ποινές που αγγίζουν αθροιστικά δισεκατομμύρια ευρώ ετησίως σε πανευρωπαϊκό επίπεδο [2].

Παράλληλα με τις νομικές εξελίξεις, ο τεχνολογικός τομέας βιώνει μια επανάσταση μέσω της εμφάνισης και της αλματώδους εξέλιξης των Μεγάλων Γλωσσικών Μοντέλων (Large Language

Models – LLMs) [3] και της Παραγωγικής Τεχνητής Νοημοσύνης (Generative AI). Τα συστήματα αυτά, εκπαιδευμένα σε τεράστιους όγκους κειμένου, επιδεικνύουν πρωτοφανείς ικανότητες στην κατανόηση, σύνθεση και παραγωγή φυσικής γλώσσας, ανοίγοντας νέους ορίζοντες στην αυτοματοποίηση πνευματικών εργασιών. Ενώ η χρήση της Τεχνητής Νοημοσύνης (AI) έχει εδραιωθεί σε τομείς όπως η ανάλυση δεδομένων, η εξυπηρέτηση πελατών και η ιατρική διάγνωση, η εφαρμογή της στον ευαίσθητο τομέα της Κανονιστικής Τεχνολογίας (RegTech) παραμένει ένα πεδίο που χρήζει περαιτέρω διερεύνησης [4].

Ειδικότερα, η δυνατότητα των LLMs να αναλύουν κείμενα και να συντάσσουν πολιτικές ασφαλείας και ιδιοτικότητας προσφέρει μια μοναδική ευκαιρία για την απλούστευση της συμμόρφωσης. Ωστόσο, η χρήση τέτοιων εργαλείων συνοδεύεται από νέους κινδύνους, όπως η πιθανότητα διαρροής εμπιστευτικών δεδομένων σε δημόσια μοντέλα AI (π.χ. ChatGPT) ή η παραγωγή ανακριβών νομικών συμβουλών (hallucinations) [5]. Η παρούσα διπλωματική εργασία εντάσσεται σε αυτό ακριβώς το ερευνητικό κενό, εξετάζοντας πώς η τεχνολογία των τοπικών LLMs (Local LLMs) μπορεί να γεφυρώσει το χάσμα μεταξύ των αυστηρών νομικών απαιτήσεων και της τεχνικής υλοποίησης, προσφέροντας λύσεις που είναι ασφαλείς, οικονομικές και νομικά έγκυρες.

Σε αυτό το περιβάλλον, το πρόβλημα που επιχειρεί να αντιμετωπίσει η παρούσα διπλωματική εργασία μπορεί να διατυπωθεί ως εξής: πώς μπορεί ένας οργανισμός, και ειδικότερα μία μικρομεσαία επιχείρηση με περιορισμένο εξειδικευμένο νομικό ή τεχνικό προσωπικό, να διενεργεί ουσιαστικές Εκτιμήσεις Αντικτύπου, να επιτηρεί την τεχνική του συμμόρφωση (π.χ. μέσω ελέγχου cookies) και να συντάσσει συνεκτικά κείμενα πολιτικών απορρήτων και ιδιωτικότητας χωρίς να εξαρτάται αποκλειστικά από ακριβές συμβουλευτικές υπηρεσίες ή κλειστές, ιδιόκτητες πλατφόρμες RegTech. Το ερευνητικό αυτό ερώτημα γίνεται ακόμη πιο κρίσιμο αν ληφθεί υπόψη η εμφάνιση των Μεγάλων Γλωσσικών Μοντέλων (LLMs), τα οποία υπόσχονται αυτοματοποίηση της γραπτής παραγωγής, αλλά συνοδεύονται από σημαντικούς κινδύνους παραγωγής ψευδών πληροφοριών και παραβίασης της ιδιωτικότητας. Η παρούσα εργασία τοποθετείται ακριβώς σε αυτό το σημείο τομής μεταξύ νομικής συμμόρφωσης, μηχανικής λογισμικού και τεχνητής νοημοσύνης.[5]

1.2 Σκοπός της Διπλωματικής εργασίας

Ο πρωταρχικός σκοπός της παρούσας διπλωματικής εργασίας είναι ο σχεδιασμός, η ανάπτυξη και η αξιολόγηση ενός πρότυπου πληροφοριακού συστήματος (software artifact), το οποίο φιλοδοξεί να λειτουργήσει ως ένας ολοκληρωμένος "Ψηφιακός Σύμβουλος Συμμόρφωσης"). Η έρευνα στοχεύει να απαντήσει στην επιτακτική ανάγκη για εργαλεία που γεφυρώνουν το χάσμα μεταξύ της αφηρημένης νομικής θεωρίας του GDPR και της πρακτικής, καθημερινής εφαρμογής των κανόνων προστασίας δεδομένων στις επιχειρήσεις.[5]

Συγκεκριμένα, οι επιμέρους στόχοι της εργασίας αναλύονται ως εξής:

1) **Αυτοματοποίηση της Εκτίμησης Αντικτύπου (DPIA)**: Ένας κεντρικός στόχος είναι η απλούστευση της πολύπλοκης διαδικασίας Εκτίμησης Αντικτύπου Σχετικά με την Προστασία Δεδομένων (Data Protection Impact Assessment), όπως αυτή ορίζεται στο Άρθρο 35 του Κανονισμού. Στόχος είναι η δημιουργία ενός διαδραστικού μηχανισμού που θα καθοδηγεί τον χρήστη – ακόμη και αν δεν διαθέτει εξειδικευμένες νομικές

γνώσεις – στον εντοπισμό, την αξιολόγηση και την αντιμετώπιση των κινδύνων που απορρέουν από την επεξεργασία δεδομένων. Το σύστημα φιλοδοξεί να μετατρέψει τη στατική, γραφειοκρατική διαδικασία συμπλήρωσης εγγράφων σε μια δυναμική ροή εργασίας (dynamic workflow) που προσαρμόζεται στο προφίλ του οργανισμού.[5]

2) **Εκδημοκρατισμός της Κανονιστικής Τεχνολογίας (RegTech):** Η αγορά των εργαλείων συμμόρφωσης κυριαρχείται σήμερα από λύσεις υψηλού κόστους (Enterprise Solutions) που απευθύνονται κυρίως σε πολυεθνικούς ομίλους [6]. Σκοπός της παρούσας εργασίας είναι η ανάπτυξη μιας λύσης ανοιχτού κώδικα (open-source), η οποία θα είναι προσβάσιμη σε Μικρομεσαίες Επιχειρήσεις και οργανισμούς με περιορισμένους πόρους, παρέχοντάς τους τη δυνατότητα να επιτύχουν υψηλό επίπεδο συμμόρφωσης χωρίς δυσβάσταχτο οικονομικό κόστος.
3) **Τεχνική Επαλήθευση σε Πραγματικό Χρόνο**: Πέρα από τη διοικητική συμμόρφωση, η εργασία στοχεύει στην ανάπτυξη αυτοματοποιημένων τεχνικών ελέγχων. Συγκεκριμένα, επιδιώκεται η υλοποίηση ενός μηχανισμού ελέγχου ιστοσελίδων (Cookie Audit) που θα σαρώνει τον δημόσιο ιστότοπο του οργανισμού, θα εντοπίζει τεχνολογίες ιχνηλάτησης (trackers/pixels) και θα επαληθεύει τις κατευθυντήριες γραμμές του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (EDPB) για τη λήψη συγκατάθεσης [7].
4) **Ασφαλής Αξιοποίηση της Γενετικής Τεχνητής Νοημοσύνης (Generative AI)**: Ίσως ο πιο φιλόδοξος στόχος της διατριβής είναι η διερεύνηση των δυνατοτήτων των Μεγάλων Γλωσσικών Μοντέλων (LLMs) στη συγγραφή νομικών κειμένων. Η εργασία στοχεύει να αποδείξει ότι η χρήση Τοπικών Μοντέλων (Local LLMs), τα οποία εκτελούνται εντός της υποδομής του οργανισμού, μπορεί να προσφέρει την ευφυΐα και την παραγωγικότητα της Τεχνίτης Νοημοσύνης(AI), εξαλείφοντας ταυτόχρονα τους κινδύνους ασφαλείας και ιδιωτικότητας που συνοδεύουν τις cloud-based υπηρεσίες (όπως το ChatGPT). Στόχος είναι η παραγωγή κειμένων Πολιτικής Απορρήτου (Privacy Policies) και Διαδικασιών Ασφαλείας που είναι νομικά συνεκτικά, εξατομικευμένα και άμεσα αξιοποιήσιμα.[7]

Συνολικά, ο σκοπός της διπλωματικής εργασίας δεν περιορίζεται μόνο στη δημιουργία ενός ακόμη εργαλείου συμμόρφωσης, αλλά στην ανάπτυξη ενός πρότυπου πληροφοριακού συστήματος που μπορεί να λειτουργήσει ως σημείο αναφοράς για μελλοντικά ερευνητικά και εμπορικά συστήματα RegTech. Το «GDPR ASSESSOR» αντιμετωπίζεται ως ερευνητικό τεχνούργημα (research artefact), το οποίο ενσωματώνει στην πράξη αρχές όπως η «προστασία δεδομένων εξ ορισμού και εξ αρχής» (privacy by design and by default) και επιδεικνύει πώς η τεχνολογία των τοπικών LLMs μπορεί να αξιοποιηθεί με τρόπο συμβατό με τις απαιτήσεις του GDPR και των εποπτικών αρχών.[7]

Με βάση τον παραπάνω σκοπό, η παρούσα διπλωματική εργασία καλείται να απαντήσει στα ακόλουθα ερευνητικά ερωτήματα:

1) Σε ποιο βαθμό είναι εφικτό να σχεδιαστεί ένα πληροφοριακό σύστημα που να καθοδηγεί τον χρήστη βήμα προς βήμα στη διενέργεια DPIA και Gap Analysis, αξιοποιώντας δομημένα ερωτηματολόγια τα οποία συνδέονται άμεσα με συγκεκριμένα άρθρα του GDPR;[7]
2) Πώς μπορεί να ενσωματωθεί ένα τοπικά εκτελούμενο Μεγάλο Γλωσσικό Μοντέλο, ώστε να συνθέτει κείμενα πολιτικής απορρήτου και διαδικασιών ασφαλείας, ελαχιστοποιώντας ταυτόχρονα τις νομικά επικίνδυνες παραγωγές ψευδών πληροφοριών;[7]

3) Ποια αρχιτεκτονικά πρότυπα (π.χ. schema-driven development, αποθήκευση σε JSON, modular σχεδίαση) διευκολύνουν την προσαρμογή του συστήματος σε μελλοντικές αλλαγές του κανονιστικού πλαισίου (π.χ. ερμηνευτικές οδηγίες Αρχών ή νέοι ευρωπαϊκοί κανονισμοί όπως ο AI Act);[7]
4) Σε ποιον βαθμό ένα τέτοιο σύστημα μπορεί να αποτελέσει ρεαλιστική, οικονομικά προσιτή εναλλακτική για μία ΜμΕ (Μικρομεσαία επιχείρηση) σε σχέση με τις υφιστάμενες, βαριές και υψηλού κόστους πλατφόρμες συμμόρφωσης;

1.3 Αντικείμενο της Διπλωματικής Εργασίας

Για την επίτευξη των προαναφερθέντων στόχων, το αντικείμενο της παρούσας διπλωματικής εργασίας συνίσταται στον πλήρη κύκλο ανάπτυξης λογισμικού (Software Development Life Cycle - SDLC) μιας καινοτόμου διαδικτυακής πλατφόρμας, η οποία φέρει την ονομασία "GDPR ASSESOR". Η πλατφόρμα αυτή αποτελεί ένα σύνθετο τεχνολογικό οικοσύστημα που συνδυάζει παραδοσιακές τεχνικές προγραμματισμού ιστού με προηγμένους αλγορίθμους μηχανικής μάθησης.[7]

Το αντικείμενο της εργασίας αναλύεται στις ακόλουθες διακριτές αλλά αλληλένδετες πτυχές έρευνας και υλοποίησης:

1. **Αρχιτεκτονική Λογισμικού και Backend Υποδομή**: Σχεδιασμός και υλοποίηση της λογικής του συστήματος με χρήση της γλώσσας προγραμματισμού Python και του μικρο-πλαισίου (micro-framework) Flask. Η επιλογή αυτή έγινε με γνώμονα την ευελιξία, την ταχύτητα ανάπτυξης και την άριστη συμβατότητα της Python με βιβλιοθήκες Τεχνητής Νοημοσύνης. Το σύστημα διαχειρίζεται τις συνεδρίες των χρηστών, την αποθήκευση των δεδομένων αξιολόγησης σε δομημένη μορφή (JSON) και τον συντονισμό των επιμέρους υποσυστημάτων.
2. **Σχεδιασμός Βάσης Γνώσης και Ερωτηματολογίων**: Ένα σημαντικό μέρος του αντικειμένου αφορά τη "μετάφραση" της νομικής γλώσσας σε αλγοριθμική λογική. Αναπτύχθηκαν εξειδικευμένα σχήματα δεδομένων (JSON Schemas) για τα ερωτηματολόγια DPIA (βάσει του Άρθρου 35) και Gap Analysis (βάσει προτύπων ISO/IEC 27001). Η υλοποίηση περιλαμβάνει κανόνες εξαρτήσεων (conditional logic), ώστε η ροή των ερωτήσεων να προσαρμόζεται δυναμικά ανάλογα με τις απαντήσεις, προσφέροντας μια εξατομικευμένη εμπειρία χρήσης.[7]

3. **Μηχανική Δεδομένων Ιστού (Web Scraping & Auditing):** Ανάπτυξη αλγορίθμου ("Site Inspector") που λειτουργεί ως αυτόνομος πράκτορας (agent), επισκεπτόμενος την ιστοσελίδα-στόχο. Ο αλγόριθμος αναλύει τις κεφαλίδες HTTP, τα cookies και τα scripts τρίτων (third-party scripts), κατηγοριοποιώντας τα ευρήματα σε κατηγορίες όπως "Απαραίτητα", "Στατιστικά" και "Διαφήμισης". Τα αποτελέσματα αυτά τροφοδοτούν αυτόματα την ενότητα της Πολιτικής Cookies, μειώνοντας την ανάγκη για χειροκίνητη καταγραφή.[7]

4. **Ενσωμάτωση Τοπικής Τεχνητής Νοημοσύνης (Local AI Integration):** Το πιο καινοτόμο τμήμα του αντικειμένου αφορά τη διασύνδεση της εφαρμογής με το εργαλείο Ollama για την τοπική εκτέλεση του γλωσσικού μοντέλου Llama 3. Αναπτύχθηκε μια μηχανή διαχείρισης εντολών (Prompt Engineering Engine), η οποία συνθέτει δυναμικά τις οδηγίες προς το μοντέλο AI, ενσωματώνοντας τα δεδομένα που συλλέχθηκαν από τα ερωτηματολόγια. Αυτό επιτρέπει την παραγωγή κειμένων φυσικής γλώσσας (Natural

Language Generation - NLG) ακρίβειας, τα οποία εξάγονται τελικά σε επαγγελματικές μορφές (Markdown, PDF).[7]

5. **Οπτικοποίηση Δεδομένων και Αναφορές (Analytics):** Τέλος, το αντικείμενο περιλαμβάνει τον σχεδιασμό εργαλείων οπτικής ανάλυσης. Χρησιμοποιώντας σύγχρονες βιβλιοθήκες JavaScript (Chart.js), αναπτύχθηκαν διαγράμματα ραντάρ (Radar Charts) για την αποτύπωση της ωριμότητας συμμόρφωσης και πίνακες κινδύνου (Risk Matrices), παρέχοντας στους υπευθύνους λήψης αποφάσεων μια άμεση και κατανοητή εικόνα της κατάστασης του οργανισμού.

Συνοψίζοντας, το αντικείμενο της διπλωματικής εργασίας είναι διττό: αφενός, ο συστηματικός σχεδιασμός και η υλοποίηση ενός ολοκληρωμένου πληροφοριακού συστήματος «GDPR ASSESSOR», το οποίο καλύπτει πλήρη κύκλο λειτουργιών από τη συλλογή πληροφοριών μέχρι την παραγωγή νομικών κειμένων· αφετέρου, η πειραματική διερεύνηση του κατά πόσο μια τέτοια αρχιτεκτονική μπορεί να μειώσει το γνωστικό και διοικητικό βάρος των υπευθύνων συμμόρφωσης. Η εργασία δεν περιορίζεται σε θεωρητική ανάλυση, αλλά εστιάζει στην παραγωγή ενός πρακτικού τεχνουργήματος που μπορεί να δοκιμαστεί, να αξιολογηθεί και να επεκταθεί στο μέλλον, τόσο στο πλαίσιο της ακαδημαϊκής έρευνας όσο και σε πραγματικά επιχειρησιακά περιβάλλοντα.

1.4 Δομή της διπλωματικής εργασίας

Η παρούσα διπλωματική εργασία διαρθρώνεται σε οκτώ διακριτά αλλά αλληλένδετα κεφάλαια, τα οποία ακολουθούν τη λογική αλληλουχία της ανάπτυξης λογισμικού και της επιστημονικής έρευνας. Η δομή έχει σχεδιαστεί ώστε να καθοδηγεί τον αναγνώστη από το θεωρητικό υπόβαθρο στην πρακτική υλοποίηση και τελικά στην αξιολόγηση των αποτελεσμάτων.

Αναλυτικότερα, η εργασία οργανώνεται ως εξής:

- **Κεφάλαιο 2:** Ανάλυση Τρέχοντος Επιπέδου (State of the Art) Το δεύτερο κεφάλαιο θέτει τα θεωρητικά θεμέλια της διατριβής. Πραγματοποιείται μια συστηματική βιβλιογραφική ανασκόπηση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), εστιάζοντας στις έννοιες-κλειδιά όπως η "λογοδοσία" (accountability) και η "προστασία των δεδομένων ήδη από τον σχεδιασμό" (Privacy by Design). Παράλληλα, εξετάζεται το τοπίο της Κανονιστικής Τεχνολογίας (RegTech) τόσο στην Ελλάδα όσο και διεθνώς, εντοπίζοντας τα κενά στις υπάρχουσες λύσεις λογισμικού και αναδεικνύοντας την ανάγκη για οικονομικά και ασφαλή εργαλεία αυτοματοποίησης [8].
- **Κεφάλαιο 3**: Μεθοδολογία (Methodology) Στο κεφάλαιο αυτό παρουσιάζεται το μεθοδολογικό πλαίσιο που υιοθετήθηκε για την έρευνα. Η εργασία βασίζεται στις αρχές της Έρευνας Επιστήμης Σχεδιασμού (Design Science Research - DSR) [9], η οποία είναι η κατεξοχήν κατάλληλη μεθοδολογία για την ανάπτυξη καινοτόμων τεχνουργημάτων (artifacts) στα Πληροφοριακά Συστήματα. Περιγράφονται αναλυτικά τα ερευνητικά ερωτήματα, οι φάσεις ανάπτυξης και τα κριτήρια αξιολόγησης του συστήματος.
- **Κεφάλαιο 4:** Αρχιτεκτονική Συστήματος (System Architecture) Το τέταρτο κεφάλαιο εστιάζει στον τεχνικό σχεδιασμό της πλατφόρμας "GDPR Assesor". Αναλύονται οι λειτουργικές και μη λειτουργικές απαιτήσεις, όπως αυτές προέκυψαν από τη μελέτη του

Άρθρου 35 του GDPR (DPIA). Παρουσιάζονται διαγράμματα που αποτυπώνουν τη δομή, τις ροές δεδομένων και τις αλληλεπιδράσεις μεταξύ των υποσυστημάτων, παρέχοντας μια σαφή εικόνα της "λογικής" πίσω από τον κώδικα [10].

- **Κεφάλαιο 5:** Εργαλεία Ανάπτυξης Συστήματος (Development Tools) Εδώ αιτιολογείται η επιλογή της τεχνολογικής στοίβας (tech stack). Αναλύονται τα πλεονεκτήματα της γλώσσας Python και του μικρο-πλαισίου Flask για την ανάπτυξη ασφαλών διαδικτυακών εφαρμογών. Ιδιαίτερη έμφαση δίνεται στην τεχνολογία Ollama και στο μοντέλο Llama 3, εξηγώντας πώς η τοπική εκτέλεση LLMs (Local Inference) επιλύει τα προβλήματα ιδιωτικότητας που μαστίζουν τις cloud-based λύσεις AI [11].
- **Κεφάλαιο 6:** Το Σύστημα (The System Implementation) Αποτελεί τον πυρήνα της υλοποιητικής προσπάθειας. Στο κεφάλαιο αυτό παρουσιάζεται αναλυτικά η τελική εφαρμογή μέσα από σενάρια χρήσης. Περιγράφονται βήμα προς βήμα οι λειτουργίες του συστήματος: από τη διενέργεια της Εκτίμησης Αντικτύπου (DPIA) και τον έλεγχο cookies (Cookie Audit), μέχρι την αυτόματη παραγωγή της Πολιτικής Απορρήτου. Η παρουσίαση συνοδεύεται από στιγμιότυπα οθόνης (screenshots) και επεξηγήσεις της διεπαφής χρήστη.[11]

- **Κεφάλαιο 7:** Συζήτηση (Discussion) Στο κεφάλαιο της συζήτησης επιχειρείται η κριτική αποτίμηση των ευρημάτων. Τα αποτελέσματα της αυτοματοποιημένης συγγραφής κειμένων συγκρίνονται με πρότυπα ανθρώπινης γραφής, ενώ αναλύονται οι περιορισμοί των τρεχόντων γλωσσικών μοντέλων, όπως ο κίνδυνος των "ψευδαισθήσεων" (hallucinations) [12]. Εξετάζεται κατά πόσο το σύστημα επιτυγχάνει τους στόχους που τέθηκαν και πώς τοποθετείται απέναντι στον ανταγωνισμό.
- **Κεφάλαιο 8**: Συμπεράσματα και Προοπτικές (Conclusions & Future Work) Η εργασία ολοκληρώνεται με τη σύνοψη των συμπερασμάτων και την πρόταση κατευθύνσεων για μελλοντική έρευνα. Γίνεται αναφορά στις προοπτικές επέκτασης του συστήματος ώστε να καλύπτει τον επερχόμενο Κανονισμό για την Τεχνητή Νοημοσύνη (EU AI Act) και τη δυνατότητα προσαρμογής (fine-tuning) του μοντέλου στην ελληνική νομοθεσία.[12]

Η ανωτέρω διάρθρωση εξασφαλίζει μια συστηματική πορεία από τη θεωρητική ανάλυση των τεχνικών απαιτήσεων στην έμπρακτη τεχνική υλοποίηση, διασφαλίζοντας τη συνοχή μεταξύ του κανονιστικού πλαισίου και του παραχθέντος λογισμικού. Μέσω αυτής της διαδοχικής προσέγγισης, η εργασία φιλοδοξεί να καταδείξει πώς η συνέργεια των τοπικών γλωσσικών μοντέλων (Local LLMs) και του σχεδιασμού βάσει σχήματος (schema-driven design) μπορεί να προσφέρει μια βιώσιμη λύση στο πρόβλημα της κανονιστικής συμμόρφωσης. Τελικός στόχος είναι η επικύρωση του "GDPR ASSESSOR" ως ενός λειτουργικού ερευνητικού τεχνουργήματος, το οποίο δεν περιορίζεται στην απλή καταγραφή δεδομένων, αλλά εισάγει την έννοια της "Παραγωγικής Συμμόρφωσης" (Generative Compliance) στην υπηρεσία των μικρομεσαίων επιχειρήσεων, θέτοντας ταυτόχρονα τις βάσεις για μελλοντική έρευνα στον τομέα της παραγωγής πολιτικών ιδιοτικότητας.[12]

2 Ανάλυση Τρέχοντος Επιπέδου

Στο παρόν κεφάλαιο πραγματοποιείται η ανάλυση του τρέχοντος επιπέδου (state of the art) στον χώρο της προστασίας προσωπικών δεδομένων και της κανονιστικής τεχνολογίας (RegTech), με έμφαση στον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Η ανάλυση αναπτύσσεται σε τρία επίπεδα: (α) το νομικό και κανονιστικό πλαίσιο, όπως αυτό διαμορφώνεται από τον ίδιο τον Κανονισμό, τις ερμηνευτικές οδηγίες και τη νομολογία, (β) τις διαθέσιμες λύσεις λογισμικού στην ελληνική και διεθνή αγορά που υποστηρίζουν τη συμμόρφωση, και (γ) τις τεχνολογικές εξελίξεις στα Μεγάλα Γλωσσικά Μοντέλα (LLMs) και την αξιοποίησή τους στη νομική τεχνολογία. Με τον τρόπο αυτό, το κεφάλαιο θέτει τις βάσεις για την κατανόηση του ερευνητικού κενού που έρχεται να καλύψει το σύστημα «GDPR ASSESSOR».[12]

2.1 Βασικές έννοιες και ορισμοί

Η κατανόηση του πολύπλοκου κανονιστικού πλαισίου της Ευρωπαϊκής Ένωσης αποτελεί προαπαιτούμενο για τον σχεδιασμό οποιουδήποτε πληροφοριακού συστήματος διαχείρισης απορρήτου. Παρακάτω αναλύονται οι κρίσιμοι ορισμοί, όπως αυτοί διατυπώνονται στο κείμενο του Κανονισμού (ΕΕ) 2016/679 και ερμηνεύονται από τη σύγχρονη βιβλιογραφία.[12]

Η συστηματική παρουσίαση των παραπάνω εννοιών δεν αποτελεί απλώς θεωρητικό υπόβαθρο, αλλά λειτουργεί ως οδηγός για τον σχεδιασμό του ίδιου του πληροφοριακού συστήματος. Κάθε βασικός νομικός όρος (π.χ. «δραστηριότητα επεξεργασίας», «υποκείμενο των δεδομένων», «εκτίμηση αντικτύπου») αντιστοιχίζεται σε συγκεκριμένα τμήματα των ερωτηματολογίων, σε πεδία καταγραφής ή σε μηχανισμούς τεχνικού ελέγχου. Με αυτόν τον τρόπο, η νομική ορολογία «μεταφράζεται» σε δομές δεδομένων και λειτουργικές απαιτήσεις, επιτρέποντας στο σύστημα να υποστηρίζει τον χρήστη όχι μόνο σε επίπεδο ορολογίας, αλλά και σε επίπεδο πρακτικών βημάτων συμμόρφωσης.[2]

2.1.1 Δεδομένα Προσωπικού Χαρακτήρα

Σύμφωνα με το Άρθρο 4(1) του GDPR, ως δεδομένα προσωπικού χαρακτήρα ορίζεται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Η νομική αυτή έννοια είναι εξαιρετικά ευρεία και δυναμική. Δεν περιορίζεται στα προφανή αναγνωριστικά, όπως το ονοματεπώνυμο ή η διεύθυνση κατοικίας, αλλά επεκτείνεται σε τεχνικά δεδομένα που παράγονται κατά την ψηφιακή αλληλεπίδραση [13].

Ιδιαίτερη σημασία για την παρούσα εργασία έχουν οι "επιγραμμικοί αναγνωριστικοί κωδικοί" (online identifiers), όπως οι διευθύνσεις πρωτοκόλλου διαδικτύου (IP Addresses), τα αναγνωριστικά συσκευών (MAC addresses) και τα αρχεία καταγραφής "cookies". Όπως

επισημαίνει το Δικαστήριο της Ευρωπαϊκής Ένωσης (υπόθεση Breyer, C-582/14), ακόμα και μια δυναμική διεύθυνση IP μπορεί να θεωρηθεί προσωπικό δεδομένο, εάν ο διαχειριστής της ιστοσελίδας διαθέτει τα νομικά μέσα να ταυτοποιήσει τον χρήστη μέσω του παρόχου διαδικτύου [14]. Αυτή η ευρεία ερμηνεία καθιστά αναγκαία την ανάπτυξη εργαλείων όπως το Cookie Audit της εφαρμογής μας, το οποίο εντοπίζει και κατηγοριοποιεί αυτούς τους ιχνηλάτες.

2.1.2 Επεξεργασία (Processing)

Ο όρος «επεξεργασία» (Άρθρο 4(2)) καλύπτει πρακτικά κάθε ενέργεια που μπορεί να πραγματοποιηθεί σε δεδομένα προσωπικού χαρακτήρα, είτε αυτή γίνεται με αυτοματοποιημένα μέσα είτε χειρωνακτικά. Με άλλα λόγια, δεν περιορίζεται σε "τεχνικές" λειτουργίες, αλλά περιλαμβάνει ολόκληρο το φάσμα ενεργειών που συνδέονται με τον τρόπο που τα δεδομένα εισέρχονται, χρησιμοποιούνται και εξέρχονται από έναν οργανισμό. Ενδεικτικά, περιλαμβάνει τη συλλογή, την καταχώριση, την οργάνωση και τη διάρθρωση, την αποθήκευση, την προσαρμογή ή τροποποίηση, την ανάκτηση και την αναζήτηση πληροφοριών, τη χρήση, την κοινολόγηση και τη διάδοση, τη συσχέτιση ή συνδυασμό, τον περιορισμό, καθώς και τη διαγραφή ή καταστροφή [GDPR Art. 4(2)]. Η ευρύτητα του ορισμού είναι κρίσιμη, διότι επιτρέπει στον Κανονισμό να εφαρμόζεται σε όλες τις πραγματικές ροές δεδομένων ενός οργανισμού, ανεξάρτητα από την τεχνολογία που χρησιμοποιείται ή το στάδιο στο οποίο βρίσκεται η πληροφορία.[14]

Στο πλαίσιο της εφαρμογής «GDPR ASSESSOR», η έννοια της επεξεργασίας επιχειρείται να αποτυπωθεί με συστηματικό τρόπο μέσω του εργαλείου ROPA (Record of Processing Activities). Συγκεκριμένα, ο χρήστης καθοδηγείται να περιγράψει τον κύκλο ζωής των δεδομένων εντός του οργανισμού: από το σημείο συλλογής ή δημιουργίας τους, τους σκοπούς και τα μέσα επεξεργασίας, τους ρόλους και τις αρμοδιότητες (π.χ. ποιος αποφασίζει και ποιος εκτελεί), μέχρι τα σημεία κοινολόγησης, τις περιόδους τήρησης, τα μέτρα ασφάλειας, και τελικά τη λήξη της επεξεργασίας μέσω διαγραφής ή καταστροφής. Με αυτόν τον τρόπο, το ROPA λειτουργεί ως δομημένο "χάρτης" των δραστηριοτήτων επεξεργασίας και ως πρακτικό εργαλείο τεκμηρίωσης, ώστε ο οργανισμός να έχει σαφή εικόνα του πού βρίσκονται τα δεδομένα, γιατί και πώς χρησιμοποιούνται, και ποια βήματα απαιτούνται για τη συμμόρφωση.[14]

2.1.3 Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA)

Η Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (Data Protection Impact Assessment – DPIA) συνιστά κεντρικό μηχανισμό υλοποίησης της αρχής της Λογοδοσίας, καθώς μετατρέπει τη συμμόρφωση από γενική υποχρέωση σε τεκμηριωμένη, ελέγξιμη πρακτική. Σύμφωνα με το Άρθρο 35 του GDPR, η διενέργεια DPIA είναι υποχρεωτική όταν ένα είδος επεξεργασίας—ιδίως όταν αξιοποιεί νέες τεχνολογίες—είναι πιθανό να δημιουργήσει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων [15]. Η λογική της διάταξης είναι προληπτική: ο οργανισμός καλείται να εντοπίσει εγκαίρως πιθανούς κινδύνους και να υιοθετήσει μέτρα μετριασμού πριν η επεξεργασία τεθεί σε πλήρη λειτουργία ή κλιμακωθεί.

Η DPIA δεν αποτελεί μια απλή "λίστα ελέγχου" (checklist), αλλά μια συστηματική και επαναληπτική διαδικασία ανάλυσης και τεκμηρίωσης, η οποία, σε λειτουργικό επίπεδο, περιλαμβάνει τέσσερις βασικές συνιστώσες:[15]

1. τη συστηματική περιγραφή των πράξεων επεξεργασίας, ώστε να αποτυπώνεται με σαφήνεια τι δεδομένα εμπλέκονται, ποιοι είναι οι σκοποί, ποιοι είναι οι ρόλοι και οι ροές, καθώς και ποια συστήματα ή πάροχοι συμμετέχουν,
2. την αξιολόγηση της αναγκαιότητας και της αναλογικότητας, δηλαδή τη διερεύνηση κατά πόσο η επιλεγμένη επεξεργασία είναι κατάλληλη και περιορίζεται στο απολύτως απαιτούμενο για τον σκοπό,
3. την εκτίμηση των κινδύνων για τα δικαιώματα των υποκειμένων, με έμφαση στις πιθανές επιπτώσεις (π.χ. απώλεια ελέγχου, διακρίσεις, μη εξουσιοδοτημένη πρόσβαση, ή άλλες αρνητικές συνέπειες), και
4. τον καθορισμό μέτρων για την αντιμετώπιση των κινδύνων, μέσω τεχνικών και οργανωτικών ελέγχων που μειώνουν τόσο την πιθανότητα όσο και τη σοβαρότητα των επιπτώσεων.

Η πολυπλοκότητα της DPIA—ιδίως όταν υπάρχουν πολλαπλές ροές δεδομένων, εμπλοκή τρίτων, ή τεχνολογίες αυξημένου ρίσκου—αποτελεί βασικό κίνητρο για την αυτοματοποίησή της. Στο πλαίσιο του συστήματος που αναπτύχθηκε, η διαδικασία υποστηρίζεται με καθοδήγηση βήμα-βήμα, ώστε ο χρήστης να μεταφράζει τις απαιτήσεις του Άρθρου 35 σε συγκεκριμένες ενέργειες τεκμηρίωσης και αξιολόγησης. Με αυτόν τον τρόπο, μειώνεται η αβεβαιότητα ως προς το "τι ακριβώς πρέπει να καταγραφεί", περιορίζεται ο διοικητικός φόρτος, και ενισχύεται η συνέπεια της αξιολόγησης μεταξύ διαφορετικών περιπτώσεων επεξεργασίας, χωρίς να υποκαθίσταται η ευθύνη του οργανισμού για την τελική κρίση και τεκμηρίωση [15].

2.1.4 Ανάλυση Κενών (Gap Analysis)

Παρότι ο όρος «Gap Analysis» δεν εμφανίζεται ρητά στο κείμενο του GDPR, χρησιμοποιείται ευρέως ως διεθνώς αναγνωρισμένη βέλτιστη πρακτική στη διαχείριση ασφάλειας πληροφοριών και στη συμμόρφωση, ιδίως σε πλαίσια που βασίζονται σε πρότυπα όπως το ISO/IEC 27001. Η Ανάλυση Κενών περιγράφεται ως μια δομημένη διαδικασία σύγκρισης μεταξύ της υφιστάμενης κατάστασης ενός οργανισμού («As-Is») και της επιθυμητής/στόχευσης κατάστασης πλήρους συμμόρφωσης («To-Be») [16]. Σκοπός της δεν είναι απλώς η "καταγραφή προβλημάτων", αλλά η συστηματική αποτύπωση του τι υπάρχει ήδη, τι απαιτείται βάσει των κανόνων, και ποια συγκεκριμένα βήματα πρέπει να υλοποιηθούν για να κλείσει η απόσταση μεταξύ των δύο καταστάσεων.

Στο πλαίσιο της παρούσας διατριβής, η Ανάλυση Κενών εστιάζει στα οργανωτικά και τεχνικά μέτρα ασφαλείας (Άρθρο 32), αντιμετωπίζοντας τη συμμόρφωση ως ένα σύνολο πρακτικών που πρέπει να λειτουργούν στην καθημερινή επιχειρησιακή πραγματικότητα. Ειδικότερα, η ανάλυση στοχεύει στον εντοπισμό ελλείψεων: [16]

1) σε πολιτικές και διαδικασίες (π.χ. σαφήνεια ρόλων και κανόνων, τυποποιημένες οδηγίες χειρισμού δεδομένων),
2) στην εκπαίδευση και ευαισθητοποίηση προσωπικού (ώστε οι απαιτήσεις να εφαρμόζονται ομοιόμορφα και όχι αποσπασματικά)
3) σε μηχανισμούς ανίχνευσης και απόκρισης σε περιστατικά παραβίασης (ώστε να υπάρχει έγκαιρη αναγνώριση, καταγραφή, κλιμάκωση και αποκατάσταση). Με αυτόν

τον τρόπο, η Gap Analysis λειτουργεί ως εργαλείο προτεραιοποίησης: δεν περιορίζεται στο να δηλώσει ότι «υπάρχει έλλειμμα», αλλά βοηθά να προσδιοριστεί πού ακριβώς βρίσκεται το κενό, ποια είναι η επιχειρησιακή του σημασία, και ποια μέτρα είναι αναγκαία για τη μετάβαση από το «As-Is» στο «To-Be» [16].

Παράλληλα, για να είναι πρακτικά αξιοποιήσιμη, η Ανάλυση Κενών πρέπει να καταλήγει σε ένα σαφές και εφαρμόσιμο σχέδιο δράσης. Στην παρούσα προσέγγιση, τα ευρήματα δεν παραμένουν σε επίπεδο γενικών διαπιστώσεων, αλλά μετατρέπονται σε συγκεκριμένες ενέργειες βελτίωσης, με στόχο τη συστηματική κάλυψη των αποκλίσεων που εντοπίστηκαν. Αυτό προϋποθέτει ότι κάθε κενό συνδέεται με τη σχετική απαίτηση συμμόρφωσης και αξιολογείται ως προς τη σοβαρότητα και τον κίνδυνο που συνεπάγεται, ώστε να τεθούν ρεαλιστικές προτεραιότητες. Επιπλέον, καθορίζονται υπευθυνότητες και βασικά ορόσημα υλοποίησης, ώστε η μετάβαση από το «As-Is» στο «To-Be» να μην αποτελεί θεωρητικό στόχο, αλλά διαδικασία που μπορεί να παρακολουθείται, να τεκμηριώνεται και να βελτιώνεται διαρκώς, ενισχύοντας τη λογοδοσία και την αποτελεσματικότητα των οργανωτικών και τεχνικών μέτρων [16].

2.1.5 Προστασία των Δεδομένων ήδη από τον Σχεδιασμό (Privacy by Design)

Η αρχή του Privacy by Design (PbD), όπως κατοχυρώνεται στο Άρθρο 25, απαιτεί από τους οργανισμούς να ενσωματώνουν την προστασία δεδομένων ως βασική παράμετρο ήδη από τα αρχικά στάδια σχεδιασμού και ανάπτυξης ενός συστήματος, αντί να επιχειρούν να την προσθέσουν εκ των υστέρων ως διορθωτική παρέμβαση [17]. Η λογική της αρχής είναι ότι οι κρίσιμες αποφάσεις—όπως η αρχιτεκτονική, οι ροές δεδομένων, οι ρυθμίσεις πρόσβασης και οι προεπιλογές—καθορίζουν σε μεγάλο βαθμό το επίπεδο ιδιωτικότητας και ασφάλειας που μπορεί να επιτευχθεί. Στο ίδιο πνεύμα, το Privacy by Design αποτέλεσε καθοδηγητική αρχή για την ανάπτυξη του «GDPR ASSESSOR», ώστε η προστασία των δεδομένων να αποτελεί εγγενές χαρακτηριστικό της λύσης και όχι εξωτερικό πρόσθετο. Ειδικότερα, η επιλογή αρχιτεκτονικής τοπικής εκτέλεσης (Local Execution) για το μοντέλο Τεχνητής Νοημοσύνης (Ollama/Llama 3) συνιστά πρακτική εφαρμογή του PbD, καθώς διασφαλίζει ότι τα δεδομένα που σχετίζονται με τις αξιολογήσεις δεν αποστέλλονται σε εξωτερικές υπηρεσίες και δεν εγκαταλείπουν την υποδομή του χρήστη. Με αυτόν τον τρόπο μειώνεται ουσιαστικά η επιφάνεια έκθεσης, περιορίζονται οι κίνδυνοι μη εξουσιοδοτημένης πρόσβασης ή διαρροής, και ενισχύεται η εμπιστευτικότητα των πληροφοριών που επεξεργάζεται το σύστημα, σε ευθυγράμμιση με την προληπτική λογική του Άρθρου 25 [17].

2.1.6 Λογοδοσία

Η αρχή της Λογοδοσίας (Άρθρο 5(2)) καθιερώνει ότι η ευθύνη για τη συμμόρφωση δεν είναι μόνο ουσιαστική, αλλά και αποδεικτική, μεταθέτοντας το βάρος τεκμηρίωσης στον Υπεύθυνο Επεξεργασίας. Αυτό σημαίνει ότι δεν αρκεί ένας οργανισμός να εφαρμόζει τις απαιτήσεις του Κανονισμού στην πράξη· οφείλει παράλληλα να διαθέτει κατάλληλη και διαρκώς ενημερωμένη τεκμηρίωση που να αποδεικνύει ότι οι διαδικασίες, οι αποφάσεις και τα μέτρα που λαμβάνονται είναι ευθυγραμμισμένα με τον GDPR. Στην πράξη, η λογοδοσία προϋποθέτει ίχνη ελέγχου, σαφείς ρόλους και αρμοδιότητες, καταγραφή αξιολογήσεων και ελέγχων, καθώς και δυνατότητα άμεσης

παρουσίασης αποδεικτικών στοιχείων προς τις εποπτικές αρχές, όποτε αυτό ζητηθεί, χωρίς καθυστέρηση ή ασάφεια [18].

2.2 Τρέχουσα Κατάσταση στην Ελλάδα

Η ελληνική αγορά ψηφιακών υπηρεσιών και εργαλείων συμμόρφωσης παρουσιάζει μια χαρακτηριστική δυαδικότητα. Από τη μία πλευρά, καταγράφεται ενίσχυση των δράσεων ψηφιακού μετασχηματισμού σε επιχειρήσεις και οργανισμούς, κυρίως μέσω δημόσιων πρωτοβουλιών και κοινοτικών χρηματοδοτήσεων. Από την άλλη, η προστασία δεδομένων συχνά αντιμετωπίζεται ως «υποχρέωση συμμόρφωσης» που πρέπει να ολοκληρωθεί τυπικά, και όχι ως λειτουργικό στοιχείο διακυβέρνησης και ανταγωνιστικό πλεονέκτημα. Μέσα σε αυτό το περιβάλλον, οι εγχώριες λύσεις για την κάλυψη απαιτήσεων των πολιτικών απορρήτων τείνουν να κινούνται σε δύο βασικούς άξονες: είτε ως εργαλεία ροής εργασιών (workflow tools) για καταγραφή και τεκμηρίωση, είτε ως νομικές «εργαλειοθήκες» (templates/πρότυπα), με περιορισμένη ενσωμάτωση ευφυών μηχανισμών αυτοματοποίησης που θα μείωναν ουσιαστικά τον χρόνο και την αβεβαιότητα εφαρμογής.[18]

Για την αποτύπωση του τρέχοντος επιπέδου ωριμότητας, εξετάστηκαν οκτώ (8) αντιπροσωπευτικές περιπτώσεις εργαλείων/υπηρεσιών που δραστηριοποιούνται στον ελληνικό χώρο, με κριτήρια την αναγνωρισιμότητα, το εύρος λειτουργιών και την τεχνολογική προσέγγιση. Η ανάλυση που ακολουθεί δεν στοχεύει στην «αξιολόγηση αγοράς» με εμπορικούς όρους, αλλά στην ανάδειξη επαναλαμβανόμενων μοτίβων ως προς το αν τα εργαλεία υποστηρίζουν απλώς την τεκμηρίωση ή αν συμβάλλουν ενεργά στη δημιουργία συμμορφωτικών αποτελεσμάτων.

1) **e-Compliance GDPR (Bee Group)**

   Η πλατφόρμα της Bee Group συγκαταλέγεται στις πρώιμες προσπάθειες ψηφιοποίησης της συμμόρφωσης στην Ελλάδα, ως σύστημα τύπου SaaS (Software as a Service) με κύρια έμφαση στη δομημένη καταγραφή δραστηριοτήτων επεξεργασίας.

Ανάλυση: Παρέχει ψηφιακές φόρμες για τη δημιουργία του Αρχείου Δραστηριοτήτων (ROPA) και βασικά πρότυπα για DPIA. Ωστόσο, η λογική λειτουργίας βασίζεται κυρίως στη «στατική καταχώριση» πληροφοριών: ο χρήστης εισάγει χειροκίνητα κείμενο και επιλογές, χωρίς το σύστημα να προσφέρει ουσιαστική, προσαρμοσμένη καθοδήγηση ή προτάσεις περιεχομένου (π.χ. ανά κλάδο ή τύπο επεξεργασίας). Έτσι, η παραγωγή πολιτικών και κειμένων παραμένει σε μεγάλο βαθμό ευθύνη του χρήστη, με αποτέλεσμα αυξημένο συγγραφικό και διοικητικό φόρτο [19].

2) **eQualSuite GRC (Priority Quality Consultants)**

   Το eQualSuite εντάσσεται στην κατηγορία συστημάτων Διακυβέρνησης, Ρίσκου και Συμμόρφωσης (GRC) και απευθύνεται κυρίως σε μεγάλους οργανισμούς με υφιστάμενες πιστοποιήσεις (π.χ. ISO 27001).[19]

Ανάλυση: Κύριο πλεονέκτημα είναι η δυνατότητα ενοποίησης του GDPR με άλλες απαιτήσεις εταιρικών προτύπων, καθώς και η παροχή εργαλείων όπως Incident Management και έλεγχος προμηθευτών. Παρ' όλα αυτά, η αυξημένη πολυπλοκότητα και το υψηλό κόστος κτήσης/παραμετροποίησης περιορίζουν την προσβασιμότητα για Μικρομεσαίες Επιχειρήσεις (ΜΜΕ). Επιπλέον, η λειτουργική φιλοσοφία παραμένει σε μεγάλο βαθμό «record keeping» (τήρηση αρχείων) αντί για «solution generation» (παραγωγή λύσεων), καθώς το σύστημα οργανώνει και

αποθηκεύει τεκμήρια, αλλά δεν μειώνει ουσιαστικά τον χρόνο σύνταξης και λήψης αποφάσεων συμμόρφωσης [20].

3) **GDPR in a Box (Andersen Legal Greece)**

Η λύση αυτή εκφράζει την κλασική νομική προσέγγιση και αφορά κυρίως πακέτο προτύπων εγγράφων και διαδικασιών, χωρίς να συνιστά λογισμικό με την αυστηρή έννοια.

Ανάλυση: Το νομικό περιεχόμενο είναι ποιοτικό, ωστόσο τα παραδοτέα είναι στατικά και η προσαρμογή τους στη λειτουργική πραγματικότητα του κάθε οργανισμού απαιτεί χειροκίνητη επεξεργασία. Σε πρακτικό επίπεδο, αλλαγές στη δομή, στις ροές δεδομένων ή στους ρόλους συνεπάγονται επαναλαμβανόμενες τροποποιήσεις σε έγγραφα Word, κάτι που αυξάνει τον κίνδυνο ασυνέπειας μεταξύ πολιτικών και την πιθανότητα ανθρώπινου λάθους, ιδίως όταν οι επικαιροποιήσεις δεν γίνονται συστηματικά [21].

4) **Υπηρεσίες DPO & Compliance (GDPR Team)**

Η GDPR Team ακολουθεί υβριδικό μοντέλο, συνδυάζοντας συμβουλευτικές υπηρεσίες με εργαλεία IT για θέματα ασφάλειας και προστασίας δεδομένων.[21]

Ανάλυση: Το μοντέλο προσφέρει πρόσβαση σε εξειδικευμένη γνώση, αλλά εξαρτάται έντονα από τον ανθρώπινο παράγοντα. Αυτό δημιουργεί περιορισμούς κλιμάκωσης (not scalable), καθώς ο χρόνος απόκρισης και η πρόοδος των εργασιών εξαρτώνται από τη διαθεσιμότητα συμβούλων και από επαναλαμβανόμενο κόστος παροχής υπηρεσιών. Σε αυτό το σημείο εντοπίζεται ένα βασικό κίνητρο της παρούσας διπλωματικής, η οποία επιχειρεί να υποστηρίξει λειτουργίες τύπου «ψηφιακού συμβούλου» διαθέσιμου σε συνεχή βάση (24/7), μειώνοντας την καθυστέρηση και τη μεταβλητότητα που συνεπάγεται η πλήρως ανθρωποκεντρική προσέγγιση [22].

5) **Freen-WHISTLE App (Freen)**

Παρότι ο βασικός της στόχος είναι η συμμόρφωση με την οδηγία/πλαίσιο whistleblowing, συχνά προσφέρεται συμπληρωματικά με υπηρεσίες GDPR.[22]

Ανάλυση: Πρόκειται για παράδειγμα επιτυχημένου εξειδικευμένου λογισμικού (niche software), με λειτουργίες όπως ανωνυμία και ασφαλή κανάλια επικοινωνίας. Ωστόσο, η αρχιτεκτονική παραμένει «σιλό» (siloed): το εργαλείο δεν διασυνδέεται λειτουργικά με ROPA ή DPIA, γεγονός που αναγκάζει τους διαχειριστές να τηρούν παράλληλες βάσεις δεδομένων και διαδικασίες για συναφή κανονιστικά θέματα, αυξάνοντας το λειτουργικό κόστος και τον κίνδυνο ασυνέπειας [23].

6) **Epsilon Informatics GDPR Services**

Ως μεγάλος πάροχος επιχειρησιακού λογισμικού, η Epsilon ενσωματώνει λειτουργίες σχετικές με GDPR σε ERP/HR συστήματα.[23]

Ανάλυση: Η προσέγγιση είναι αποτελεσματική για δεδομένα που βρίσκονται εντός του οικοσυστήματος των εφαρμογών της (π.χ. μισθοδοσία, HR διαδικασίες). Ωστόσο, δεν καλύπτει ολιστικά τη συμμόρφωση σε επίπεδο οργανισμού, καθώς σημαντικές ροές δεδομένων μπορεί να βρίσκονται εκτός ERP/HR (π.χ. ιστοσελίδα, marketing εργαλεία, cookies/trackers, φυσικά αρχεία). Έτσι, παραμένουν ουσιαστικά κενά συμμόρφωσης (compliance gaps) που δεν αντιμετωπίζονται από την «ενσωματωμένη» λειτουργικότητα [24].

7) **Space Hellas GRC Services**

Η Space Hellas παρέχει λύσεις κυβερνοασφάλειας και συμμόρφωσης σε επίπεδο enterprise, κυρίως για μεγάλους οργανισμούς.

Ανάλυση: Η έμφαση δίνεται συχνά στην τεχνική θωράκιση (π.χ. firewalls, DLP), ενώ η διοικητική διάσταση του GDPR (τεκμηρίωση, πολιτικές, διαδικασίες, ρόλοι) δεν αποτελεί πάντα τον κεντρικό άξονα. Επιπλέον, η υλοποίηση απαιτεί συνήθως εξειδικευμένο IT προσωπικό, κάτι που δεν είναι δεδομένο στη μέση ελληνική επιχείρηση. Αντίθετα, μια λύση με επίκεντρο τη χρηστικότητα και την καθοδήγηση μπορεί να είναι λειτουργική και από μη τεχνικούς χρήστες, μειώνοντας το εμπόδιο υιοθέτησης [25].

8) Data Privacy Office Europe

Ο οργανισμός παρέχει εκπαίδευση και εργαλεία πιστοποίησης DPO, καθώς και εργαλεία αξιολόγησης.

Ανάλυση: Τα εργαλεία gap analysis σε μορφή ερωτηματολογίων είναι χρήσιμα για διάγνωση και αποτύπωση επιπέδου γνώσεων/ετοιμότητας. Ωστόσο, λειτουργούν κυρίως διαγνωστικά: εντοπίζουν ελλείψεις, αλλά δεν παράγουν αυτόματα το απαραίτητο «επόμενο βήμα», όπως σχέδιο δράσης, πολιτικές ή κείμενα διαδικασιών που να αξιοποιούν άμεσα τα ευρήματα. Έτσι, ο χρήστης παραμένει υπεύθυνος για τη σύνθεση λύσεων και για τη μετατροπή της διάγνωσης σε εφαρμόσιμα παραδοτέα [26].

Συμπερασματική Αξιολόγηση Ελληνικής Αγοράς

Η επισκόπηση των παραπάνω περιπτώσεων αναδεικνύει ένα σταθερό μοτίβο: στην ελληνική αγορά υπάρχουν ώριμες επιλογές για καταγραφή και τεκμηρίωση (recording/record-keeping) και ισχυρή παρουσία συμβουλευτικών υπηρεσιών, όμως παρατηρείται περιορισμένη διαθεσιμότητα εργαλείων «Παραγωγικής Συμμόρφωσης» (Generative Compliance). Με άλλα λόγια, πολλά συστήματα λειτουργούν ως «ηλεκτρονικοί φάκελοι» που οργανώνουν πληροφορίες, χωρίς να μειώνουν ουσιαστικά το συγγραφικό βάρος και τη λήψη αποφάσεων μέσω αυτοματοποιημένης παραγωγής περιεχομένου. Παράλληλα, η υπερβολική εξάρτηση από τον ανθρώπινο παράγοντα δυσχεραίνει την κλιμάκωση, ενώ το κόστος κτήσης ή παραμετροποίησης σε ορισμένες λύσεις καθιστά την πρόσβαση πιο δύσκολη για τις ΜΜΕ. Η απουσία ενσωματωμένων μηχανισμών Τεχνητής Νοημοσύνης και πραγματικού αυτοματισμού στη σύνταξη πολιτικών, καθώς και η περιορισμένη ενσωμάτωση τεχνικών ελέγχων στη ροή εργασίας, δημιουργούν ένα πρακτικό κενό στην αγορά που αφορά την «ενεργή παραγωγή» συμμορφωτικών παραδοτέων. Το κενό αυτό αναδεικνύει την ανάγκη για μια λύση με χαμηλό κόστος χρήσης, αυξημένη χρηστικότητα και ουσιαστικό βαθμό αυτοματοποίησης, ώστε να είναι βιώσιμη και για μικρότερους οργανισμούς. Στο πλαίσιο αυτό, η παρούσα διπλωματική εργασία στοχεύει να καλύψει το παραπάνω κενό, εισάγοντας μια προσέγγιση που δεν περιορίζεται σε διαγνωστικές ερωτήσεις του τύπου «υπάρχει πολιτική;», αλλά υποστηρίζει τη δημιουργία του απαιτούμενου περιεχομένου και των βασικών παραδοτέων με τρόπο καθοδηγούμενο και λειτουργικά αξιοποιήσιμο από τον χρήστη.[26]

2.3 Τρέχουσα Κατάσταση στο Εξωτερικό

Σε αντίθεση με το ελληνικό οικοσύστημα, όπου κυριαρχούν μικρότερες, συχνά αποσπασματικές λύσεις, η διεθνής αγορά χαρακτηρίζεται από ώριμες πλατφόρμες GRC και Privacy Management με ευρύ φάσμα λειτουργιών. Ωστόσο, η μετάβαση από το ένα περιβάλλον στο άλλο δεν είναι γραμμική. Τα διεθνή εργαλεία έχουν σχεδιαστεί πρωτίστως για μεγάλους οργανισμούς, με

πολύπλοκες δομές δεδομένων και υψηλή οργανωτική ωριμότητα. Αυτό δημιουργεί μια διττή πρόκληση: αφενός, οι ελληνικές ΜΜΕ συχνά αδυνατούν να υποστηρίξουν το οικονομικό και τεχνικό βάρος αυτών των λύσεων· αφετέρου, οι απλούστερες εγχώριες εφαρμογές δεν καλύπτουν το βάθος αυτοματοποίησης και τεχνικού ελέγχου που απαιτεί ο σύγχρονος ψηφιακός μετασχηματισμός.[26]

Η διεθνής αγορά της Κανονιστικής Τεχνολογίας (RegTech) είναι σαφώς πιο ώριμη από την ελληνική, με έντονο ανταγωνισμό και υψηλή εξειδίκευση. Παρ' όλα αυτά, η πλειονότητα των λύσεων εστιάζει σε μεγάλους οργανισμούς (Enterprise level), γεγονός που αφήνει ένα πρακτικό κενό για τις μικρομεσαίες επιχειρήσεις. Για την πληρότητα της έρευνας, εξετάστηκαν οκτώ (8) αντιπροσωπευτικές πλατφόρμες που κυριαρχούν διεθνώς, με έμφαση στα πλεονεκτήματα και στους περιορισμούς τους.[26]

1) OneTrust: Ο Ηγέτης της Αγοράς

   Η OneTrust αποτελεί ολοκληρωμένο οικοσύστημα διαχείρισης απορρήτου και καλύπτει μεγάλο εύρος απαιτήσεων, από τη διαχείριση συγκατάθεσης έως την ανάλυση κινδύνου τρίτων μερών (Vendor Risk Management) [27].

Ανάλυση: Διαθέτει υψηλό βαθμό παραμετροποίησης, καθώς και έτοιμα πρότυπα για πολλαπλά νομικά πλαίσια (GDPR, CCPA, LGPD). Επιπλέον, αξιοποιεί ενημερωμένη βάση γνώσης (DataGuidance), η οποία ανανεώνεται συστηματικά από νομικούς [28]. Ωστόσο, η πολυπλοκότητά της αποτελεί ουσιαστικό εμπόδιο υιοθέτησης, καθώς η πλήρης παραμετροποίηση συχνά απαιτεί εξειδικευμένους συμβούλους και σημαντικό χρόνο υλοποίησης (6–12 μήνες). Το κόστος είναι επίσης υψηλό, με τιμολόγηση ανά ενότητα (module), που μπορεί να φτάσει δεκάδες χιλιάδες ευρώ ετησίως, καθιστώντας την μη ρεαλιστική επιλογή για μικρότερες επιχειρήσεις [29].

2) TrustArc: Η Παραδοσιακή Δύναμη

   Η TrustArc (πρώην TRUSTe) έχει μακρά παρουσία στον χώρο και εστιάζει στη στρατηγική διαχείριση κινδύνου, αξιοποιώντας αλγορίθμους για workflow automation [30].

Ανάλυση: Προσφέρει ισχυρά εργαλεία αναφορών (reporting) και dashboards με προσανατολισμό στη διοίκηση, διευκολύνοντας την τεκμηρίωση της λογοδοσίας έναντι εποπτικών αρχών. Παράλληλα, η εμπειρία χρήσης αξιολογείται συχνά ως λιγότερο φιλική σε σχέση με νεότερες πλατφόρμες, ενώ η περιορισμένη διαφάνεια στην τιμολόγηση και η ανάγκη επικοινωνίας με πωλήσεις για άδεια χρήσης δυσχεραίνουν την άμεση υιοθέτηση από μικρότερες εταιρείες [31].

3) Osano: Η Λύση "Zero-Fines"

   Η Osano υιοθετεί ένα μοντέλο έμφασης στην απλότητα και τη διαβεβαίωση αποτελέσματος, προβάλλοντας τη δέσμευση "No Fines pledge", δηλαδή κάλυψη προστίμων σε περίπτωση που προκύψουν λόγω αστοχίας του λογισμικού [32].

Ανάλυση: Είναι ιδιαίτερα φιλική προς τον χρήστη και απαιτεί χαμηλές τεχνικές δεξιότητες, με βασική εστίαση σε Consent Management Platform (CMP) και τεχνικούς ελέγχους ιστοσελίδων. Ωστόσο, το λειτουργικό της εύρος είναι περιορισμένο, καθώς δεν υποστηρίζει με βάθος σύνθετες DPIAs, διαθέτει μικρό βαθμό παραμετροποίησης και δεν ενσωματώνει εργαλεία παραγωγής κειμένου (Generative AI) για εξειδικευμένες πολιτικές, γεγονός που μεταφέρει το συγγραφικό βάρος στον χρήστη [33].

4) Cookiebot by Usercentrics

   Το Cookiebot αποτελεί σημείο αναφοράς στον τεχνικό έλεγχο ιστοσελίδων, εστιάζοντας αποκλειστικά στη σάρωση (scanning) και κατηγοριοποίηση cookies, με στόχο τη συμμόρφωση με την Οδηγία ePrivacy [34].

Ανάλυση: Διαθέτει ισχυρή τεχνολογία σάρωσης και μπορεί να εντοπίζει ιχνηλάτες που συχνά παραβλέπονται από άλλα εργαλεία, ενώ η ενσωμάτωση γίνεται με απλό script. Παρά ταύτα, πρόκειται για εργαλείο ειδικού σκοπού (niche tool) που δεν καλύπτει οργανωτικές απαιτήσεις του GDPR (π.χ. ROPA, DPIA). Για πλήρη συμμόρφωση απαιτείται συνδυασμός με επιπλέον λογισμικό, αυξάνοντας το συνολικό κόστος και την πολυπλοκότητα [35].

5) Securiti.ai: Η Προσέγγιση AI-First

   Η Securiti.ai αξιοποιεί μηχανική μάθηση για Data Discovery, σαρώνοντας βάσεις δεδομένων και cloud storage ώστε να εντοπίζει αυτόματα προσωπικά δεδομένα [36].

Ανάλυση: Αυτοματοποιεί τη χαρτογράφηση δεδομένων (Data Mapping) και μειώνει τον χρόνο εντοπισμού ευαίσθητων πληροφοριών, κάτι που είναι κρίσιμο σε περιβάλλοντα Big Data. Ωστόσο, η τεχνολογική της έμφαση αφορά κυρίως την ταξινόμηση (classification) και όχι την παραγωγή νομικού/οργανωτικού κειμένου (generation). Επιπλέον, η καμπύλη εκμάθησης είναι απότομη και απαιτείται τεχνική εξειδίκευση για ενσωμάτωση με τα πληροφοριακά συστήματα του οργανισμού [37].

6) BigID: Η Δύναμη της Ανακάλυψης Δεδομένων

   Η BigID έχει καθιερωθεί στον χώρο της "Data Intelligence", βασιζόμενη σε αλγορίθμους μηχανικής μάθησης που σαρώνουν υποδομές για εντοπισμό δεδομένων [38].

Ανάλυση: Εντοπίζει "σκοτεινά δεδομένα" (dark data) και παράγει χάρτες ροής δεδομένων, ενώ υποστηρίζει Identity Correlation, διευκολύνοντας σημαντικά αιτήματα δικαιωμάτων πρόσβασης (DSARs) [39]. Παράλληλα, απαιτεί σημαντικούς υπολογιστικούς πόρους και πρόσβαση σε ευαίσθητες βάσεις δεδομένων, γεγονός που μπορεί να δημιουργήσει εσωτερικές τριβές με τμήματα InfoSec. Το υψηλό κόστος την καθιστά επιλογή κυρίως για πολύ μεγάλους οργανισμούς (π.χ. Fortune 500) [40].

7) Collibra: Η Προσέγγιση της Διακυβέρνησης

   Η Collibra προσεγγίζει το GDPR μέσα από το πρίσμα του Data Governance, θεωρώντας ότι η συμμόρφωση είναι υποσύνολο της συνολικής ποιότητας και διακυβέρνησης δεδομένων, ενοποιώντας νομικούς κανόνες με επιχειρηματικό λεξικό [41].

Ανάλυση: Παρέχει ισχυρή ιχνηλασιμότητα (data lineage) και διευκολύνει τη συνεργασία μεταξύ νομικών και data engineers, κάτι ιδιαίτερα χρήσιμο σε πολύπλοκες δομές δεδομένων [42]. Ωστόσο, είναι "βαρύ" σύστημα για απλές εργασίες συμμόρφωσης, με απότομη καμπύλη εκμάθησης και ανάγκη αλλαγής οργανωτικής κουλτούρας. Η παραμετροποίηση μπορεί να διαρκέσει μήνες και δεν στοχεύει άμεσα στη σύνταξη πολιτικών για μικρότερους οργανισμούς [43].

8) Vanta: Η Αυτοματοποίηση της Ασφάλειας

   Η Vanta ξεκίνησε ως εργαλείο πιστοποίησης SOC 2 και επεκτάθηκε στο GDPR, με κεντρική φιλοσοφία το continuous monitoring. Συνδέεται με cloud υπηρεσίες (π.χ. AWS, Google Workspace) και ελέγχει ρυθμίσεις ασφαλείας σε πραγματικό χρόνο [44].

Ανάλυση: Αυτοματοποιεί τη συλλογή αποδεικτικών στοιχείων (evidence collection) και μειώνει σημαντικά τον χρόνο προετοιμασίας για audits, ενώ είναι δημοφιλής σε τεχνολογικές startups. Παρότι παρέχει πρότυπα πολιτικών που ενημερώνονται, η εστίασή της παραμένει κυρίως στην τεχνική ασφάλεια. Έτσι, δεν καλύπτει επαρκώς ποιοτικές απαιτήσεις του GDPR, όπως η αξιολόγηση αντικτύπου στα θεμελιώδη δικαιώματα (DPIA), ενώ οι πολιτικές που παράγει είναι συχνά τυποποιημένες και όχι κατάλληλα εξατομικευμένες για σύνθετες επεξεργασίες [45] [31].

Συνολική Αξιολόγηση Διεθνούς Ανταγωνισμού

Η ανάλυση των παραπάνω περιπτώσεων δείχνει ότι η διεθνής αγορά διαθέτει υψηλή ωριμότητα και εξειδικευμένα εργαλεία για επιμέρους διαστάσεις, όπως Data Discovery (BigID), Data Governance (Collibra) και continuous security monitoring (Vanta). Παρά ταύτα, οι πλατφόρμες αυτές έχουν σχεδιαστεί με παραδοχές που ταιριάζουν κυρίως σε οργανισμούς με εξειδικευμένες ομάδες IT και DPO, καθώς και με δυνατότητα απορρόφησης κόστους και πολυπλοκότητας. Ως αποτέλεσμα, δεν απαντούν πλήρως στο πρακτικό πρόβλημα των μικρότερων οργανισμών που χρειάζονται καθημερινή παραγωγή και συντήρηση πολιτικών, διαδικασιών παραβίασης και αναφορών DPIA, με τρόπο οικονομικά προσβάσιμο και λειτουργικά απλό. Επιπλέον, η συχνή εξάρτηση από cloud υποδομές και κλειστά μοντέλα AI εισάγει πρόσθετους προβληματισμούς ως προς ιδιωτικότητα και διαφάνεια όταν εμπλέκονται ευαίσθητα δεδομένα. Συνεπώς, παραμένει ένα εμφανές κενό για μια ολιστική αλλά «ελαφριά» και «έξυπνη» εφαρμογή που θα μπορεί να λειτουργεί τοπικά, να περιορίζει τον κίνδυνο έκθεσης δεδομένων και να παράγει εξατομικευμένο νομικό/οργανωτικό κείμενο χωρίς το κόστος των enterprise λύσεων.[31]

2.4 Ανασκόπηση Πεδίου

Η επιστημονική περιοχή που συνδυάζει τη Νομική Επιστήμη με την Πληροφορική αναφέρεται διεθνώς ως «Υπολογιστική Νομική» (Computational Law). Στο παρόν υποκεφάλαιο παρουσιάζονται, σε γενικό επίπεδο, οι βασικές ερευνητικές τάσεις που έχουν διαμορφωθεί τα τελευταία χρόνια και σχετίζονται με την ψηφιακή υποστήριξη νομικών διαδικασιών και κανονιστικής συμμόρφωσης, με ιδιαίτερη έμφαση στο πεδίο της προστασίας δεδομένων. Η ανάλυση εστιάζει στη σταδιακή μετατόπιση του ενδιαφέροντος από εργαλεία που περιορίζονται στην πρόβλεψη ή αξιολόγηση (π.χ. εκτίμηση κινδύνου, ταξινόμηση, εντοπισμός μη συμμορφώσεων) προς συστήματα που υποστηρίζουν την παραγωγή περιεχομένου και τεκμηρίωσης, όπως η σύνταξη και η επικαιροποίηση πολιτικών απορρήτου. Στόχος είναι να τεθεί το ευρύτερο θεωρητικό και τεχνολογικό πλαίσιο μέσα στο οποίο εντάσσεται η παρούσα διατριβή, και να αναδειχθεί η συμβολή της ως προς την πρακτική αυτοματοποίηση της δημιουργίας κειμένων συμμόρφωσης στον χώρο της ιδιωτικότητας [31].

2.4.1 Από την Πρόβλεψη στην Παραγωγή (Predicive vs Generative AI)

Μέχρι πρόσφατα, σημαντικό μέρος της ακαδημαϊκής έρευνας στον χώρο του Legal Tech εστίαζε κυρίως σε προσεγγίσεις «Προβλεπτικής Ανάλυσης» (Predictive Analytics). Σε αυτό το πλαίσιο, αξιοποιήθηκαν κλασικοί αλγόριθμοι Μηχανικής Μάθησης (Machine Learning), όπως τα SVMs και τα Random Forests, με σκοπό την εξαγωγή προβλέψεων από ιστορικά δεδομένα—για παράδειγμα, την εκτίμηση της πιθανής έκβασης δικαστικών αποφάσεων με βάση προηγούμενες υποθέσεις και μοτίβα επιχειρηματολογίας [46]. Παράλληλα, αναπτύχθηκαν τεχνικές Επεξεργασίας Φυσικής

Γλώσσας (NLP) που στόχευαν στην αυτόματη ανάλυση, οργάνωση και ταξινόμηση νομικών εγγράφων. Ενδεικτικά, μοντέλα όπως το Legal-BERT αξιοποιήθηκαν για εργασίες όπως η αναγνώριση νομικών οντοτήτων (Named Entity Recognition) και η ανίχνευση ρητρών σε συμβάσεις, διευκολύνοντας την αναζήτηση, τη σύγκριση και την επισημείωση κρίσιμων τμημάτων κειμένου [47]. Παρότι οι προσεγγίσεις αυτές συνέβαλαν ουσιαστικά στην αυτοματοποίηση της νομικής ανάλυσης, παρέμεναν κατά βάση «αναλυτικές»: μπορούσαν να επεξεργαστούν και να κατηγοριοποιήσουν υπάρχον κείμενο, αλλά δεν είχαν τη δυνατότητα να παράγουν νέο νομικό περιεχόμενο με συνεκτικό τρόπο.

Η εμφάνιση των Μεγάλων Γλωσσικών Μοντέλων (LLMs), όπως το GPT-3 και το Llama, επέφερε μια σημαντική μετατόπιση στο ερευνητικό ενδιαφέρον, καθώς κατέστη εφικτή η μετάβαση από τη διάγνωση και την ταξινόμηση στη σύνθεση και παραγωγή περιεχομένου. Έτσι, η σύγχρονη έρευνα στον χώρο του Legal Tech στρέφεται ολοένα περισσότερο προς τη «Γενετική Τεχνητή Νοημοσύνη» (Generative AI), εξετάζοντας κατά πόσο τα μοντέλα μπορούν να υποστηρίξουν εργασίες που παραδοσιακά απαιτούσαν ανθρώπινη συγγραφή, όπως η σύνταξη νομικών επιχειρημάτων, η απάντηση σε εξειδικευμένα νομικά ερωτήματα και η παραγωγή προσχεδίων εγγράφων (π.χ. συμβάσεων ή πολιτικών) [3]. Η μετατόπιση αυτή είναι ιδιαίτερα σημαντική για το πεδίο της προστασίας δεδομένων, όπου η συμμόρφωση δεν εξαντλείται στην ανίχνευση αποκλίσεων, αλλά προϋποθέτει τη συνεχή παραγωγή και επικαιροποίηση τεκμηρίωσης, όπως πολιτικές απορρήτου, διαδικασίες και αναφορές που πρέπει να είναι κατανοητές, συνεπείς και προσαρμοσμένες στο εκάστοτε οργανωτικό πλαίσιο

2.4.2 Τεχνητή Νοημοσύνη στην Παραγωγή πολιτικών απορρήτου

Μία σημαντική κατηγορία ερευνών αφορά την αυτοματοποίηση της ανάλυσης πολιτικών απορρήτου ως κειμένων που είναι κρίσιμα για τη διαφάνεια προς τον χρήστη. Εργαλεία όπως το «Polisis» αξιοποιούν τεχνικές βαθιάς μάθησης (Deep Learning) για να «διαβάζουν» πολιτικές απορρήτου, να εξάγουν τη δομή και τα βασικά τους σημεία, και να τα αποδίδουν με πιο κατανοητό και οπτικοποιημένο τρόπο, ώστε οι χρήστες να αντιλαμβάνονται ευκολότερα τι δεδομένα συλλέγονται, για ποιους σκοπούς και με ποιους αποδέκτες ενδέχεται να κοινοποιούνται [48]. Παράλληλα, μια δεύτερη ερευνητική κατεύθυνση σχετίζεται με την ανωνυμοποίηση και τη μείωση του κινδύνου επαναταυτοποίησης, όπου αλγόριθμοι AI χρησιμοποιούνται για τον εντοπισμό προσωπικών δεδομένων μέσα σε μεγάλα σύνολα δεδομένων και για την αφαίρεση ή μετασχηματισμό τους, ώστε να περιορίζεται η έκθεση ευαίσθητης πληροφορίας και να ενισχύεται η ιδιωτικότητα κατά τον χειρισμό δεδομένων σε κλίμακα [49]. Ωστόσο, παρότι η βιβλιογραφία είναι πλούσια σε μεθόδους που αξιολογούν και αναλύουν ήδη υπάρχουσες πολιτικές απορρήτου ή υποστηρίζουν τεχνικές ιδιωτικότητας σε επίπεδο δεδομένων, παρατηρείται συγκριτικά περιορισμένη εστίαση σε προσεγγίσεις που υποστηρίζουν την ίδια τη συγγραφή και την παραγωγή πολιτικών απορρήτου.

Δηλαδή, είναι λίγες οι μελέτες που εξετάζουν πώς ένα σύστημα μπορεί να συλλέξει δομημένα πληροφορίες για μια υπηρεσία (π.χ. τύπους δεδομένων, σκοπούς, αποδέκτες, διάρκεια διατήρησης, δικαιώματα χρηστών) και να συνθέσει αυτόματα ένα συνεκτικό, κατανοητό και προσαρμοσμένο κείμενο πολιτικής απορρήτου· η πλειονότητα των εργασιών παραμένει προσανατολισμένη στον

έλεγχο και την επισημείωση υφιστάμενων κειμένων, και όχι στη δημιουργία νέου περιεχομένου πολιτικής.[49]

2.4.3 Προκλήσεις και περιορισμοί των LLMs στη παραγωγή Νομικού κειμένου

Η ενσωμάτωση των Μεγάλων Γλωσσικών Μοντέλων (LLMs) σε νομικές εφαρμογές και σε διαδικασίες συγγραφής κειμένων δεν είναι απαλλαγμένη από κινδύνους, και η σχετική βιβλιογραφία έχει αναδείξει κρίσιμα ζητήματα αξιοπιστίας και ασφάλειας. Η σημαντικότερη πρόκληση αφορά το φαινόμενο της «παραγωγής ψευδών πληροφοριών» (hallucinations), δηλαδή την παραγωγή περιεχομένου που εμφανίζεται πειστικό, αλλά είναι ουσιαστικά λανθασμένο ή ανύπαρκτο. Στο νομικό πλαίσιο, αυτό μεταφράζεται σε «νομικές παραγωγής ψευδών πληροφοριών», όπου το μοντέλο μπορεί να κατασκευάσει αναφορές σε διατάξεις, νομολογία ή διαδικαστικές απαιτήσεις που δεν υφίστανται. Ενδεικτικά, πρόσφατη μελέτη του Πανεπιστημίου Stanford (2024) κατέδειξε ότι γενικά μοντέλα AI παράγουν εσφαλμένες νομικές πληροφορίες σε ποσοστό που φτάνει το 58% σε συγκεκριμένες δικαιοδοσίες [12]. Ένα τέτοιο ποσοστό καθιστά προβληματική την ανεξέλεγκτη χρήση τους, ιδίως όταν το παραγόμενο κείμενο προορίζεται να λειτουργήσει ως επίσημο ή κανονιστικά κρίσιμο έγγραφο.

Μια δεύτερη, εξίσου σημαντική κατηγορία προκλήσεων αφορά ζητήματα ιδιωτικότητας και ασφάλειας δεδομένων. Η αξιοποίηση cloud-based μοντέλων (όπως το ChatGPT) για την επεξεργασία πληροφοριών οργανισμών ενδέχεται να αυξήσει την επιφάνεια έκθεσης, καθώς τα δεδομένα μεταφέρονται εκτός της εσωτερικής υποδομής και ενδέχεται να εμπλέκονται τρίτα συστήματα ή πάροχοι. Στο πλαίσιο αυτό, η έρευνα γύρω από τα “Privacy-Preserving LLMs” βρίσκεται ακόμη σε εξέλιξη, ενώ η τοπική εκτέλεση (Local Inference) προβάλλεται συχνά ως η ασφαλέστερη επιλογή για ευαίσθητα δεδομένα, παρότι συνοδεύεται από πρακτικούς περιορισμούς, όπως αυξημένες απαιτήσεις σε υπολογιστικούς πόρους και τεχνική πολυπλοκότητα εγκατάστασης/συντήρησης [50]. Η διάσταση αυτή είναι ιδιαίτερα κρίσιμη όταν το ζητούμενο είναι η σύνταξη κειμένων που βασίζονται σε εσωτερικές πληροφορίες (π.χ. διαδικασίες, ροές δεδομένων, ρυθμίσεις συστημάτων), όπου η διαρροή ή η μη εξουσιοδοτημένη πρόσβαση μπορεί να έχει ουσιαστικές συνέπειες.

Συνεπώς, τα LLMs μπορούν να λειτουργήσουν ως ισχυροί «επιταχυντές» στη συγγραφή νομικών κειμένων και ειδικότερα στη δημιουργία πολιτικών απορρήτου, υπό την προϋπόθεση ότι η χρήση τους είναι αυστηρά οριοθετημένη και σχεδιασμένη με επίγνωση των παραπάνω κινδύνων. Η αδυναμία εγγύησης πλήρους νομικής ορθότητας, σε συνδυασμό με τον κίνδυνο παραγωγής ψευδών παραπομπών ή εσφαλμένων συμπερασμάτων, σημαίνει ότι δεν μπορούν να υποκαταστήσουν τον ρόλο του νομικού συμβούλου ή του υπευθύνου που φέρει την τελική ευθύνη για το περιεχόμενο. Αντίθετα, η πιο ρεαλιστική και ασφαλής αξιοποίησή τους είναι ως εργαλεία υποβοήθησης, μέσα σε ένα πλαίσιο αυστηρού ανθρώπινου ελέγχου (human-in-the-loop), όπου ο χρήστης επαληθεύει το περιεχόμενο, διορθώνει ασάφειες και εγκρίνει την τελική έκδοση. Παράλληλα, ο κατάλληλος σχεδιασμός της ροής δεδομένων—με ελαχιστοποίηση των εισροών, σαφή διαχωρισμό ευαίσθητων πληροφοριών και προτίμηση τοπικής εκτέλεσης όπου αυτό είναι εφικτό—μπορεί να μειώσει την πιθανότητα παραγωγής ψευδών πληροφοριών και να ενισχύσει την ασφάλεια, διατηρώντας την ευθύνη και τον έλεγχο σταθερά στον άνθρωπο [12] [50].

2.4.4 Το Ερευνητικό Ερώτημα

Από την επισκόπηση της βιβλιογραφίας προκύπτει ένα σαφές ερευνητικό κενό, το οποίο είναι συνεπές με τα ευρήματα που παρουσιάστηκαν στις προηγούμενες ενότητες για το Legal/Privacy Tech. Συγκεκριμένα, η υφιστάμενη έρευνα και τα διαθέσιμα εργαλεία καλύπτουν επαρκώς την «αναλυτική» διάσταση: υπάρχουν προσεγγίσεις που υποστηρίζουν την ανάλυση και την επισημείωση νομικών κειμένων, καθώς και εργαλεία που ενισχύουν την ιδιωτικότητα μέσω ανωνυμοποίησης ή τεχνικών μείωσης κινδύνου σε επίπεδο δεδομένων. Παράλληλα, η πρόσφατη άνοδος των LLMs έχει καταστήσει εφικτή τη συγγραφή κειμένου σε υψηλή ποιότητα γλώσσας, αλλά η χρήση γενικών μοντέλων συνοδεύεται από τεκμηριωμένα προβλήματα αξιοπιστίας (hallucinations) και από ζητήματα ιδιωτικότητας όταν η εκτέλεση γίνεται σε cloud υποδομές. [50]

Ως αποτέλεσμα, παραμένει ανεπαρκώς καλυμμένο το σημείο τομής ανάμεσα στη δομημένη συλλογή πληροφοριών και στη δημιουργία κειμένων πολιτικής απορρήτου: δεν συναντάται, σε ώριμη μορφή, μια ολοκληρωμένη μεθοδολογία που να συνδυάζει τη συνέπεια και την ακρίβεια που προσφέρει ένα δομημένο ερωτηματολόγιο (structured inputs), με τη δυνατότητα σύνθεσης συνεκτικού κειμένου που παρέχουν τα generative μοντέλα, και ταυτόχρονα να διασφαλίζει την προστασία των εισροών μέσω τοπικής εκτέλεσης (local execution). Η παρούσα διπλωματική εργασία τοποθετείται ακριβώς σε αυτό το κενό και ευθυγραμμίζεται με τα ερευνητικά ερωτήματα του Κεφαλαίου 1, καθώς προτείνει μια υβριδική αρχιτεκτονική που αξιοποιεί τοπικά LLMs (Llama 3) για την παραγωγή κειμένου πολιτικής απορρήτου, αλλά τα καθοδηγεί αυστηρά μέσω δομημένων δεδομένων και ελεγχόμενης παροχής συμφραζομένων (context injection). Με αυτόν τον σχεδιασμό, το σύστημα επιδιώκει να μειώσει τη μεταβλητότητα και τις παραγωγές ψευδών πληροφοριών ώστε να ενισχύσει την επαναληψιμότητα του αποτελέσματος και να διατηρήσει τα δεδομένα του χρήστη εντός της υποδομής του, ώστε η προτεινόμενη λύση να είναι εφαρμόσιμη σε πραγματικά περιβάλλοντα και ιδιαίτερα σε μικρότερους οργανισμούς που χρειάζονται πρακτική υποστήριξη στη συγγραφή και συντήρηση πολιτικών απορρήτου.[50]

2.5 Η χαρτογράφηση του Οργανισμού και η παραγωγή κειμένου μέσα από το Μεγάλο Γλωσσικό Μοντέλο

Το πληροφοριακό σύστημα «GDPR ASSESSOR» σχεδιάστηκε με στόχο να χαρτογραφεί, με λειτουργικό τρόπο, κρίσιμες απαιτήσεις του Κανονισμού μέσω της συμπλήρωσης δομημένων ερωτηματολογίων και της αξιοποίησης των απαντήσεων ως ελεγχόμενων εισροών προς το Μεγάλο Γλωσσικό Μοντέλο. Η βασική λογική είναι ότι ο χρήστης (ή ο αρμόδιος ρόλος, όπως ο DPO) δεν χρειάζεται να συγγράψει από την αρχή το απαιτούμενο περιεχόμενο, αλλά να παρέχει τεκμηριωμένες και συγκεκριμένες πληροφορίες, οι οποίες στη συνέχεια μετατρέπονται σε συνεκτικά παραδοτέα. Στο πλαίσιο αυτό, το σύστημα υποστηρίζει, μεταξύ άλλων, δύο κεντρικές περιοχές απαιτήσεων. Πρώτον, σε σχέση με την Ασφάλεια της Επεξεργασίας (Άρθρο 32), το σύστημα αξιοποιεί τη λογική της Ανάλυσης Κενών (Gap Analysis) για να αποτυπώσει το επίπεδο υιοθέτησης κατάλληλων Τεχνικών και Οργανωτικών Μέτρων (TOMs) με βάση τον κίνδυνο, δίνοντας έμφαση στον εντοπισμό ελλείψεων σε οργανωτικές πολιτικές, σε πρακτικές εκπαίδευσης/ευαισθητοποίησης και σε μηχανισμούς απόκρισης σε περιστατικά παραβίασης. Με αυτόν τον τρόπο, διερευνάται ρητά η ικανότητα του οργανισμού να διασφαλίζει τη διαρκή

εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων επεξεργασίας, όπως προβλέπεται στο Άρθρο 32(1)(β), και τα ευρήματα μετατρέπονται σε στοχευμένες προτάσεις βελτίωσης. Δεύτερον, ως προς τα Δικαιώματα των Υποκειμένων (Άρθρα 12–22), το σύστημα αναγνωρίζει ότι αιτήματα πρόσβασης, διόρθωσης και διαγραφής (DSARs) απαιτούν από έναν οργανισμό να μπορεί να εντοπίζει έγκαιρα ποια δεδομένα συνδέονται με ένα συγκεκριμένο άτομο και πού τηρούνται (identity correlation). [50]

Παρότι η παρούσα έκδοση δεν πραγματοποιεί αυτόματη σάρωση βάσεων δεδομένων, η ακριβής καταγραφή κατηγοριών δεδομένων, σκοπών επεξεργασίας και σχετικών ροών μέσω των ερωτηματολογίων (ιδίως στο πλαίσιο DPIA) παρέχει το αναγκαίο δομημένο υπόβαθρο τεκμηρίωσης που υποστηρίζει τον DPO στη διαχείριση των αιτημάτων και, ταυτόχρονα, δημιουργεί μια σαφή βάση για μελλοντική επέκταση του συστήματος με εργαλεία αυτοματοποιημένου εντοπισμού δεδομένων.[50]

2.6 Παραγωγική Συμμόρφωση και το Ερευνητικό Ερώτημα

Η διεξοδική ανάλυση της αγοράς (Κεφάλαια 2.2 και 2.3) επιβεβαίωσε την ύπαρξη ενός σαφούς κενού που συνδέεται άμεσα με το ερευνητικό πρόβλημα και τα ερευνητικά ερωτήματα του Κεφαλαίου 1. Ενώ το διεθνές οικοσύστημα προσφέρει ώριμες λύσεις για επιμέρους λειτουργίες—όπως Ανακάλυψη Δεδομένων (Data Discovery) (π.χ., BigID) και τεχνική Διαχείριση Συγκατάθεσης/ελέγχους ιστοσελίδων (π.χ., Cookiebot) η πλειονότητα των διαθέσιμων εργαλείων, τόσο διεθνώς όσο και εγχώρια, παραμένει προσανατολισμένη είτε στην καταγραφή και οργάνωση πληροφοριών (record keeping/workflow) είτε στη διάθεση στατικών νομικών προτύπων. Ως αποτέλεσμα, το κρίσιμο «τελευταίο μίλι» της διαδικασίας, δηλαδή η μετατροπή των δομημένων ευρημάτων (τύποι δεδομένων, σκοποί, αποδέκτες, περίοδοι διατήρησης, μέτρα ασφάλειας) σε συνεκτικό και προσαρμοσμένο κείμενο πολιτικής απορρήτου, εξακολουθεί να στηρίζεται σχεδόν αποκλειστικά στη χειροκίνητη εργασία του DPO ή του νομικού συμβούλου.[50]

Το κενό αυτό μπορεί να περιγράφει ως έλλειψη εργαλείων «Παραγωγικής Συμμόρφωσης» (Generative Compliance) με πρακτικό προσανατολισμό στη συγγραφή πολιτικών απορρήτου. Οι υφιστάμενες πλατφόρμες δεν αξιοποιούν συστηματικά την Τεχνητή Νοημοσύνη για να συντάξουν αυτόματα εξατομικευμένο νομικό κείμενο (π.χ., Privacy Policy) με βάση συγκεκριμένα χαρακτηριστικά της εκάστοτε υπηρεσίας/οργανισμού. Αντίθετα, μεταφέρουν το βάρος στον άνθρωπο, ο οποίος καλείται να ερμηνεύσει τις καταγραφές και να παράγει κείμενα που είναι ταυτόχρονα νομικά συνεκτικά, κατανοητά για τον τελικό χρήστη και συνεπή με τις πραγματικές ροές δεδομένων. Αυτή η διαπίστωση ευθυγραμμίζεται με τον πυρήνα των ερευνητικών ερωτημάτων του Κεφαλαίου 1, τα οποία εστιάζουν στο πώς μπορεί να υποστηριχθεί, με αξιόπιστο και ασφαλή τρόπο, η παραγωγή προσαρμοσμένου περιεχομένου πολιτικής απορρήτου από οργανωτικά και τεχνικά δεδομένα που συλλέγονται δομημένα.[50]

Στο πλαίσιο αυτό, η παρούσα εργασία εισάγει μια υβριδική αρχιτεκτονική που συνδυάζει την ακρίβεια των δομημένων ερωτηματολογίων (structured data) με τη συνθετική ικανότητα των Generative AI μοντέλων (Llama 3), ενσωματώνοντας ταυτόχρονα την ασφάλεια της τοπικής εκτέλεσης (local execution). Η επιλογή αυτή απαντά ευθέως στις βασικές προκλήσεις που αναδείχθηκαν στη βιβλιογραφία και στην ανάλυση αγοράς: αφενός, μειώνει την αβεβαιότητα και

τον συγγραφικό φόρτο μέσω αυτοματοποίησης της σύνταξης· αφετέρου, περιορίζει τους κινδύνους που σχετίζονται με cloud-based επεξεργασία ευαίσθητων εισροών, διατηρώντας τα δεδομένα εντός της υποδομής του χρήστη. Επιπλέον, η αυστηρή καθοδήγηση του μοντέλου μέσω ελεγχόμενων εισροών (context injection) λειτουργεί ως μηχανισμός περιορισμού των παραγωγής ψευδών πληροφοριών, ενισχύοντας την επαναληψιμότητα και την τεκμηριωσιμότητα του παραγόμενου κειμένου, σύμφωνα με τον στόχο του Κεφαλαίου 1 για αξιόπιστη παραγωγή περιεχομένου.[50]

Η έννοια της «Παραγωγικής Συμμόρφωσης» (Generative Compliance), όπως ορίζεται στην παρούσα εργασία, αφορά ακριβώς αυτή τη γεφύρωση: τη μετάβαση από εργαλεία που απλώς αποθηκεύουν καταγραφές ή προσφέρουν πρότυπα, σε συστήματα που μετασχηματίζουν δομημένες πληροφορίες σε εξατομικευμένο κείμενο πολιτικής απορρήτου σε σχεδόν πραγματικό χρόνο. Η παραγωγική αυτή διάσταση δεν αναιρεί την ανάγκη ανθρώπινης εποπτείας· αντιθέτως, ευθυγραμμίζεται με τη λογική human-in-the-loop που έχει αναδειχθεί ως απαραίτητη προϋπόθεση για ασφαλή χρήση LLMs. Συνεπώς, ο ρόλος του DPO μετασχηματίζεται από «χειρωνακτικό συντάκτη» σε κριτικό επιβλέποντα και εγκριτή, ο οποίος εστιάζει στην ορθότητα των εισροών, στη συνεκτικότητα του αποτελέσματος και στη διαχείριση των ουσιαστικών κινδύνων, αντί στη μηχανική παραγωγή τυποποιημένων κειμένων. Με αυτόν τον τρόπο, το «GDPR ASSESSOR» προτείνεται ως ένα πρώτο, λειτουργικό παράδειγμα εφαρμογής της έννοιας Generative Compliance σε ένα πρακτικό σενάριο που συνδέεται άμεσα με τα ερευνητικά ερωτήματα και το ερευνητικό κενό που τέθηκαν στο Κεφάλαιο 1.[50]

2.7 Παραγωγική Συμμόρφωση και το Ερευνητικό Ερώτημα

Στο παρόν κεφάλαιο παρουσιάστηκε το θεωρητικό και τεχνολογικό υπόβαθρο της εργασίας, τόσο ως προς το κανονιστικό πλαίσιο του GDPR όσο και ως προς το οικοσύστημα των διαθέσιμων εργαλείων προστασίας δεδομένων και ιδιωτικότητας. Αρχικά, αποσαφηνίστηκαν βασικές έννοιες, όπως η προστασία προσωπικών δεδομένων, η «επεξεργασία» και η Εκτίμηση Αντικτύπου (DPIA), αναδεικνύοντας πώς οι έννοιες αυτές μεταφράζονται σε συγκεκριμένες απαιτήσεις για πληροφοριακά συστήματα και οργανωτικές διαδικασίες. Στη συνέχεια, εξετάστηκαν αντιπροσωπευτικές λύσεις της ελληνικής και διεθνούς αγοράς, με στόχο να αποτυπωθούν τα πλεονεκτήματα και οι περιορισμοί τους από την οπτική της πρακτικής εφαρμογής σε οργανισμούς διαφορετικού μεγέθους και διαφορετικού βαθμού ωριμότητας.[50]

Η ανάλυση κατέδειξε ότι, παρά την ύπαρξη ώριμων πλατφορμών διακυβέρνησης δεδομένων και διαχείρισης κινδύνων, οι περισσότερες λύσεις είτε είναι οικονομικά και τεχνικά δυσπρόσιτες για μικρομεσαίες επιχειρήσεις είτε εστιάζουν κυρίως στην καταγραφή πληροφοριών και στην τεκμηρίωση, χωρίς ουσιαστική υποστήριξη της παραγωγής προσαρμοσμένων κειμένων πολιτικής απορρήτου και συναφών αναφορών. Παράλληλα, η διερεύνηση της χρήσης Μεγάλων Γλωσσικών Μοντέλων στη νομική τεχνολογία ανέδειξε τις δυνατότητες αυτοματοποίησης της συγγραφής, αλλά και σοβαρούς κινδύνους αξιοπιστίας (π.χ. παραγωγές ψευδών πληροφοριών) και κινδύνους ιδιωτικότητας, ιδίως όταν η επεξεργασία γίνεται σε cloud περιβάλλοντα. Τα παραπάνω ευρήματα συγκλίνουν στη διαπίστωση ότι το κρίσιμο «τελευταίο μίλι» —η μετατροπή δομημένων τεχνικών και οργανωτικών πληροφοριών σε συνεκτικό, κατανοητό και εξατομικευμένο κείμενο πολιτικής απορρήτου— παραμένει σε μεγάλο βαθμό χειροκίνητη διαδικασία.[50]

Τα κύρια συμπεράσματα του κεφαλαίου μπορούν να συνοψιστούν ως εξής. Πρώτον, παρατηρείται μια πολωμένη αγορά (market polarization): διεθνώς κυριαρχούν πλατφόρμες enterprise υψηλής πληρότητας που όμως απαιτούν σημαντικούς πόρους και εξειδικευμένη παραμετροποίηση, ενώ εγχώρια συναντώνται κυρίως απλούστερες λύσεις και υπηρεσίες που βασίζονται σε στατικά έγγραφα ή συμβουλευτική υποστήριξη, χωρίς να προσφέρεται μια «ενδιάμεση» κατηγορία λογισμικού που να είναι ταυτόχρονα προσιτή και λειτουργικά ολοκληρωμένη [6]. Δεύτερον, διαπιστώνεται έλλειψη παραγωγικής αξιοποίησης Γενετικής Τεχνητής Νοημοσύνης (generative AI gap): τα περισσότερα εργαλεία λειτουργούν ως μηχανισμοί καταγραφής (record keeping) και διαχείρισης ροών εργασίας, χωρίς δυνατότητα αυτόματης σύνταξης εξατομικευμένου κειμένου πολιτικής απορρήτου, με αποτέλεσμα ο συγγραφικός φόρτος να παραμένει στον άνθρωπο [40]. Τρίτον, αναδεικνύεται το παράδοξο της ιδιωτικότητας (privacy paradox): όπου εμφανίζονται εφαρμογές που «τυλίγουν» cloud-based μοντέλα, η αποστολή δεδομένων εκτός υποδομής δημιουργεί νέους κινδύνους εμπιστευτικότητας, γεγονός που καθιστά την ανάγκη για τοπική επεξεργασία (local processing) κρίσιμη, αλλά όχι πάντα τεχνικά εύκολη σε πρακτικό επίπεδο [11]. Τέταρτον, η συμμόρφωση και η διαχείριση ιδιωτικότητας συχνά είναι αποσπασματική (siloed), καθώς οι οργανισμοί καταφεύγουν σε πολλαπλά εργαλεία για διαφορετικές εργασίες (π.χ. cookies/trackers, τεκμηρίωση, τεχνική ασφάλεια), γεγονός που αυξάνει την πολυπλοκότητα, δημιουργεί ασυνέπειες και δυσχεραίνει τη συνεκτική συντήρηση πολιτικών σε βάθος χρόνου.

2.8 Συμπεράσματα

Στο παρόν κεφάλαιο παρουσιάστηκε το θεωρητικό και τεχνολογικό υπόβαθρο της εργασίας, τόσο ως προς το κανονιστικό πλαίσιο του GDPR όσο και ως προς το οικοσύστημα των διαθέσιμων εργαλείων συμμόρφωσης/ιδιωτικότητας. Αρχικά αποσαφηνίστηκαν οι βασικές έννοιες της προστασίας προσωπικών δεδομένων, της «επεξεργασίας» και της Εκτίμησης Αντικτύπου (DPIA), αναδεικνύοντας πώς οι έννοιες αυτές μεταφράζονται σε λειτουργικές απαιτήσεις για πληροφοριακά συστήματα και για τη σχετική τεκμηρίωση (π.χ. καταγραφή ροών, σκοπών, κατηγοριών δεδομένων και μέτρων). Στη συνέχεια εξετάστηκαν αντιπροσωπευτικές λύσεις της ελληνικής και διεθνούς αγοράς, ώστε να αποτυπωθούν συστηματικά τα πλεονεκτήματα και οι περιορισμοί τους από την οπτική της πρακτικής εφαρμογής σε οργανισμούς διαφορετικού μεγέθους.[11]

Η ανάλυση κατέδειξε ότι, παρότι υπάρχουν ώριμες πλατφόρμες διακυβέρνησης δεδομένων και διαχείρισης κινδύνων, οι περισσότερες λύσεις είτε είναι οικονομικά και τεχνικά απρόσιτες για μικρομεσαίες επιχειρήσεις είτε εστιάζουν κυρίως στην καταγραφή πληροφοριών και όχι στην παραγωγική υποστήριξη της συγγραφής πολιτικών και αναφορών. Παράλληλα, η διερεύνηση της χρήσης Μεγάλων Γλωσσικών Μοντέλων στη νομική τεχνολογία ανέδειξε τη διττή τους φύση: από τη μία πλευρά προσφέρουν ισχυρές δυνατότητες αυτοματοποίησης της συγγραφής, από την άλλη όμως συνοδεύονται από κινδύνους αξιοπιστίας (παραγωγές ψευδών πληροφοριών/ψευδείς αναφορές) και κινδύνους ιδιωτικότητας, ιδιαίτερα όταν χρησιμοποιούνται cloud-based λύσεις. Τα ευρήματα αυτά συνδέονται άμεσα με το ερευνητικό πρόβλημα του Κεφαλαίου 1, όπου το ζητούμενο δεν είναι μόνο «να υπάρχει εργαλείο», αλλά να υπάρχει αξιόπιστη και ασφαλής μεθοδολογία παραγωγής προσαρμοσμένου περιεχομένου (ιδίως πολιτικής απορρήτου) από δομημένα δεδομένα οργανισμού.[11]

Πίνακας1: Συγκριτικός Πίνακας μεταξύ πλατφορμών Διακυβέρνησης Δεδομένων

Χαρακτηριστικό	**Enterprise GRC (π.χ. OneTrust)**	**Niche Tools (π.χ. Cookiebot)**	**Ελληνικές Λύσεις / Συμβουλευτική**	**Σύστημα (GDPR Assesor)**
Κόστος Κτήσης	Πολύ Υψηλό (>10k€/έτος)	Μεσαίο	Υψηλό	Χαμηλό / Open Source
Ευκολία Χρήσης	Χαμηλή (Απαιτεί εκπαίδευση)	Υψηλό	Μεσαία	Υψηλή (Wizard-based)
Παραγωγή Κειμένου (GenAI)	Όχι (Χρήση Προτύπων)	Όχι	Όχι (Χειροκίνητη)	Ναι (Llama 3 / Local)
Τεχνικοί Έλεγχοι (Audit)	Ναι (Modules)	Ναι	Όχι	Ναι (Cookie/Tracker Scan)
Ιδιωτικότητα Δεδομένων	Cloud (SaaS)	Cloud (SaaS)	Cloud/Local	Αυστηρά Τοπική (On-premise)
Προσαρμοστικότητα	Υψηλή	Χαμηλή	Υψηλή	Υψηλή (Context-aware)

Τα κυριότερα ευρήματα συνοψίζονται στα εξής, σε αντιστοίχιση με το ερευνητικό κενό και τα ερευνητικά ερωτήματα του Κεφαλαίου 1. Πρώτον, παρατηρείται πολωμένη αγορά (market polarization): διεθνώς κυριαρχούν πλατφόρμες «μαμούθ» (π.χ. OneTrust, TrustArc) που παρέχουν βάθος λειτουργιών αλλά απαιτούν σημαντικούς πόρους, ενώ στο ελληνικό περιβάλλον κυριαρχούν στατικά έγγραφα και συμβουλευτικές υπηρεσίες, με απουσία μιας «ενδιάμεσης» λύσης λογισμικού που να είναι ταυτόχρονα προσιτή και ολοκληρωμένη [6]. Δεύτερον, διαπιστώνεται έλλειψη ουσιαστικής παραγωγικής αξιοποίησης Γενετικής ΤΝ (generative AI gap): τα περισσότερα εργαλεία λειτουργούν ως record keeping (βάσεις καταγραφής), χωρίς δυνατότητα αυτόματης σύνταξης προσαρμοσμένων κειμένων πολιτικής απορρήτου, γεγονός που αφήνει τον DPO/νομικό να μεταφράζει χειροκίνητα τα ευρήματα σε συνεκτικό νομικό κείμενο [40]. Τρίτον, αναδεικνύεται το παράδοξο της ιδιωτικότητας (privacy paradox): όταν χρησιμοποιούνται AI-εργαλεία που βασίζονται σε cloud, απαιτείται αποστολή δεδομένων εκτός υποδομής, κάτι που δημιουργεί νέους κινδύνους εμπιστευτικότητας και ενισχύει την ανάγκη για τοπική επεξεργασία (local processing) ως αρχιτεκτονική προϋπόθεση ασφαλούς χρήσης [11]. Τέταρτον, η συμμόρφωση παραμένει αποσπασματική (siloed compliance), καθώς οι οργανισμοί αναγκάζονται να χρησιμοποιούν διαφορετικά εργαλεία για διαφορετικές εργασίες (π.χ. cookies/trackers, έγγραφα, τεχνική ασφάλεια), χωρίς ενιαία πλατφόρμα που να ενοποιεί ροές δεδομένων και παραδοτέα.

Μέσα από αυτή τη χαρτογράφηση τεκμηριώθηκε ένα σαφές ερευνητικό κενό, το οποίο συνδέεται άμεσα με τα ερευνητικά ερωτήματα του Κεφαλαίου 1: απουσιάζει μια ολοκληρωμένη

και οικονομικά προσιτή λύση που να συνδυάζει (α) δομημένα ερωτηματολόγια DPIA/Gap Analysis, (β) βασικούς τεχνικούς ελέγχους ιστοσελίδας και (γ) παραγωγή κειμένου πολιτικής απορρήτου μέσω τοπικών LLMs, υπό καθεστώς ανθρώπινης εποπτείας (human-in-the-loop). Το κενό αυτό δεν είναι μόνο τεχνολογικό, αλλά μεθοδολογικό: αφορά το πώς ενοποιούνται οι δομημένες εισροές, τα τεχνικά ευρήματα και η παραγωγή κειμένου με τρόπο αξιόπιστο, επαναλήψιμο και ασφαλή—δηλαδή ακριβώς τα σημεία που διερευνώνται από τα ερευνητικά ερωτήματα (σχεδιασμός συστήματος, αρχιτεκτονική επιλογή, ενσωμάτωση LLMs, καταλληλότητα/προσιτότητα για ΜΜΕ).[11]

Για την καλύτερη κατανόηση του κενού που έρχεται να καλύψει η παρούσα διατριβή, παρατίθεται συγκριτικός πίνακας (Πίνακας 1) που αντιπαραβάλλει τις βασικές κατηγορίες λύσεων της αγοράς με το σύστημα που αναπτύχθηκε στο πλαίσιο της εργασίας. Η αντιπαραβολή αυτή λειτουργεί ως γέφυρα προς τη μεθοδολογία του επόμενου κεφαλαίου, καθώς αιτιολογεί γιατί οι επιλογές που θα παρουσιαστούν (schema-driven ανάπτυξη, modular αρχιτεκτονική, τοπική εκτέλεση LLM και ελεγχόμενη παραγωγή κειμένου) δεν αποτελούν απλώς τεχνικές προτιμήσεις, αλλά απαντήσεις σε συγκεκριμένα κενά που αναδείχθηκαν εμπειρικά από την αγορά και τη βιβλιογραφία.[11]

Συμπερασματικά, η ανάλυση του τρέχοντος επιπέδου καταδεικνύει ότι δεν υπάρχει σήμερα στην αγορά—και ειδικότερα στην ελληνική—ένα εργαλείο που να συνδυάζει την οικονομική προσιτότητα με την ασφαλή, τοπική αξιοποίηση LLMs για την αυτόματη παραγωγή πολιτικών, μαζί με τεχνικούς ελέγχους και δομημένη τεκμηρίωση. Η ανάπτυξη ενός συστήματος που εκτελείται τοπικά, πραγματοποιεί τεχνικό έλεγχο ιστοσελίδας και συντάσσει προσχέδια πολιτικής με ανθρώπινη έγκριση συνιστά τόσο ερευνητική καινοτομία όσο και πρακτική απάντηση σε υπαρκτή ανάγκη. Στο επόμενο κεφάλαιο παρουσιάζεται η μεθοδολογία που ακολουθήθηκε για να δομηθεί, να υλοποιηθεί και να αξιολογηθεί το πληροφοριακό σύστημα «GDPR ASSESSOR», με τρόπο που να επιτρέπει την εμπειρική διερεύνηση των παραπάνω ερευνητικών ερωτημάτων.

3 *Μεθοδολογία*

Στο παρόν κεφάλαιο περιγράφεται η μεθοδολογική προσέγγιση που ακολουθήθηκε για τον σχεδιασμό, την υλοποίηση και την αρχική αξιολόγηση του συστήματος «GDPR ASSESSOR». Η μεθοδολογία δεν αντιμετωπίζεται ως μια στενά τεχνική περιγραφή, αλλά ως δομημένο πλαίσιο που συνδέει άμεσα τα θεωρητικά συμπεράσματα των προηγούμενων κεφαλαίων με τις σχεδιαστικές αποφάσεις και τις πρακτικές επιλογές υλοποίησης. Με δεδομένο ότι στα Κεφάλαια 2.1–2.3 αποσαφηνίστηκαν (α) οι κρίσιμες έννοιες του κανονιστικού πλαισίου (π.χ. επεξεργασία, λογοδοσία, DPIA, μέτρα ασφάλειας), (β) οι ανάγκες τεκμηρίωσης και παραγωγής πολιτικών απορρήτου, (γ) το κενό της «Παραγωγικής Συμμόρφωσης» (Generative Compliance) και (δ) οι περιορισμοί των LLMs (παραγωγές ψευδών πληροφοριών , κίνδυνοι cloud), το παρόν κεφάλαιο εξηγεί πώς τα παραπάνω μετασχηματίστηκαν σε συγκεκριμένες μεθοδολογικές αρχές: τοπική εκτέλεση (local execution) για μείωση κινδύνων ιδιωτικότητας, αυστηρή καθοδήγηση του μοντέλου μέσω δομημένων εισροών για περιορισμό παραγωγής ψευδών πληροφοριών , και ενοποίηση τεχνικών ελέγχων ιστοσελίδας με τη διαδικασία συγγραφής πολιτικής απορρήτου ώστε να αντιμετωπιστεί η αποσπασματικότητα (siloed compliance) που εντοπίστηκε στην ανάλυση αγοράς.[11]

Η ανάπτυξη του «GDPR ASSESSOR» βασίστηκε σε μια αυστηρή προσέγγιση Μηχανικής Λογισμικού, υιοθετώντας τις αρχές της Αρθρωτής Ανάπτυξης (Modular Design) και της Επιστήμης Σχεδιασμού (Design Science Research) με στόχο την παραγωγή λειτουργικού τεχνουργήματος που απαντά σε σαφώς ορισμένο πρόβλημα. Στην πράξη, αυτό σημαίνει ότι η μεθοδολογία οργανώθηκε γύρω από δύο κεντρικές επιδιώξεις: αφενός, την αποσύνδεση των δεδομένων (data) από τη λογική επεξεργασίας (logic), ώστε το σύστημα να είναι ευέλικτο, επεκτάσιμο και ελέγξιμο, και αφετέρου, την επαληθευσιμότητα των αποτελεσμάτων μέσω αυτοματοποιημένων ελέγχων (unit testing) και επαναλήψιμων σεναρίων αξιολόγησης. Η επιλογή αυτή ευθυγραμμίζεται με το ερευνητικό κενό που αναδείχθηκε στα προηγούμενα κεφάλαια: ένα σύστημα που παράγει κείμενο πολιτικής απορρήτου δεν αρκεί να «λειτουργεί», αλλά πρέπει να παρέχει σταθερή συμπεριφορά, ελεγχόμενες εισροές και δυνατότητα τεκμηριωμένης αναπαραγωγής των αποτελεσμάτων.[11]

Με βάση τα παραπάνω, η υλοποίηση ακολούθησε αρχές αρχιτεκτονικής «βάσει σχήματος» (schema-driven development), όπου η δομή των ερωτηματολογίων, των πεδίων τεκμηρίωσης και των παραγόμενων εξόδων ορίζεται σε σχήματα (schemas) και όχι σε σκληρά ενσωματωμένο κώδικα. Η προσέγγιση αυτή επιτρέπει, αφενός, να διατηρείται συνέπεια μεταξύ των εννοιών που προκύπτουν από το GDPR (π.χ. κατηγορίες δεδομένων, σκοποί επεξεργασίας, αποδέκτες, μέτρα ασφάλειας) και των πεδίων που συμπληρώνει ο χρήστης, και αφετέρου, να τροφοδοτείται το LLM με ελεγχόμενο «πλαίσιο» (context injection) που περιορίζει την ασάφεια και μειώνει την πιθανότητα παραγωγής ψευδών πληροφοριών. Παράλληλα, ως μεθοδολογική συνέπεια των κινδύνων που εντοπίστηκαν στη βιβλιογραφία, το μοντέλο ΤΝ εκτελείται τοπικά (local inference),

ώστε τα δεδομένα που σχετίζονται με την πολιτική απορρήτου και τις αξιολογήσεις να μην αποστέλλονται σε cloud περιβάλλοντα.[11]

Σε επίπεδο συστημικής οργάνωσης, το «GDPR ASSESSOR» διασπάστηκε σε επιμέρους υποσυστήματα, καθένα από τα οποία αντιστοιχεί σε μια διακριτή ανάγκη που αναδείχθηκε στη θεωρητική και αγοραστική επισκόπηση: (i) το Assessment Engine, που υλοποιεί τη δομημένη συλλογή πληροφοριών και την αποτύπωση ευρημάτων (π.χ. μέσω DPIA/Gap Analysis), (ii) το Site Inspector, που ενσωματώνει τεχνικούς ελέγχους ιστοσελίδας (π.χ. εντοπισμό cookies/trackers) ώστε να αντιμετωπίζεται η έλλειψη τεχνικού ελέγχου στα απλούστερα εργαλεία και να μειώνεται η εξάρτηση από «σιλό» εφαρμογές, και (iii) το Policy Engine, που αξιοποιεί τις δομημένες εισροές και τα τεχνικά ευρήματα για να παράγει προσχέδια πολιτικής απορρήτου με συνεκτικό τρόπο. Η διάσπαση αυτή δεν είναι μόνο τεχνική επιλογή, αλλά μεθοδολογικό μέσο για να μπορεί να εξεταστεί χωριστά η συμβολή κάθε υποσυστήματος στα ερευνητικά ερωτήματα του Κεφαλαίου 1, όπως η καταλληλότητα της αρχιτεκτονικής, η μείωση φόρτου συγγραφής, η ασφάλεια της επεξεργασίας, και η χρησιμότητα για μικρότερους οργανισμούς.[11]

Τέλος, η στρατηγική επαλήθευσης της ορθής λειτουργίας σχεδιάστηκε ώστε να καλύπτει τόσο τη σταθερότητα του λογισμικού όσο και την αξιοπιστία της παραγωγής κειμένου. Στο τεχνικό επίπεδο, εφαρμόστηκαν αυτοματοποιημένοι έλεγχοι (unit tests) για βασικές λειτουργίες, όπως η εγκυρότητα των σχημάτων, η ορθότητα μετασχηματισμών δεδομένων και η συνέπεια εξαγωγής αποτελεσμάτων. Σε επίπεδο λειτουργικής αξιολόγησης, εξετάστηκε η ικανότητα του συστήματος να παράγει συνεκτικά κείμενα πολιτικής απορρήτου από επαναλήψιμες εισροές, να ενσωματώνει τεχνικά ευρήματα (π.χ. cookies/trackers) και να διατηρεί ελεγχόμενη συμπεριφορά μέσω του schema-driven πλαισίου. Με αυτόν τον τρόπο, η μεθοδολογία δεν περιορίζεται στην περιγραφή του «πώς υλοποιήθηκε» το σύστημα, αλλά τεκμηριώνει «γιατί» οι συγκεκριμένες επιλογές ήταν αναγκαίες με βάση τα κενά, τους κινδύνους και τις απαιτήσεις που αναδείχθηκαν στα προηγούμενα κεφάλαια, επιτρέποντας τη συστηματική διερεύνηση και εμπειρική απάντηση των ερευνητικών ερωτημάτων του Κεφαλαίου 1.[11]

3.1 Στρατηγική Σχεδιασμού: Schema-Driven Development

Κεντρικός άξονας της μεθοδολογίας αποτέλεσε η απόφαση η νομική γνώση του συστήματος—δηλαδή οι ερωτήσεις, οι κατηγορίες πεδίων και οι σχετικές κανονιστικές παραπομπές—να μην ενσωματωθεί «σκληρά» μέσα στον πηγαίο κώδικα της εφαρμογής (hard-coded), αλλά να διατηρηθεί σε εξωτερικά, δομημένα αρχεία. Η προσέγγιση αυτή, γνωστή ως Schema-Driven Development, υλοποιήθηκε μέσω της δημιουργίας αρχείων JSON (dpia.json, gap.json), τα οποία λειτουργούν ως «προσχέδια» (blueprints) που καθορίζουν τη δομή και τη ροή των ερωτηματολογίων, καθώς και τον τρόπο με τον οποίο οι απαντήσεις οργανώνονται σε συνεκτικά δεδομένα εισόδου για τα επόμενα στάδια του συστήματος. Με τον τρόπο αυτό, ο κώδικας (π.χ. app.py) παραμένει γενικού σκοπού και εκτελεί την ίδια λογική ανεξάρτητα από το περιεχόμενο των ερωτήσεων, ενώ το περιεχόμενο και η κανονιστική «γνώση» εκφράζονται σε σχήματα που μπορούν να εξελίσσονται.[11]

Η επιλογή αυτή εξυπηρετεί άμεσα τους μεθοδολογικούς στόχους της εργασίας και συνδέεται με τα ερευνητικά ερωτήματα του Κεφαλαίου 1.

1) **Επιτρέπει δυναμική προσαρμογή:** τα ερωτηματολόγια μπορούν να τροποποιηθούν, να επεκταθούν ή να αναδιαρθρωθούν χωρίς αλλαγές στον πηγαίο κώδικα, γεγονός που ενισχύει την επεκτασιμότητα και τη μακροχρόνια βιωσιμότητα του συστήματος, ιδίως σε ένα ρυθμιστικό περιβάλλον που μεταβάλλεται.
2) **Ενισχύει τη διαλειτουργικότητα και την ιχνηλασιμότητα** μεταξύ νομικών απαιτήσεων και τεχνικής υλοποίησης, καθώς τα σχήματα δεδομένων σχεδιάστηκαν ώστε να φέρουν μεταδεδομένα (metadata) που συνδέουν τα πεδία με τη νομική τους βάση—ενδεικτικά, παραπομπές σε άρθρα του GDPR μέσω κατάλληλων πεδίων (π.χ. gdpr_refs στο gdpr_wizard.py). Αυτή η σύνδεση δεν έχει μόνο τεκμηριωτικό χαρακτήρα, αλλά λειτουργεί και ως μηχανισμός ελέγχου συνέπειας: επιτρέπει να τεκμηριώνεται γιατί συλλέγεται κάθε πληροφορία και πώς αυτή αξιοποιείται στην παραγωγή παραδοτέων, όπως η πολιτική απορρήτου.[11]

Συνολικά, στο παρόν κεφάλαιο παρουσιάζεται η μεθοδολογική προσέγγιση που ακολουθήθηκε για τον σχεδιασμό, την υλοποίηση και την αρχική αξιολόγηση του «GDPR ASSESSOR», με τρόπο που να υπερβαίνει μια απλή τεχνική περιγραφή και να επιτρέπει τη συστηματική διερεύνηση των ερευνητικών ερωτημάτων του Κεφαλαίου 1. Ειδικότερα, περιγράφονται οι αρχές της αρχιτεκτονικής βάσει σχήματος (schema-driven development), η διάσπαση του συστήματος σε επιμέρους υποσυστήματα (Assessment Engine, Site Inspector, Policy Engine) και η στρατηγική επαλήθευσης της ορθής λειτουργίας μέσω αυτοματοποιημένων ελέγχων. Μέσα από αυτή τη δομημένη επιλογή, η μεθοδολογία συνδέει τις θεωρητικές και κανονιστικές παραδοχές των προηγούμενων κεφαλαίων με πρακτικές αποφάσεις σχεδιασμού, επιτρέποντας να αξιολογηθεί εμπειρικά αν και σε ποιο βαθμό το σύστημα μπορεί να υποστηρίξει την παραγωγή αξιόπιστων και ασφαλών παραδοτέων στον χώρο της ιδιωτικότητας.[11]

3.2 Διαδικασία Υλοποίησης Υποσυστημάτων

Η ανάπτυξη της πλατφόρμας πραγματοποιήθηκε σε διακριτές φάσεις, καθεμία από τις οποίες εστίασε σε ένα σαφώς οριοθετημένο υποσύστημα (module), ακολουθώντας την αρχή του Separation of Concerns. Η επιλογή αυτή δεν ήταν μόνο τεχνική, αλλά και μεθοδολογική: επέτρεψε να υλοποιηθούν και να ελεγχθούν ανεξάρτητα οι κρίσιμες λειτουργίες του συστήματος, να μειωθεί η πολυπλοκότητα κατά την ολοκλήρωση, και να διασφαλιστεί ότι κάθε μέρος συνεισφέρει με διαφανή τρόπο στους στόχους της εργασίας, όπως αυτοί προκύπτουν από το θεωρητικό υπόβαθρο και το ερευνητικό κενό των προηγούμενων κεφαλαίων.

3.2.1 Μηχανισμός Αξιολόγησης (Assessment Engine)

Το πρώτο στάδιο αφορούσε την υλοποίηση της λογικής πίσω από τα δομημένα ερωτηματολόγια και τη μετατροπή των απαντήσεων του χρήστη σε συνεκτικά, μετρήσιμα αποτελέσματα. Στο πλαίσιο αυτό αναπτύχθηκε η κλάση AssessmentBuilder (στο αρχείο gdpr_wizard.py), η οποία «διαβάζει» τις απαντήσεις και εκτελεί προκαθορισμένους μετασχηματισμούς και κανόνες αξιολόγησης. Με βάση αυτή τη διαδικασία, το σύστημα υπολογίζει αυτόματα ποσοστά ανά θεματική ενότητα (section scores), εντοπίζει κενά κάλυψης (coverage gaps) σύμφωνα με συγκεκριμένες λογικές συνθήκες, και επισημαίνει δείκτες υψηλού κινδύνου (high risk indicators). Μεθοδολογικά, η φάση αυτή υπηρετεί την ανάγκη που αναδείχθηκε στη βιβλιογραφία: να υπάρχει

ένας μηχανισμός που μετατρέπει «άτυπες» πληροφορίες σε δομημένο πλαίσιο, μειώνοντας την αβεβαιότητα και δημιουργώντας σταθερές, ελέγξιμες εισροές για τα επόμενα στάδια, ιδίως για τη συγγραφή κειμένων πολιτικής απορρήτου.[11]

3.2.2 Τεχνικός Έλεγχος (Audit Module)

Στο δεύτερο στάδιο αναπτύχθηκε το υποσύστημα τεχνικού ελέγχου ιστοσελίδας (cookie_audit.py και site_inspector.py), με στόχο να ενσωματωθεί στη ροή εργασίας ένας πρακτικός έλεγχος που απαντά στο πρόβλημα της αποσπασματικότητας (siloed tools) που εντοπίστηκε στην ανάλυση αγοράς. Η μεθοδολογία εδώ βασίστηκε σε τεχνικές web scraping, με έναν αλγόριθμο που προσομοιώνει τη συμπεριφορά επισκέπτη ιστοσελίδας, καταγράφει τα cookies που αποθηκεύονται στον browser και τα αντιπαραβάλλει με λίστες γνωστών ιχνηλατών (trackers). Στη συνέχεια, τα ευρήματα κατηγοριοποιούνται αυτόματα (π.χ. «Απαραίτητα» ή «Marketing»), ώστε να παράγεται μια πιο αντικειμενική τεχνική εικόνα που μπορεί να τροφοδοτήσει, με τεκμηριωμένο τρόπο, τα τμήματα της πολιτικής απορρήτου που αφορούν τεχνολογίες παρακολούθησης και συναφείς πρακτικές διαφάνειας. Με αυτόν τον σχεδιασμό, το σύστημα δεν περιορίζεται στην υποκειμενική δήλωση του χρήστη, αλλά ενσωματώνει ένα ελάχιστο επίπεδο τεχνικής επαλήθευσης.[11]

3.2.3 Μηχανή Παραγωγής Πολιτικών (Policy Engine)

Το τελικό στάδιο αφορούσε τη διασύνδεση με το Γλωσσικό Μοντέλο και τη μετατροπή των δομημένων εισροών σε συνεκτικό κείμενο πολιτικής απορρήτου. Η μεθοδολογική επιλογή εδώ δεν ήταν η «ελεύθερη συνομιλία» με ένα μοντέλο, αλλά μια ελεγχόμενη διαδικασία Μηχανικής Εντολών (prompt engineering), ώστε να περιοριστούν οι πιθανότητες παραγωγής ψευδών πληροφοριών και να αυξηθεί η επαναληψιμότητα του αποτελέσματος, όπως προέκυψε από τη σχετική βιβλιογραφία. Συγκεκριμένα, σχεδιάστηκαν πρότυπα (templates) στον φάκελο prompts/ που καθορίζουν ρόλο, ύφος και περιορισμούς (π.χ. «Είσαι ειδικός σύμβουλος GDPR»), ενώ το μοντέλο τροφοδοτείται αποκλειστικά με τα δεδομένα που παρήχθησαν στις προηγούμενες φάσεις μέσω ελεγχόμενης έγχυσης συμφραζομένων (context.py). Η υλοποίηση υποστηρίζεται από το llm.py και βασίζεται σε τοπική εκτέλεση του Llama 3, ώστε να περιορίζονται οι κίνδυνοι που συνδέονται με cloud-based επεξεργασία ευαίσθητων πληροφοριών και να διασφαλίζεται ότι οι εισροές δεν εγκαταλείπουν την υποδομή του χρήστη.[11]

Η διάσπαση του συστήματος σε τρία βασικά υποσυστήματα επιτρέπει τη σαφή αντιστοίχιση της υλοποίησης με τα ερευνητικά ερωτήματα του Κεφαλαίου 1. Το Assessment Engine απαντά στον πυρήνα του ερωτήματος που αφορά τη δομημένη καθοδήγηση και τη συστηματική συλλογή/οργάνωση πληροφοριών (μέσω DPIA/Gap Analysis), καθώς υλοποιεί έναν επαναλήψιμο μηχανισμό μετασχηματισμού απαντήσεων σε αξιολογήσεις και ευρήματα. Το Policy Engine αντιστοιχεί στο ερώτημα που αφορά την ενσωμάτωση ενός LLM για παραγωγή κειμένου πολιτικής απορρήτου με ελεγχόμενες εισροές και τοπική εκτέλεση, διερευνώντας στην πράξη πώς μπορούν να συνδυαστούν generative δυνατότητες με περιορισμούς αξιοπιστίας και ιδιωτικότητας. Τέλος, η συνολική αρθρωτή οργάνωση, η χρήση JSON σχημάτων και η διαχείριση κατάστασης με δομημένο τρόπο συνδέονται με το ερώτημα που αφορά τις κατάλληλες αρχιτεκτονικές επιλογές για επεκτασιμότητα και συντηρησιμότητα σε μια λύση RegTech/Privacy Tech, καθώς καθιστούν το

σύστημα προσαρμόσιμο, ελέγξιμο και ευκολότερο στην εξέλιξη χωρίς εκτεταμένες αλλαγές στον πυρήνα του κώδικα.[11]

3.3 Επαλήθευση και Έλεγχος Λογισμικού

Αντί να βασιστεί κυρίως σε υποθετικά σενάρια χρήσης, η εγκυρότητα και η αξιοπιστία του συστήματος τεκμηριώθηκαν με συστηματικό τρόπο μέσω τεχνικών ελέγχων ορθότητας (unit testing), ώστε η αξιολόγηση να είναι επαναλήψιμη και άμεσα συνδεδεμένη με το ερευνητικό κενό και τα ερευνητικά ερωτήματα του Κεφαλαίου 1. Όπως αποτυπώνεται στη δομή του κώδικα (φάκελος tests/), αναπτύχθηκε μια οργανωμένη σουίτα αυτοματοποιημένων δοκιμών με χρήση της βιβλιοθήκης pytest. Η μεθοδολογική επιλογή των tests ανταποκρίνεται στο βασικό πρόβλημα που αναδείχθηκε στη βιβλιογραφία: ενώ τα LLMs μπορούν να επιταχύνουν τη συγγραφή, η αξιοπιστία τους (π.χ. παραγωγή ψευδών πληροφοριών) και η ανάγκη ασφαλούς διαχείρισης εισροών καθιστούν απαραίτητη μια αρχιτεκτονική με ελεγχόμενη συμπεριφορά. Συνεπώς, οι αυτοματοποιημένοι έλεγχοι λειτουργούν ως μηχανισμός που αποδεικνύει ότι το προτεινόμενο σύστημα μπορεί να μετασχηματίζει δομημένες εισροές σε σταθερά και ελέγξιμα αποτελέσματα, ενισχύοντας το επιχείρημα ότι μια λύση «Παραγωγικής Συμμόρφωσης»/παραγωγής πολιτικής απορρήτου μπορεί να είναι πρακτικά αξιόπιστη.[11]

Σε επίπεδο επικύρωσης εισόδων, ο Validation Testing (π.χ. test_validators.py) επιβεβαιώνει ότι το σύστημα απορρίπτει ελλιπή ή λανθασμένα δεδομένα πριν αυτά περάσουν στη φάση επεξεργασίας. Αυτό συνδέεται άμεσα με το πρώτο ερευνητικό ερώτημα του Κεφαλαίου 1, καθώς η δυνατότητα ενός «βήμα-προς-βήμα» μηχανισμού καθοδήγησης προϋποθέτει ότι οι απαντήσεις που συλλέγονται είναι συνεπείς και επαρκείς ώστε να μπορούν να αξιοποιηθούν στην παραγωγή κειμένου πολιτικής απορρήτου. Σε επίπεδο λογικής και ποιότητας του πλαισίου που τροφοδοτεί το μοντέλο, ο Logic Testing (π.χ. test_context.py) επαληθεύει ότι τα δεδομένα που αποστέλλονται στο LLM είναι σωστά δομημένα, αντιστοιχισμένα στα κατάλληλα πεδία και δεν περιέχουν «θόρυβο». Η διάσταση αυτή απαντά στο δεύτερο ερευνητικό ερώτημα, καθώς εξετάζει εμπειρικά την κεντρική υπόθεση της εργασίας: ότι η αυστηρή καθοδήγηση του LLM μέσω δομημένων δεδομένων (schema/context injection) μπορεί να περιορίσει την ασάφεια και να μειώσει την πιθανότητα παραγωγής ψευδών πληροφοριών στην παραγωγή πολιτικής απορρήτου. Παράλληλα, η Noise Reduction ελέγχει ότι αφαιρούνται κενά πεδία και άσχετα μεταδεδομένα από τα prompts, κάτι που δεν λειτουργεί μόνο ως βελτιστοποίηση ποιότητας, αλλά και ως πρακτική εφαρμογή ελαχιστοποίησης εισροών: μειώνει την περιττή επεξεργασία προσωπικών δεδομένων και ενισχύει την αρχή της ιδιωτικότητας-by-design σε επίπεδο ροής δεδομένων. Τέλος, ο Integration Testing (π.χ. test_official_policy.py) επιβεβαιώνει ότι η αλληλουχία των βημάτων—από τη συμπλήρωση φόρμας και τον μετασχηματισμό σε δομημένο context έως την παραγωγή και εξαγωγή του τελικού παραδοτέου (π.χ. PDF)—εκτελείται απρόσκοπτα, τεκμηριώνοντας ότι η αρθρωτή αρχιτεκτονική (modular design) δεν είναι θεωρητική, αλλά παράγει μια συνεκτική end-to-end ροή.[11]

Με αυτόν τον σχεδιασμό, η στρατηγική επαλήθευσης μέσω αυτοματοποιημένων ελέγχων δεν τεκμηριώνει μόνο την τεχνική ορθότητα, αλλά συνδέεται ρητά με το ερευνητικό κενό που αναδείχθηκε στα προηγούμενα κεφάλαια: την απουσία μιας ενοποιημένης, «ελαφριάς» και αξιόπιστης λύσης που να συνδυάζει δομημένη συλλογή πληροφοριών, τεχνική επαλήθευση και παραγωγή πολιτικής απορρήτου με ασφαλή τρόπο. Επιπλέον, η επιλογή ανοικτών τεχνολογιών

(Python, Flask, JSON) και εργαλείων ελέγχου χωρίς εμπορικές άδειες ενισχύει την εμπειρική διερεύνηση του τέταρτου ερευνητικού ερωτήματος, καθώς υποστηρίζει ότι η προτεινόμενη λύση μπορεί να αναπαραχθεί και να λειτουργήσει σε τυπικό hardware με χαμηλό κόστος εγκατάστασης, ανάπτυξης και συντήρησης—χαρακτηριστικό που είναι κρίσιμο για μικρομεσαίους οργανισμούς. Τέλος, τα tests ενσωματώνουν περιπτώσεις που προσεγγίζουν ρεαλιστικές αστοχίες (π.χ. ελλιπείς ή αντιφατικές απαντήσεις, σφάλματα κατά τη σάρωση ιστοσελίδων), επιτρέποντας μια πιο τεκμηριωμένη εκτίμηση της αξιοπιστίας και της πρακτικής χρησιμότητας του συστήματος στο πραγματικό περιβάλλον εφαρμογής, όπως ακριβώς ζητούν τα ερευνητικά ερωτήματα του Κεφαλαίου 1.[11]

3.4 Σύνδεση Μεθοδολογίας και Ερευνητικών Ερωτημάτων

Η μεθοδολογική προσέγγιση που παρουσιάστηκε στο παρόν κεφάλαιο έχει σχεδιαστεί έτσι ώστε να επιτρέπει τη συστηματική και τεκμηριωμένη διερεύνηση των τεσσάρων ερευνητικών ερωτημάτων που διατυπώθηκαν στην Εισαγωγή, σε άμεση συνάφεια με το ερευνητικό κενό που αναδείχθηκε στα προηγούμενα κεφάλαια. Με δεδομένο ότι το βασικό πρόβλημα δεν είναι απλώς η «καταγραφή» πληροφοριών αλλά η παραγωγή αξιόπιστων παραδοτέων (ιδίως κειμένων πολιτικής απορρήτου) με ασφαλή και επαναλήψιμο τρόπο, η μεθοδολογία οργανώθηκε ώστε κάθε σχεδιαστική επιλογή να αντιστοιχεί σε συγκεκριμένη υπόθεση που ελέγχεται εμπειρικά μέσα από την υλοποίηση.[11]

Ως προς το πρώτο ερευνητικό ερώτημα, το οποίο αφορά τη δυνατότητα σχεδιασμού ενός πληροφοριακού συστήματος που καθοδηγεί τον χρήστη βήμα-προς-βήμα στη διενέργεια DPIA και Gap Analysis, η μεθοδολογία υιοθετεί ερωτηματολόγια βάσει σχήματος (schema-driven questionnaires) και δυναμική απόδοση (dynamic rendering) μέσω Jinja2, ώστε η διαδικασία να μοντελοποιείται ως αλληλουχία σαφών και τυποποιημένων βημάτων. Παράλληλα, η συνεχής επικύρωση (validation) των εισαγόμενων δεδομένων διασφαλίζει ότι οι απαντήσεις είναι επαρκείς και συνεπείς, μειώνοντας την αβεβαιότητα που χαρακτηρίζει τις μη τυποποιημένες «συνεντεύξεις» και δημιουργώντας δομημένες εισροές που μπορούν να αξιοποιηθούν με σταθερό τρόπο στα επόμενα στάδια. Έτσι, η μεθοδολογία συνδέεται άμεσα με το ερευνητικό κενό της αγοράς/βιβλιογραφίας, όπου κυριαρχούν είτε εργαλεία καταγραφής είτε υπηρεσίες έντονα εξαρτημένες από ανθρώπινη ερμηνεία.[11]

Σε σχέση με το δεύτερο ερευνητικό ερώτημα, που εξετάζει πώς μπορεί να ενσωματωθεί ένα τοπικά εκτελούμενο Μεγάλο Γλωσσικό Μοντέλο για τη σύνθεση κειμένων πολιτικής απορρήτου, η μεθοδολογία προτείνει ελεγχόμενη χρήση του LLM αντί «ελεύθερης συνομιλίας». Συγκεκριμένα, προβλέπεται η χρήση εξειδικευμένων system prompts, η τροφοδότηση του μοντέλου αποκλειστικά με δομημένα δεδομένα που παράγονται από τα JSON schemas (context injection) και η λειτουργία σε περιβάλλον Local AI μέσω Ollama. Η επιλογή αυτή απαντά στις δύο κεντρικές προκλήσεις που αναδείχθηκαν στη βιβλιογραφία: αφενός, περιορίζει το πληροφοριακό πλαίσιο μέσα στο οποίο λειτουργεί το μοντέλο, μειώνοντας την πιθανότητα νομικά επικίνδυνων παραγωγής ψευδών πληροφοριών · αφετέρου, διατηρεί τις εισροές εντός της υποδομής του χρήστη, αντιμετωπίζοντας τους κινδύνους ιδιωτικότητας που συνδέονται με cloud-based λύσεις. Με τον τρόπο αυτό, η μεθοδολογία διερευνά εμπειρικά αν είναι εφικτή η παραγωγή συνεκτικού κειμένου πολιτικής απορρήτου με ελεγχόμενη συμπεριφορά, όπως απαιτείται από το ερευνητικό κενό της «generative» υποστήριξης.[11]

Το τρίτο ερευνητικό ερώτημα, που αφορά τα κατάλληλα αρχιτεκτονικά πρότυπα ώστε το σύστημα να μπορεί να προσαρμόζεται σε μελλοντικές αλλαγές του κανονιστικού πλαισίου και των απαιτήσεων τεκμηρίωσης, αντιμετωπίζεται μέσω της επιλογής modular αρχιτεκτονικής και του σαφούς διαχωρισμού περιεχομένου/λογικής (JSON vs Python). Η αποθήκευση ερωτηματολογίων σε εξωτερικά σχήματα, η χρήση μεταδεδομένων (π.χ. παραπομπές σε άρθρα) και η αξιοποίηση dataclasses για αυστηρό ορισμό δομών δεδομένων ενισχύουν τη συντηρησιμότητα και την ιχνηλασιμότητα, καθώς οι αλλαγές στο περιεχόμενο ή στους κανόνες μπορούν να υλοποιηθούν χωρίς αναδόμηση του πυρήνα της εφαρμογής. Έτσι, η μεθοδολογία συνδέεται άμεσα με τον στόχο του Κεφαλαίου 1 για αρχιτεκτονική επεκτασιμότητα και με το πρακτικό πρόβλημα που αναδείχθηκε στην ανάλυση αγοράς, όπου η παραμετροποίηση και η συντήρηση αποτελούν συχνά εμπόδια υιοθέτησης.[11]

Τέλος, το τέταρτο ερευνητικό ερώτημα, σχετικά με το κατά πόσο το σύστημα μπορεί να αποτελέσει ρεαλιστική και οικονομικά προσιτή εναλλακτική για ΜΜΕ, προσεγγίζεται με μεθοδολογικές επιλογές που μειώνουν άμεσα το κόστος και την τεχνική εξάρτηση: χρήση τεχνολογιών ανοικτού κώδικα, αποφυγή εμπορικών cloud υπηρεσιών AI, και στόχευση σε λειτουργία σε τυπικό εξοπλισμό γραφείου. Επιπλέον, η μεθοδολογία ενσωματώνει στοιχεία αρχικής εμπειρικής αξιολόγησης, όπως μετρήσεις απόδοσης (latency) σε βασικές λειτουργίες και πρώιμες ενδείξεις χρηστικότητας, ώστε η καταλληλότητα για ΜΜΕ να μην παραμείνει θεωρητικό επιχείρημα αλλά να υποστηριχθεί με πρακτικές παρατηρήσεις, οι οποίες αναλύονται στα επόμενα κεφάλαια. Με αυτόν τον τρόπο, η μεθοδολογία ολοκληρώνει τη σύνδεση ανάμεσα στο ερευνητικό κενό, στα ερευνητικά ερωτήματα του Κεφαλαίου 1 και στην υλοποίηση του «GDPR ASSESSOR» ως λειτουργικού πρωτότυπου.[11]

4 Αρχιτεκτονική Συστήματος

Στο παρόν κεφάλαιο παρουσιάζεται η αρχιτεκτονική του πληροφοριακού συστήματος «GDPR ASSESSOR», με στόχο την αποτύπωση του τρόπου με τον οποίο οι λειτουργικές και μη λειτουργικές απαιτήσεις μεταφράζονται σε συγκεκριμένες δομές λογισμικού. Η αρχιτεκτονική περιγράφεται σε πολλαπλά επίπεδα αφαίρεσης (use case, δραστηριότητας, ακολουθίας, κλάσεων, συστατικών στοιχείων), ώστε να καταστεί σαφές πώς ο χρήστης αλληλεπιδρά με το σύστημα, πώς ρέουν τα δεδομένα μεταξύ των υποσυστημάτων και πώς ενσωματώνονται οι μηχανισμοί Τεχνητής Νοημοσύνης και ελέγχου cookies στο συνολικό πλαίσιο. Με τον τρόπο αυτό, το κεφάλαιο λειτουργεί ως γέφυρα ανάμεσα στη μεθοδολογία σχεδιασμού και στην υλοποίηση που αναλύεται στα επόμενα κεφάλαια.[11]

4.1 Απαιτήσεις Συστήματος

Ο καθορισμός των απαιτήσεων αποτελεί το θεμέλιο για την επιτυχή υλοποίηση κάθε πληροφοριακού συστήματος. Στην περίπτωση του "GDPR ASSESSOR", η διαδικασία αυτή δεν ήταν μονοδιάστατη. Απαιτούσε τη συνέργεια δύο διαφορετικών πεδίων: της Μηχανικής Λογισμικού και της Νομικής Επιστήμης.[11]

Για την εξαγωγή των απαιτήσεων (Requirements Elicitation), ακολουθήθηκε μια μεθοδολογία βασισμένη σε σενάρια. Μελετήθηκαν οι καθημερινές ανάγκες ενός Υπευθύνου Προστασίας Δεδομένων (DPO). Αναλύθηκαν επίσης οι κατευθυντήριες γραμμές του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (EDPB). Στόχος ήταν να μετατραπούν οι νομικές υποχρεώσεις σε σαφείς τεχνικές προδιαγραφές.[11]

Οι απαιτήσεις διακρίνονται σε δύο κατηγορίες: τις Λειτουργικές (τι πρέπει να κάνει το σύστημα) και τις Μη Λειτουργικές (πώς πρέπει να συμπεριφέρεται το σύστημα).

4.1.1 Λειτουργικές Απαιτήσεις (Functional Requirements)

Οι λειτουργικές απαιτήσεις περιγράφουν τις συγκεκριμένες υπηρεσίες που παρέχει η εφαρμογή στον χρήστη. Κάθε απαίτηση σχεδιάστηκε για να καλύπτει ένα συγκεκριμένο άρθρο του Κανονισμού ή μια πρακτική ανάγκη της αγοράς.[11]

Ακολουθεί η αναλυτική παρουσίαση των απαιτήσεων σε μορφή πινάκων.

Πίνακας 2: Λειτουργικές απαιτήσεις

Id	Απαίτηση	***Περιγραφή***	Προτεραιότητα	Συσχέτιση
FR-01	Διενέργεια DPIA	Το σύστημα πρέπει να παρέχει διαδραστικό ερωτηματολόγιο για την εκτέλεση Εκτίμησης Αντικτύπου	Υψηλή	GDPR Art. 35

		(DPIA) βάσει του Άρθρου 35, με δυνατότητα αποθήκευσης προόδου.		
FR-02	Ανάλυση Κενών (Gap Analysis)	Δυνατότητα ελέγχου συμμόρφωσης με οργανωτικά μέτρα (Governance & Oversight) και εντοπισμός ελλείψεων.	Υψηλή	ISO 27001
FR-03	Αυτόματος Έλεγχος Cookies	Το σύστημα πρέπει να δέχεται URL ιστοσελίδας, να τη σαρώνει (crawl) και να εντοπίζει cookies/trackers κατηγοριοποιώντας τα (Marketing, Analytics, Necessary).	Μεσαία	e-Privacy Dir.
FR-04	Παραγωγή Πολιτικών με AI	Δυνατότητα αυτόματης σύνταξης κειμένων (Πολιτική Απορρήτου, Διαδικασία Παραβίασης) αξιοποιώντας τοπικά γλωσσικά μοντέλα (LLMs) βάσει των απαντήσεων του χρήστη.	Υψηλή	FR-01, FR-02
FR-05	Υπολογισμός Σκορ Ετοιμότητας	Αυτόματος υπολογισμός και οπτικοποίηση (μέσω γραφημάτων) του βαθμού ετοιμότητας (Readiness Score) και του επιπέδου ρίσκου.	Μεσαία	-
FR-06	Εξαγωγή Αναφορών	Δυνατότητα εξαγωγής των τελικών αποτελεσμάτων και των παραγόμενων πολιτικών σε μορφή PDF και Markdown.	Υψηλή	-

Ανάλυση Λειτουργικών Απαιτήσεων Η απαίτηση FR-01 (DPIA) είναι η πιο κρίσιμη. Το Άρθρο 35 του GDPR καθιστά την εκτίμηση αντικτύπου υποχρεωτική για επεξεργασίες υψηλού κινδύνου. Το σύστημα πρέπει να καθοδηγεί τον χρήστη. Δεν αρκεί μια απλή φόρμα. Απαιτείται δυναμική ροή ερωτήσεων που προσαρμόζεται ανάλογα με τον κλάδο της επιχείρησης.[11]

Η απαίτηση **FR-04** εισάγει την καινοτομία της Τεχνητής Νοημοσύνης. Συνδέει τα δεδομένα των αξιολογήσεων (FR-01, FR-02) με τη μηχανή παραγωγής κειμένου. Αυτό επιλύει το πρόβλημα του "λευκού χαρτιού" που αντιμετωπίζουν πολλοί DPOs.

Τέλος, η **FR-03** (Cookie Audit) καλύπτει την τεχνική πλευρά. Η Οδηγία ePrivacy απαιτεί ρητή συγκατάθεση για μη απαραίτητα cookies. Ο αυτόματος έλεγχος διασφαλίζει ότι η νομική της πολιτικής απορρήτου συμβαδίζει με την τεχνική πραγματικότητα της ιστοσελίδας.[11]

4.1.2 Σύντομη Ανάλυση και Παρατηρήσεις

Βάσει των παραπάνω απαιτήσεων, προκύπτουν τα εξής ενδιαφέροντα σημεία για την αρχιτεκτονική του συστήματος:

1) Ιδιωτικότητα μέσω Τοπικού AI (Privacy-First Approach): Η απαίτηση FR-04 είναι ιδιαίτερα σημαντική. Η διευκρίνιση για χρήση τοπικών γλωσσικών μοντέλων (Local LLMs) και όχι

cloud-based APIs (όπως π.χ. του OpenAI) δείχνει μια αρχιτεκτονική απόφαση προσανατολισμένη στην ασφάλεια. Αυτό διασφαλίζει ότι τα ευαίσθητα δεδομένα που εισάγονται στα DPIA (FR-01) και Gap Analysis (FR-02) δεν φεύγουν ποτέ από την υποδομή του πελάτη για να δημιουργηθούν οι πολιτικές. Αυτό όμως αυξάνει τις απαιτήσεις υλικού (hardware requirements) του συστήματος.[11]

2) Διακριτό Υποσύστημα Crawler: Η απαίτηση FR-03 (Cookie Scanner) περιγράφει μια λειτουργία που τεχνικά διαφέρει από τις υπόλοιπες. Απαιτεί την υλοποίηση ενός web crawler/scraper, ο οποίος πρέπει να μπορεί να διαχειρίζεται δυναμικές ιστοσελίδες (πιθανώς να απαιτείται headless browser) για να εντοπίζει σωστά τα cookies που φορτώνονται μέσω JavaScript.
3) Ροή Δεδομένων και Εξαρτήσεις: Υπάρχει μια σαφής ροή εργασίας:
   - Ο χρήστης εισάγει δεδομένα μέσω των διαδραστικών φορμών (FR-01, FR-02) και το σύστημα συλλέγει δεδομένα αυτόματα (FR-03).
   - Τα δεδομένα αυτά τροφοδοτούν το τοπικό AI για τη δημιουργία κειμένων (FR-04) και την μηχανή υπολογισμού ρίσκου (FR-05).
   - Τέλος, όλα τα παραπάνω συγκεντρώνονται για την τελική εξαγωγή (FR-06).

Πίνακας 3: Μη Λειτουργικές απαιτήσεις

ID	Τίτλος Απαίτησης	Περιγραφή	Κατηγορία	Σημαντικότητα
NFR-01	Προστασία Ιδιωτικότητας (Local Processing)	Όλα τα δεδομένα των αξιολογήσεων και η επεξεργασία AI (Inference) πρέπει να εκτελούνται αποκλειστικά τοπικά (on-premise/local execution) χωρίς αποστολή δεδομένων στο cloud.	Ασφάλεια	Κρίσιμη
NFR-02	Επεκτασιμότητα Μοντέλων	Η αρχιτεκτονική πρέπει να είναι αρθρωτή (modular), επιτρέποντας την εύκολη εναλλαγή ή αναβάθμιση του γλωσσικού μοντέλου (π.χ. σε νεότερη έκδοση Llama/Mistral) μέσω του μηχανισμού llm.py.	Συντηρησιμότητα	Υψηλή
NFR-03	Χρόνος Απόκρισης AI	Η παραγωγή κειμένου από το τοπικό LLM δεν πρέπει να υπερβαίνει τα 60 δευτερόλεπτα ανά ενότητα πολιτικής απορρήτου, για να	Απόδοση	Μεσαία

Οι μη			διασφαλίζεται μια αποδεκτή εμπειρία χρήστη.		
	NFR-04	Φιλικότητα Διεπαφής	Το UI πρέπει να είναι διαισθητικό και κατανοητό από χρήστες χωρίς βαθύ τεχνικό υπόβαθρο (π.χ. DPOs, Νομικούς Συμβούλους), παρέχοντας σαφείς οδηγίες και οπτική ένδειξη προόδου.	Ευχρηστία	Υψηλή

λειτουργικές απαιτήσεις ορίζουν τα ποιοτικά χαρακτηριστικά και τους περιορισμούς υπό τους οποίους πρέπει να λειτουργεί το σύστημα. Ιδιαίτερη έμφαση δίνεται στην ασφάλεια και την ιδιωτικότητα.

4.1.3 Ανάλυση Μη Λειτουργικών Απαιτήσεων

Η απαίτηση NFR-01 αποτελεί τον ακρογωνιαίο λίθο της αρχιτεκτονικής μας. Σε αντίθεση με τις εμπορικές λύσεις SaaS, το σύστημά μας πρέπει να λειτουργεί σε περιβάλλον "Air-Gapped" (χωρίς σύνδεση στο διαδίκτυο, εάν απαιτείται). Αυτό επιβάλλει τη χρήση τοπικών μοντέλων AI (Local LLMs) μέσω εργαλείων όπως το Ollama.[11]

Η NFR-02 διασφαλίζει τη μακροζωία του συστήματος. Ο τομέας της Τεχνητής Νοημοσύνης εξελίσσεται ραγδαία. Νέα μοντέλα κυκλοφορούν κάθε μήνα. Ο κώδικας πρέπει να είναι αρθρωτός (modular), ώστε η αναβάθμιση του "εγκεφάλου" της εφαρμογής να μην απαιτεί επανασυγγραφή του λογισμικού.

Η NFR-03 έχει άμεση εξάρτηση με το hardware το οποίο φιλοξενεί το σύστημα καθώς η γρήγορη εκτέλεση των εντολών-prompts από το Μεγάλο Γλωσσικό Μοντέλο επηρεάζεται άμεσα από τον επεξεργαστή , την RAM , την κάρτα γραφικών όπως επίσης και το σκληρό δίσκο που έχει ο χρήστης ο οποίος χρησιμοποιεί/φιλοξενεί το σύστημα.

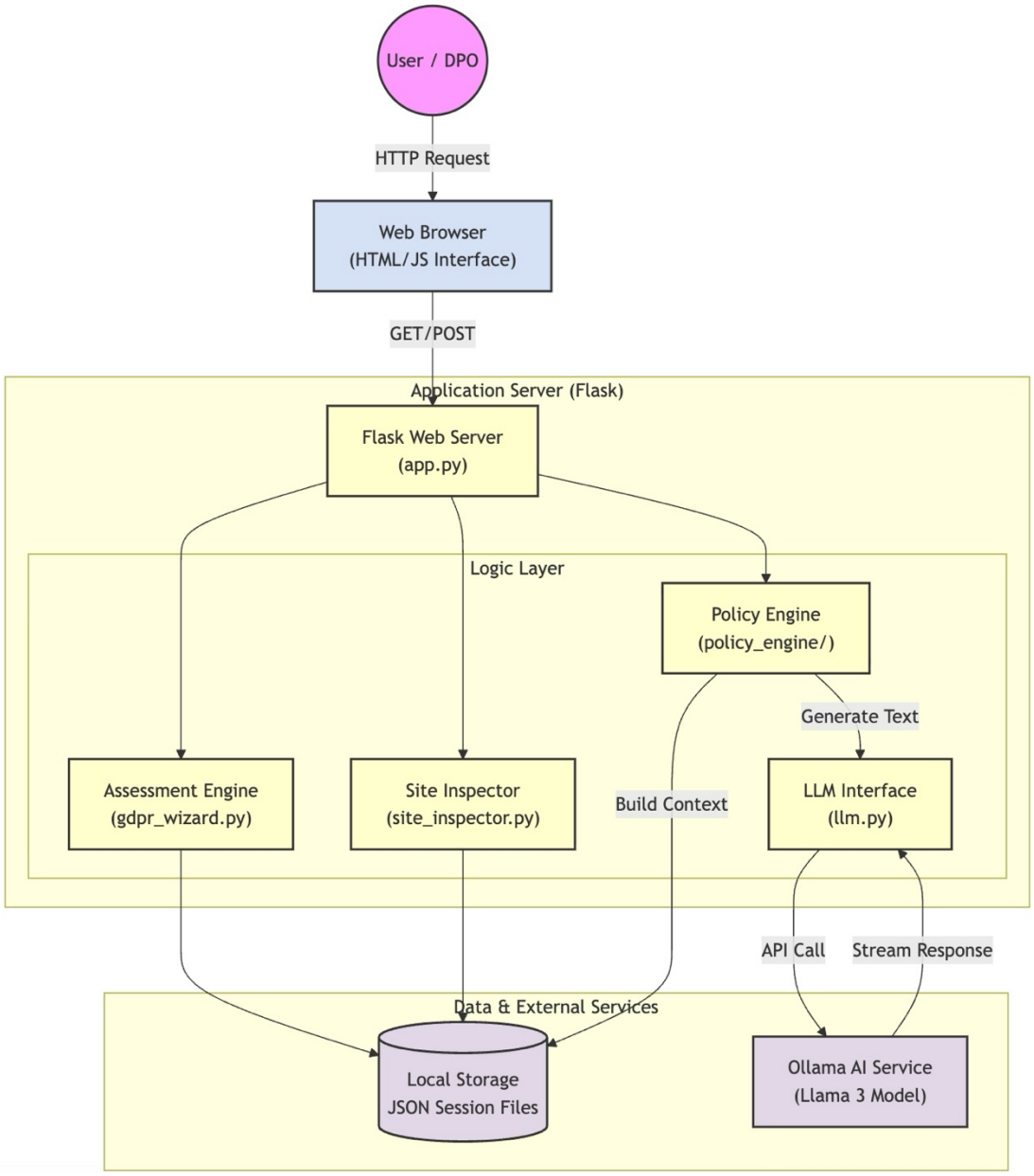
Τέλος, η NFR-04 αναγνωρίζει το προφίλ του τελικού χρήστη. Ο DPO συχνά δεν είναι μηχανικός πληροφορικής. Η διεπαφή πρέπει να είναι απλή, καθαρή και καθοδηγητική, μειώνοντας την πιθανότητα σφάλματος χειρισμού.

4.2 Διαγράμματα

Η αρχιτεκτονική του συστήματος "GDPR Assesor" σχεδιάστηκε με γνώμονα την ασφάλεια, την ιδιωτικότητα και την αρθρωτή (modular) ανάπτυξη. Η πολυπλοκότητα του "GDPR ASSESOR" επέβαλε τη χρήση προτύπων οπτικής μοντελοποίησης πριν και κατά τη διάρκεια της συγγραφής του κώδικα. Η μοντελοποίηση εστιάζει σε τρεις κρίσιμες όψεις: τις λειτουργίες χρήστη (Use Case), τη ροή εργασιών (Activity) και τη δομική συγκρότηση (Component).[11]

Η αρχιτεκτονική που απεικονίζεται στο διάγραμμα ακολουθεί μια καθαρή λογική τριών επιπέδων: επίπεδο παρουσίασης (web διεπαφή μέσω browser), επίπεδο λογικής (Flask application και υποσυστήματα Python) και επίπεδο δεδομένων (αρχεία JSON και δομημένοι φάκελοι εξόδου). Ο διαχωρισμός αυτός επιτρέπει την ανεξάρτητη εξέλιξη του κάθε επιπέδου: η διεπαφή μπορεί να βελτιωθεί χωρίς αλλαγές στον πυρήνα των αλγορίθμων, ενώ τα σχήματα των δεδομένων μπορούν

να εμπλουτιστούν χωρίς να απαιτείται ανασχεδιασμός της διεπαφής. Επιπλέον, η απουσία εξωτερικής βάσης δεδομένων μειώνει την πολυπλοκότητα εγκατάστασης και ενισχύει την αρχή της «ελαχιστοποίησης των δεδομένων», καθώς τα δεδομένα παραμένουν σε τοπικά, διαφανή αρχεία, υπό τον πλήρη έλεγχο του οργανισμού.



Εικόνα 1: Αρχιτεκτονική Συστήματος και Ροή Δεδομένων

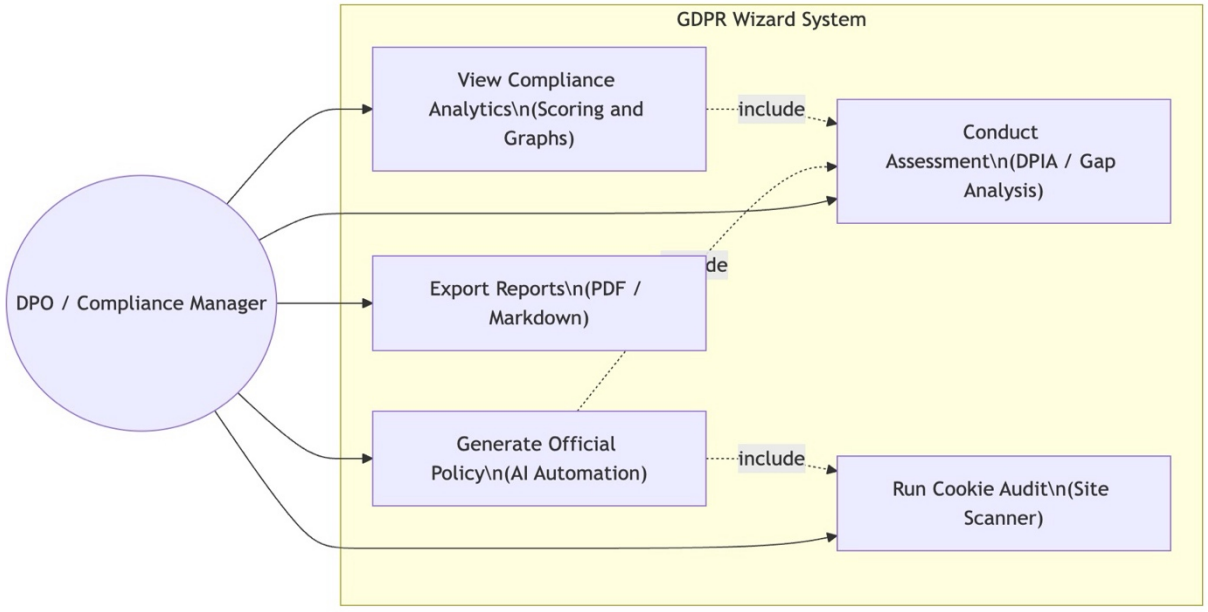
Ανάλυση Διαγράμματος : Όπως φαίνεται στο διάγραμμα, ο χρήστης αλληλεπιδρά με το σύστημα μέσω ενός Web Browser. Τα αιτήματα (HTTP Requests) διαχειρίζεται ο εξυπηρετητής εφαρμογής που έχει υλοποιηθεί με το πλαίσιο Flask (app.py). Στο επίπεδο της λογικής (Logic Layer), διακρίνουμε τρία βασικά υποσυστήματα:

1) **Assessment Engine (gdpr_wizard.py):** Υπεύθυνο για τη διαχείριση των ερωτηματολογίων DPIA/Gap, την επικύρωση των απαντήσεων και τον υπολογισμό των σκορ.[11]
2) **Site Inspector (cookie_audit.py):** Υποσύστημα που εκτελεί τη σάρωση ιστοσελίδων για την ανίχνευση cookies.
3) **Policy Engine (policy_engine/):** Ο μηχανισμός που συνθέτει τα "Prompts" και επικοινωνεί με το τοπικό API του Ollama (llm.py) για την παραγωγή κειμένου. Τέλος, στο επίπεδο δεδομένων (Data Layer), η κατάσταση αποθηκεύεται σε δομημένα αρχεία JSON (Session Storage), εξασφαλίζοντας την ακεραιότητα και τη φορητότητα των δεδομένων χωρίς την ανάγκη βαριάς βάσης δεδομένων.[11]

4.2.1 Διάγραμμα Περιπτώσεων Χρήσης (Use Case Diagram)

Το Διάγραμμα Περιπτώσεων Χρήσης (Εικόνα 2) περιγράφει τις λειτουργίες που παρέχει το σύστημα στους τελικούς χρήστες. Ο βασικός δρων του συστήματος (Actor) είναι ο Υπεύθυνος Προστασίας Δεδομένων (DPO) ή ο διαχειριστής συμμόρφωσης.

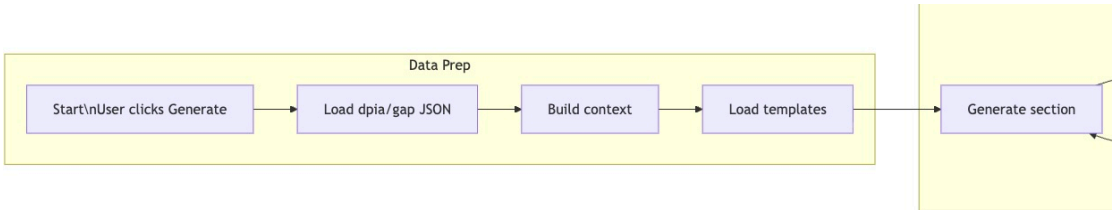
Το διάγραμμα περιπτώσεων χρήσης αναδεικνύει ότι το σύστημα έχει σχεδιαστεί με γνώμονα τον ρόλο του Υπευθύνου Προστασίας Δεδομένων ως κεντρικού «δρώντος» (actor). Αντί να προσφέρει έναν μεγάλο αριθμό αποσπασματικών λειτουργιών, η αρχιτεκτονική οργανώνει τις δυνατότητες σε ολοκληρωμένες ροές εργασίας (workflows): από τη διενέργεια αξιολόγησης (DPIA/Gap) και τον τεχνικό έλεγχο του ιστότοπου, έως την παραγωγή πολιτικών και την ανάλυση κινδύνου. Με τον τρόπο αυτό, απαντάται σε αρχικό επίπεδο το πρώτο ερευνητικό ερώτημα, καθώς η ίδια η δομή των περιπτώσεων χρήσης υλοποιεί την ανάγκη για βήμα-προς-βήμα καθοδήγηση του χρήστη, ενσωματώνοντας τα άρθρα του GDPR στις λειτουργίες που αναλαμβάνει το σύστημα.[11]



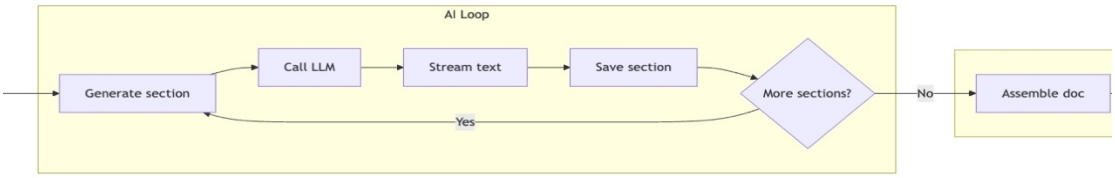
Εικόνα 2 : Διάγραμμα Περιπτώσεων Χρήσης

4.2.2 Διάγραμμα Δραστηριότητας: Παραγωγή Πολιτικής Απορρήτου με AI (Activity Diagram)

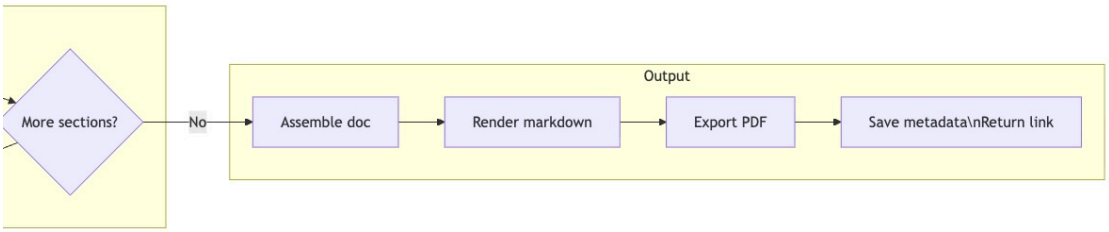
Το συγκεκριμένο διάγραμμα (Εικόνα 4.3) αναλύει τη ροή εκτέλεσης της πιο σύνθετης λειτουργίας του συστήματος: την αυτόματη παραγωγή κειμένου πολιτικής απορρήτου μέσω του LLM.[11]



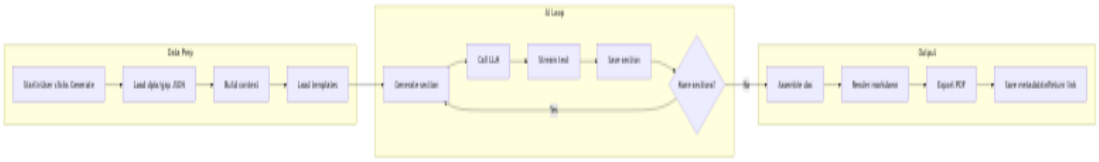
Εικόνα 3: Απεικόνιση Δραστηριότητας Διαδικασίας Παραγωγής Πολιτικής [1/3]



Εικόνα 4: Απεικόνηση Δραστηριότητας διαδικασίας παραγωγής Πολιτικής [2/3]



Εικόνα 5: Απεικόνιση Δραστηριότητας διαδικασίας παραγωγής Πολιτικής [3/3]



Εικόνα 6: Δραστηριότητας διαδικασίας παραγωγής [ολοκληρωμένο]

Το σύστημα ανακτά τις αποθηκευμένες απαντήσεις από τα αρχεία dpia.json και gap.json (λειτουργία combined_assessment_inputs στο app.py).[11]

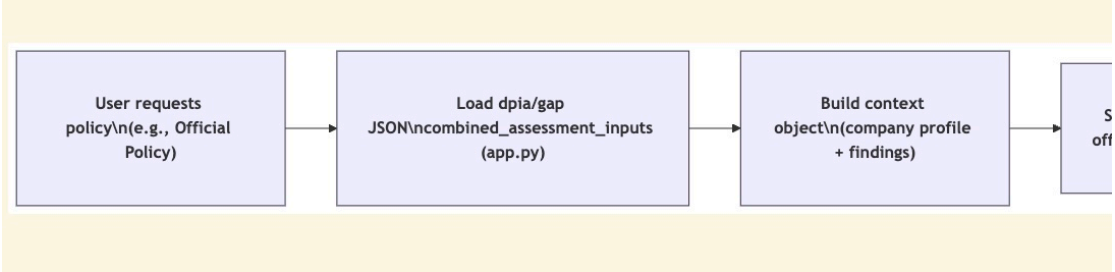
1. Δημιουργείται ένα "Context Object" που περιλαμβάνει το προφίλ της εταιρείας και τα ευρήματα των ελέγχων.
2. Επιλέγεται το κατάλληλο "System Prompt" (π.χ. από το αρχείο official_policy_overview_en.txt) το οποίο καθοδηγεί το AI για το ύφος και τη δομή του κειμένου.
3. Το αίτημα αποστέλλεται ασύγχρονα στην υπηρεσία Ollama (run_ollama στο llm.py).
4. Το παραγόμενο κείμενο λαμβάνεται, μετατρέπεται από Markdown σε HTML/PDF και παρουσιάζεται στον χρήστη για λήψη.

Η ανάλυση της ροής δραστηριοτήτων για την παραγωγή πολιτικής απορρήτου αναδεικνύει τον τρόπο με τον οποίο η αρχιτεκτονική επιχειρεί να «περιορίσει» λειτουργικά το Μεγάλο Γλωσσικό Μοντέλο μέσα σε ένα αυστηρά ορισμένο πλαίσιο. Το LLM δεν καλείται να απαντήσει σε ελεύθερες νομικές ερωτήσεις, αλλά να μετασχηματίσει σε συνεκτικό κείμενο ένα ήδη δομημένο σύνολο δεδομένων (προφίλ οργανισμού, αποτελέσματα DPIA/Gap, ευρήματα ελέγχου cookies). Στο επίπεδο της αρχιτεκτονικής, αυτό υλοποιείται μέσω της δημιουργίας ενός «αντικειμένου συμφραζομένων» (context object), το οποίο συγκεντρώνει όλα τα απαραίτητα στοιχεία πριν από την κλήση του μοντέλου. Η σχεδιαστική αυτή επιλογή συνδέεται άμεσα με το δεύτερο ερευνητικό ερώτημα, καθώς δείχνει πώς η ενσωμάτωση ενός τοπικού LLM μπορεί να γίνει με τρόπο που μειώνει τις παραγωγής ψευδών πληροφοριών και διατηρεί τον έλεγχο της ροής πληροφορίας.[11]

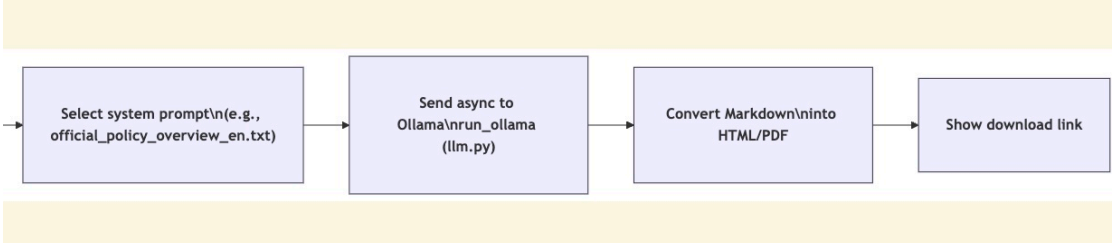
Η χρήση αυτών των διαγραμμάτων κατά την ανάπτυξη βοήθησε στον εντοπισμό πιθανών σημείων καθυστέρησης (bottlenecks) κατά την επικοινωνία με το μοντέλο AI και στη βελτιστοποίηση της διαχείρισης μνήμης κατά τη σύνθεση μεγάλων εγγράφων.

4.3 Διάγραμμα Κλάσεων (Class Diagram)

Το παρόν διάγραμμα αποτυπώνει τη δομή του Assessment Engine. Βασίζεται στο αρχείο gdpr_wizard.py και αναδεικνύει τον αντικειμενοστραφή σχεδιασμό για τη διαχείριση των ερωτηματολογίων.[11]



Εικόνα 7: Δομή Assesment Engine [1/2]



Εικόνα 8: Δομή Assesment Engine [2/2]

Εικόνα 9: Δομή Assesment Engine [ολοκληρωμένο]

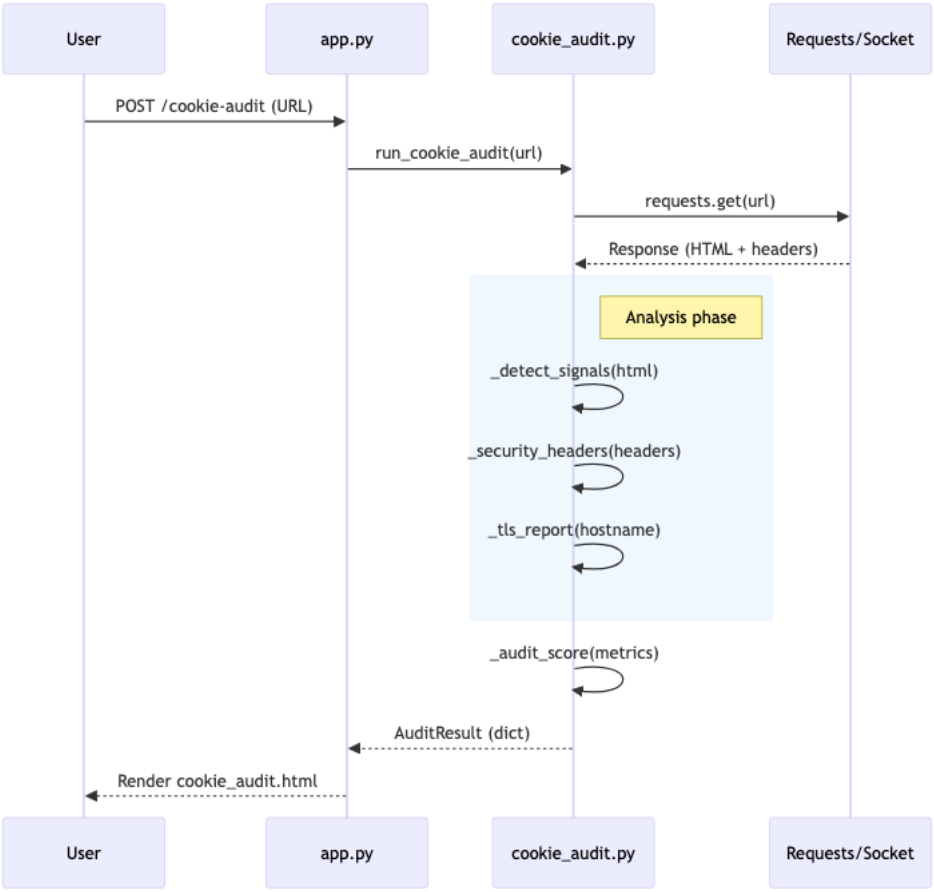
Περιγραφή: Το διάγραμμα δείχνει τη σχέση μεταξύ της κλάσης Question, που ορίζει τη δομή της ερώτησης, και του Assesment Enigne, που εκτελεί τον υπολογισμό του σκορ.

Τα διαγράμματα κλάσεων αποτυπώνουν την προσπάθεια να συγκεντρωθεί η επιχειρησιακή λογική της αξιολόγησης σε λίγες, σαφώς ορισμένες κλάσεις, με ξεκάθαρες ευθύνες. Η κλάση Question, για παράδειγμα, λειτουργεί ως βασική μονάδα πληροφορίας, ενώ η AssessmentBuilder αναλαμβάνει τη σύνθεση των επιμέρους απαντήσεων σε συνολικό σκορ και δομημένες αναφορές.

Η χρήση τέτοιων αντικειμενοστραφών δομών σε συνδυασμό με dataclasses καθιστά τον κώδικα πιο αναγνώσιμο και ελέγξιμο, διευκολύνοντας τόσο την επαναχρησιμοποίηση όσο και την επέκταση των λειτουργιών. Σε όρους αρχιτεκτονικής, αυτό σημαίνει ότι η μελλοντική προσθήκη νέων τύπων αξιολόγησης (π.χ. αξιολόγηση βάσει AI Act) μπορεί να υλοποιηθεί μέσω νέων κλάσεων ή υποκλάσεων, χωρίς να διαρραγεί η συνολική δομή του συστήματος.[11]

4.4 Διάγραμμα Ακολουθίας Ελέγχου Cookies (Sequence Diagram)

Αυτό το διάγραμμα αναλύει τη λειτουργία του Site Inspector. Εστιάζει στη χρονική αλληλουχία των κλήσεων από τη στιγμή που ο χρήστης εισάγει ένα URL μέχρι την παραγωγή της αναφοράς.



Εικόνα 10: Δομή Cookie Audit

- **Περιγραφή:** Ο χρήστης ζητά έλεγχο μέσω του app.py. Η συνάρτηση run_cookie_audit εκτελεί HTTP request, αναλύει τα headers ασφαλείας και εντοπίζει ιχνηλάτες μέσω Regular Expressions.
- **Στοιχείο Κώδικα:** Απεικονίζει τη ροή δεδομένων μεταξύ του app.py και των βοηθητικών συναρτήσεων _detect_signals και _audit_score.

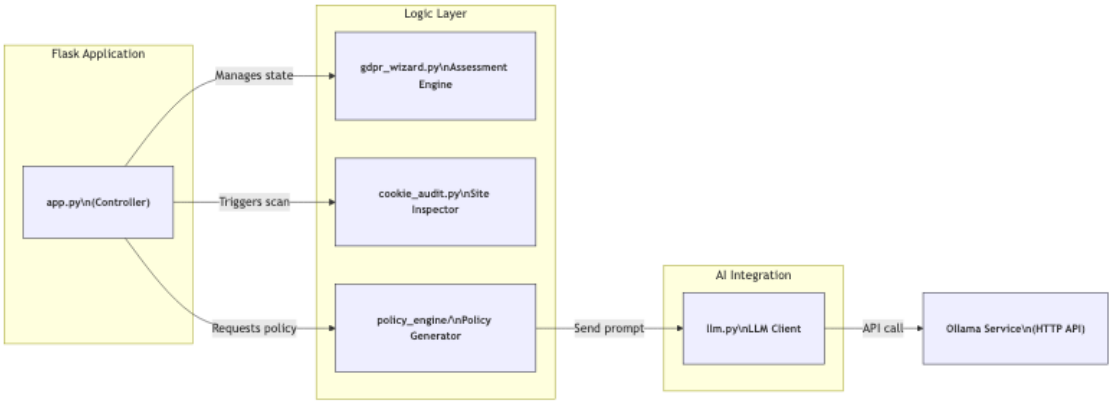
Το διάγραμμα ακολουθίας για τον έλεγχο cookies αναδεικνύει τη διαφοροποίηση του υποσυστήματος Site Inspector από τα υπόλοιπα μέρη της εφαρμογής. Ενώ το Assessment Engine βασίζεται κυρίως σε δηλώσεις του χρήστη, ο έλεγχος cookies αξιοποιεί τεχνικές στατικής ανάλυσης για να αποτυπώσει την πραγματική συμπεριφορά του ιστότοπου. Η αρχιτεκτονική διασφαλίζει ότι

το συγκεκριμένο υποσύστημα παραμένει αρθρωτό και ανεξάρτητο, έτσι ώστε μελλοντικά να μπορεί να αντικατασταθεί από πιο προηγμένες τεχνικές (π.χ. χρήση headless browser) χωρίς να επηρεαστεί η υπόλοιπη εφαρμογή. Αυτό αποτελεί πρακτική εφαρμογή της modular σχεδίασης που σχετίζεται με το τρίτο ερευνητικό ερώτημα, καθώς επιτρέπει την εξέλιξη του εργαλείου σύμφωνα με τις τεχνικές και κανονιστικές απαιτήσεις της αγοράς.

4.5 Διάγραμμα Συστατικών Στοιχείων (Component Diagram)

Το διάγραμμα αυτό χαρτογραφεί την αρθρωτή αρχιτεκτονική του backend. Δείχνει πώς τα διαφορετικά Python modules αλληλεπιδρούν για να συνθέσουν την τελική εφαρμογή.

- **Περιγραφή:** Το app.py λειτουργεί ως ο ενορχηστρωτής. Συνδέεται με το policy_engine για τη δημιουργία κειμένων, το llm.py για την επικοινωνία με το Ollama και το gdpr_wizard για τη λογική αξιολόγησης.[11]
    - **Στοιχείο Κώδικα:** Αποτυπώνει τα import statements και την οργάνωση των φακέλων (policy_engine/) όπως ορίζονται στο σύστημα αρχείων.



Εικόνα 11: Διάγραμμα Συστατικών Στοιχείων

Η χαρτογράφηση των συστατικών στοιχείων του backend αποδεικνύει ότι η εφαρμογή έχει σχεδιαστεί με σαφείς «συμβάσεις» επικοινωνίας μεταξύ των modules. Το app.py λειτουργεί ως ενορχηστρωτής (orchestrator), αλλά η πραγματική λογική βρίσκεται σε διακριτά components, όπως το gdpr_wizard για τις αξιολογήσεις, το policy_engine για τη διαχείριση των prompts και το llm.py για την επικοινωνία με το LLM. Αυτή η διάσπαση επιτρέπει τόσο την παράλληλη ανάπτυξη από διαφορετικές ομάδες όσο και την αντικατάσταση επιμέρους modules (π.χ. διαφορετικό LLM ή διαφορετικός μηχανισμός οπτικοποίησης) χωρίς συνολική ανακατασκευή. Στο πλαίσιο του τέταρτου ερευνητικού ερωτήματος, η modular αρχιτεκτονική συμβάλλει επίσης στη μείωση του κόστους συντήρησης, καθώς οι αλλαγές εντοπίζονται σε περιορισμένα τμήματα κώδικα.[11]

4.6 Σύνοψη Κεφαλαίου

Στο παρόν κεφάλαιο παρουσιάστηκε η αρχιτεκτονική του συστήματος «GDPR ASSESSOR» σε πολλαπλά επίπεδα αφαίρεσης. Μέσα από τα διαγράμματα περιπτώσεων χρήσης, δραστηριότητας, ακολουθίας, κλάσεων και συστατικών στοιχείων αποτυπώθηκε ο τρόπος με τον οποίο οι λειτουργικές απαιτήσεις (DPIA, Gap Analysis, έλεγχος cookies, παραγωγή πολιτικών,

οπτικοποίηση αποτελεσμάτων) και οι μη λειτουργικές απαιτήσεις (ασφάλεια, επεκτασιμότητα, τοπική επεξεργασία) ενσωματώνονται σε μια συνεκτική αρχιτεκτονική λύση.[11]

Η ανάλυση ανέδειξε ότι η επιλογή τριεπίπεδης αρχιτεκτονικής, schema-driven ανάπτυξης, modular οργάνωσης των υποσυστημάτων και τοπικής εκτέλεσης του LLM επιτρέπει στο σύστημα να παραμένει ευέλικτο, επεκτάσιμο και συμβατό με τις αρχές του GDPR περί προστασίας δεδομένων εξ ορισμού και εξ αρχής. Επιπλέον, έγινε σαφές ότι η αρχιτεκτονική δεν εξυπηρετεί μόνο τεχνικούς στόχους, αλλά συνδέεται άμεσα με τα ερευνητικά ερωτήματα της εργασίας, καθώς καθορίζει πώς υλοποιείται η βήμα-προς-βήμα καθοδήγηση του χρήστη, πώς ενσωματώνεται ένα τοπικό LLM με ελεγχόμενο τρόπο, ποιες αρχιτεκτονικές επιλογές διευκολύνουν την προσαρμογή σε νέους κανονισμούς και σε ποιο βαθμό η λύση παραμένει προσιτή για μικρομεσαίους οργανισμούς.[11]

Στο επόμενο κεφάλαιο παρουσιάζονται τα συγκεκριμένα εργαλεία ανάπτυξης και τεχνολογίες που επιλέχθηκαν για την υλοποίηση της παραπάνω αρχιτεκτονικής, καθώς και ο τρόπος με τον οποίο οι επιλογές αυτές ενισχύουν την ασφάλεια, την απόδοση και τη συντηρησιμότητα του συστήματος.

5 Εργαλεία Ανάπτυξης Συστήματος

Στο κεφάλαιο αυτό παρουσιάζονται τα βασικά εργαλεία και οι τεχνολογίες που συγκροτούν την τεχνολογική στοίβα (tech stack) του «GDPR ASSESSOR». Η επιλογή κάθε εργαλείου δεν ήταν τυχαία, αλλά συνδέεται με συγκεκριμένες λειτουργικές και μη λειτουργικές απαιτήσεις, όπως η ανάγκη για τοπική εκτέλεση της τεχνητής νοημοσύνης (Local AI), η ευελιξία στην προσαρμογή των ερωτηματολογίων και η ευχρηστία της διεπαφής για μη τεχνικούς χρήστες. Στις επόμενες ενότητες αιτιολογείται η επιλογή της Python ως γλώσσας ανάπτυξης, του Flask ως μικρο-πλαισίου διαδικτύου, του Ollama και του Llama 3 για την υλοποίηση της μηχανής τεχνητής νοημοσύνης, καθώς και των εργαλείων Jinja2 και Chart.js για τη δυναμική σύνθεση της διεπαφής και την οπτικοποίηση των αποτελεσμάτων.[11]

Η επιλογή των εργαλείων ανάπτυξης βασίστηκε σε μία αυστηρή διαδικασία αξιολόγησης. Κάθε εργαλείο επιλέχθηκε για να εξυπηρετήσει συγκεκριμένες ανάγκες του συστήματος "GDPR ASSESSOR". Η αρχιτεκτονική εστιάζει στην ασφάλεια των δεδομένων και την ευελιξία του κώδικα. Η ανάπτυξη βασίστηκε αποκλειστικά σε τεχνολογίες ανοιχτού κώδικα (open-source). Αυτό εξασφαλίζει τη διαφάνεια και τη δυνατότητα ελέγχου του λογισμικού.[11]

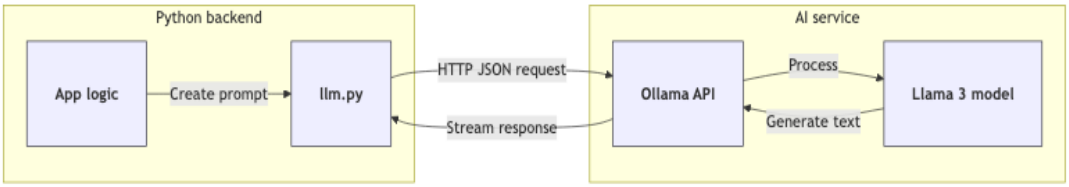
Ως κεντρική γλώσσα προγραμματισμού επιλέχθηκε η Python (έκδοση 3.12+). Η Python προσφέρει τρία βασικά πλεονεκτήματα που κρίθηκαν απαραίτητα για την υλοποίηση της διπλωματικής εργασίας:

5.1 Οικοσύστημα Τεχνητής Νοημοσύνης

Η Python αποτελεί τη βασική γλώσσα για εφαρμογές Τεχνητής Νοημοσύνης. Το σύστημά μας πρέπει να επικοινωνεί με το γλωσσικό μοντέλο Llama 3. Η Python διαθέτει βιβλιοθήκες που επιτρέπουν αυτή την επικοινωνία άμεσα. Στο αρχείο llm.py, χρησιμοποιούμε τη βιβλιοθήκη requests. Αυτή στέλνει τα δεδομένα στο μοντέλο και λαμβάνει τις απαντήσεις σε πραγματικό χρόνο (streaming). Δεν χρειάζονται ενδιάμεσα εργαλείο μετατροπής. Αυτό καθιστά την εφαρμογή πιο γρήγορη και λιγότερο επιρρεπή σε σφάλματα.[11]

Πέρα από την ευρεία διάδοση και την απλότητα της σύνταξής της, η Python προσφέρει ένα ώριμο οικοσύστημα βιβλιοθηκών που ευνοεί την ανάπτυξη λύσεων RegTech. Βιβλιοθήκες όπως requests, json και pathlib διευκολύνουν τη διαχείριση HTTP αιτημάτων, τη σειριοποίηση δεδομένων και την ασφαλή πρόσβαση στο σύστημα αρχείων, ενώ εργαλεία όπως pytest και unittest επιτρέπουν την εύκολη υλοποίηση αυτοματοποιημένων ελέγχων. Επιπλέον, η στενή διασύνδεση της Python με τα σύγχρονα frameworks μηχανικής μάθησης και τεχνητής νοημοσύνης καθιστά

εφικτή τη μελλοντική ενσωμάτωση πιο εξειδικευμένων μοντέλων, χωρίς ριζική αλλαγή της γλώσσας ή της στοίβας ανάπτυξης.[11]

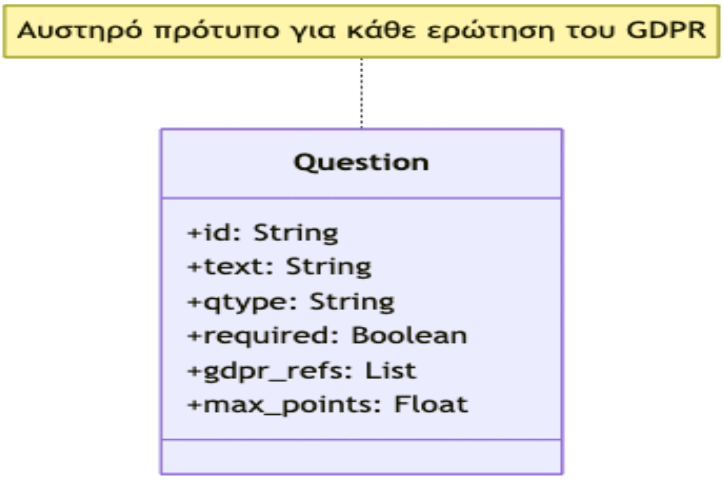


Εικόνα 12: Διάγραμμα Επικοινωνίας Ollama-Llama με το σύστημα

5.1.1 Αυστηρός Ορισμός Δομών Δεδομένων

Η αξιοπιστία του κώδικα είναι κρίσιμη. Για να αποφύγουμε λάθη κατά την εκτέλεση, χρησιμοποιούμε "κλάσεις δεδομένων" (dataclasses). Αυτό σημαίνει ότι ορίζουμε αυστηρά τη μορφή που πρέπει να έχει κάθε πληροφορία. Στο αρχείο gdpr_wizard.py, η κλάση Question λειτουργεί ως καλούπι. Καθορίζει ότι κάθε ερώτηση πρέπει να έχει συγκεκριμένα πεδία, όπως κωδικό (id) και κείμενο (text). Αν λείπει κάποιο στοιχείο, το σύστημα ειδοποιεί τον προγραμματιστή πριν τρέξει η εφαρμογή. Αυτό εξασφαλίζει τη σταθερότητα του συστήματος.[11]

Ο αυστηρός ορισμός των δομών δεδομένων δεν αποτελεί μόνο ζήτημα καλής πρακτικής προγραμματισμού, αλλά και κρίσιμο παράγοντα για τη νομική αξιοπιστία του συστήματος. Λάθη στον χειρισμό των δεδομένων (π.χ. εσφαλμένος τύπος μεταβλητής, απώλεια πεδίων ή λανθασμένη αντιστοίχιση ερωτήσεων–απαντήσεων) μπορούν να οδηγήσουν σε ασυνεπείς ή ελλιπείς αναφορές DPIA, με άμεσες συνέπειες για τη συμμόρφωση. Με τη χρήση dataclasses και στατικών τύπων, οι δομές που αντιπροσωπεύουν ερωτήσεις, απαντήσεις, αποτελέσματα και πολιτικές καθίστανται ρητά ορισμένες, επιτρέποντας στον προγραμματιστή να εντοπίζει εγκαίρως ασυμβατότητες κατά τη φάση ανάπτυξης και δοκιμών.[11]



Εικόνα 13: Διαγραμμα προτύπων των ερωτήσεων

Κυριαρχία στο AI και ML: Η Python αποτελεί την de facto γλώσσα για την ανάπτυξη εφαρμογών Τεχνητής Νοημοσύνης. Η πληθώρα βιβλιοθηκών όπως το PyTorch και το TensorFlow επιτρέπει την άμεση ενσωμάτωση αλγορίθμων μηχανικής μάθησης [51]. Στην περίπτωσή μας, η συμβατότητα της Python με το οικοσύστημα των LLMs (Large Language Models) ήταν καθοριστική για τη διασύνδεση με το τοπικό μοντέλο Llama 3.

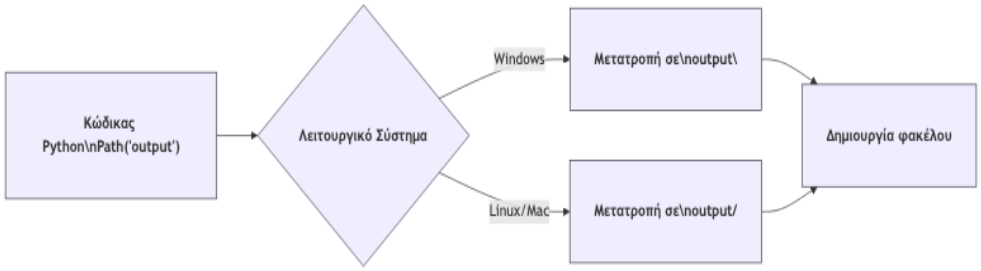
Αναγνωσιμότητα και Συντηρησιμότητα: Η σύνταξη της Python χαρακτηρίζεται από υψηλή αναγνωσιμότητα, γεγονός που μειώνει τον χρόνο ανάπτυξης και διευκολύνει τη συντήρηση του κώδικα (maintainability) [52]. Αυτό είναι ιδιαίτερα σημαντικό σε ακαδημαϊκά έργα όπου η καθαρότητα του κώδικα είναι προαπαιτούμενο.

Επεκτασιμότητα (Extensibility): Η δυνατότητα της Python να ενσωματώνει εύκολα scripts και modules (όπως το site_inspector.py για το web crawling) επέτρεψε την υλοποίηση πολύπλοκων λειτουργιών, όπως ο έλεγχος cookies, με ελάχιστες γραμμές κώδικα [53].

5.1.2 Διαχείρηση Συστήματος Αρχείων

Η εφαρμογή πρέπει να λειτουργεί σε κάθε υπολογιστή, είτε χρησιμοποιεί Windows είτε Linux. Τα λειτουργικά συστήματα διαχειρίζονται διαφορετικά τις διαδρομές των αρχείων. Για να λυθεί αυτό το ζήτημα, χρησιμοποιήθηκε η βιβλιοθήκη pathlib. Στο αρχείο config.py, ορίζουμε τους φακέλους εξόδου χρησιμοποιώντας την εντολή Path. Η Python αναλαμβάνει να μετατρέψει αυτόματα τη διαδρομή στη σωστή μορφή για το εκάστοτε λειτουργικό σύστημα. Αυτό καθιστά το λογισμικό "φορητό" (portable).

Ο αυστηρός ορισμός των δομών δεδομένων δεν αποτελεί μόνο ζήτημα καλής πρακτικής προγραμματισμού, αλλά και κρίσιμο παράγοντα για τη νομική αξιοπιστία του συστήματος. Λάθη στον χειρισμό των δεδομένων (π.χ. εσφαλμένος τύπος μεταβλητής, απώλεια πεδίων ή λανθασμένη αντιστοίχιση ερωτήσεων–απαντήσεων) μπορούν να οδηγήσουν σε ασυνεπείς ή ελλιπείς αναφορές DPIA, με άμεσες συνέπειες για τη συμμόρφωση. Με τη χρήση dataclasses και στατικών τύπων, οι δομές που αντιπροσωπεύουν ερωτήσεις, απαντήσεις, αποτελέσματα και πολιτικές καθίστανται ρητά ορισμένες, επιτρέποντας στον προγραμματιστή να εντοπίζει εγκαίρως ασυμβατότητες κατά τη φάση ανάπτυξης και δοκιμών.[53]



Εικόνα 14: Διαχείριση αρχείων Συστήματος

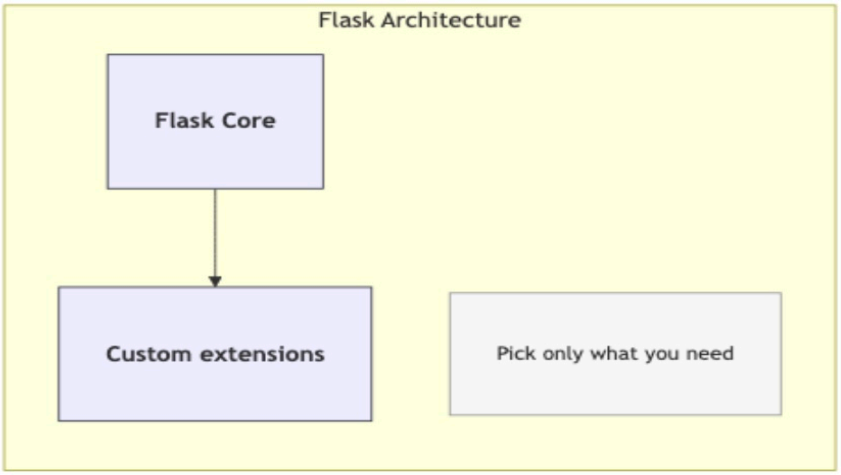
5.1.3 Πλαίσιο Ανάπτυξης Εφαρμογής : Flask cs Django

Για την ανάπτυξη της διαδικτυακής διεπαφής και του API εξετάστηκαν τα δύο επικρατέστερα πλαίσια της Python, το Django και το Flask, με κριτήριο όχι μόνο τη δημοφιλία τους αλλά και τον βαθμό στον οποίο εξυπηρετούν τον σκοπό μιας ελαφριάς, ελεγχόμενης εφαρμογής παραγωγής πολιτικής απορρήτου. Η τελική επιλογή του Flask ήταν συνειδητή και συνδέεται άμεσα με τις αρχές σχεδιασμού της εργασίας. Συγκεκριμένα, το Flask προσφέρει ένα «μικρό» και ευέλικτο πυρήνα (microframework), ο οποίος επιτρέπει στον προγραμματιστή να ορίσει ρητά τη ροή των δεδομένων από τη συλλογή εισροών έως την παραγωγή των τελικών εγγράφων, χωρίς να επιβάλλει έτοιμες, σύνθετες συμβάσεις και μηχανισμούς που συχνά συνοδεύουν πιο βαριά πλαίσια. Αυτό ήταν κρίσιμο για μια εφαρμογή που ενσωματώνει Local AI και επεξεργάζεται δυνητικά ευαίσθητες πληροφορίες:

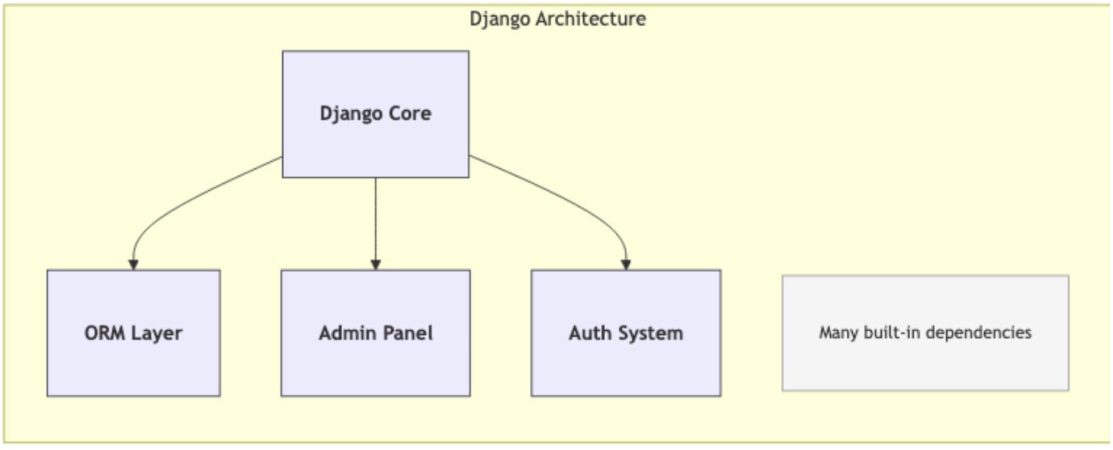
η απλότητα της στοίβας περιορίζει τις «αόρατες» διεργασίες, μειώνει την επιφάνεια επίθεσης και διευκολύνει την τεκμηρίωση των ροών επεξεργασίας. Επιπλέον, η ελαχιστοποίηση εξαρτήσεων δεν αποτέλεσε απλώς τεχνική προτίμηση, αλλά πρακτικό πλεονέκτημα για το κοινό-στόχο (MME), καθώς μειώνει την πολυπλοκότητα εγκατάστασης και συντήρησης και καθιστά πιο ρεαλιστική την εκτέλεση του συστήματος σε τυπικό hardware, χωρίς ανάγκη εκτεταμένης παραμετροποίησης.[53]

5.1.4 Μηχανισμός Αξιολόγησης (Assessment Engine)

Το Django ακολουθεί την προσέγγιση "batteries-included". Αυτό σημαίνει ότι παρέχει προεγκατεστημένα εργαλεία για τα πάντα: διαχείριση χρηστών, βάση δεδομένων και πίνακα διαχειριστή. Αυτό δημιουργεί ένα άκαμπτο πλαίσιο. Αντίθετα, το Flask είναι ένα μικρο-πλαίσιο (micro-framework). Παρέχει μόνο τα απολύτως απαραίτητα για να λειτουργήσει ένας διακομιστής (web server). Αφήνει την αρχιτεκτονική ευθύνη στον προγραμματιστή. Στην περίπτωσή μας, θέλαμε να αποφύγουμε την πολυπλοκότητα του Django, καθώς η εφαρμογή λειτουργεί ως "γέφυρα" μεταξύ των αρχείων JSON και του μοντέλου AI.



Εικόνα 15: Συγκριτική Ανάλυση Αρχιτεκτονικής (Παράδειγμα Flask)



Εικόνα 16: Συγκριτική Ανάλυση Αρχιτεκτονικής (Παράδειγμα Django)

Στο πλαίσιο της συγκεκριμένης εργασίας, ο έλεγχος της ροής των δεδομένων και η διαφάνεια της αρχιτεκτονικής ήταν σημαντικότεροι από την ύπαρξη ενός έτοιμου οικοσυστήματος πρόσθετων

λειτουργιών. Το Flask επέτρεψε την κατασκευή μιας ελαφριάς, προσαρμοσμένης εφαρμογής, στην οποία κάθε route και κάθε σημείο πρόσβασης είναι ρητά ορισμένο στον κώδικα, διευκολύνοντας την τεκμηρίωση και τον έλεγχο ασφαλείας. Αντί να προσαρμοστεί το πρόβλημα στις προδιαγραφές ενός «βαριού» framework, η επιλογή του Flask επέτρεψε την κατασκευή ενός framework «γύρω από το πρόβλημα», στοιχείο που είναι κρίσιμο όταν ο στόχος είναι η υλοποίηση ενός ερευνητικού πρωτοτύπου (research prototype) με αυξημένες απαιτήσεις διαφάνειας.

5.2 Μηχανική Τεχνητής Νοημοσύνης: Ollama & Llama 3

Η καρδιά του συστήματος είναι η μηχανή παραγωγής φυσικής γλώσσας. Αντί της χρήσης cloud APIs (όπως το OpenAI GPT-4), επιλέχθηκε η τοπική εκτέλεση μοντέλων για λόγους συμμόρφωσης με τον GDPR.[53]

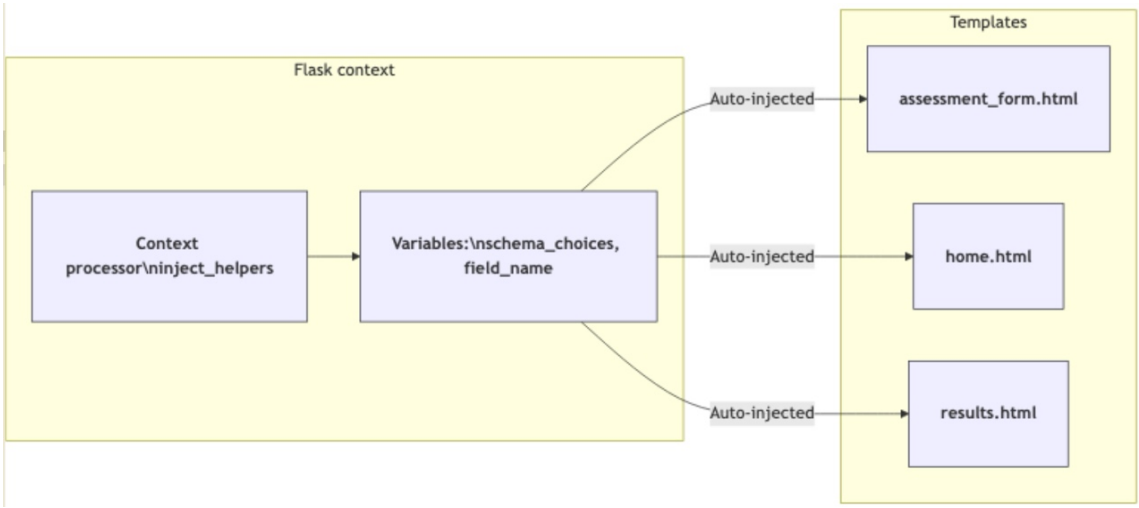
Η τεχνολογία Ollama λειτουργεί ως ενδιάμεσο επίπεδο (middleware) ανάμεσα στην εφαρμογή Flask και στο ίδιο το γλωσσικό μοντέλο, προσφέροντας ένα απλό και ελεγχόμενο API για την υποβολή prompts και τη λήψη απαντήσεων. Η αρχιτεκτονική αυτή επιτρέπει την αντικατάσταση ή την αναβάθμιση του υποκείμενου μοντέλου (π.χ. χρήση διαφορετικών παραλλαγών του Llama 3 ή άλλων ανοικτών LLMs) χωρίς αλλαγές στον κώδικα της web εφαρμογής. Επιπλέον, η τοπική εκτέλεση σημαίνει ότι οι κλήσεις προς το LLM δεν εξαρτώνται από την διαθεσιμότητα εξωτερικών υπηρεσιών, αυξάνοντας την ανθεκτικότητα του συστήματος και επιτρέποντας τη λειτουργία του ακόμη και σε απομονωμένα περιβάλλοντα (air-gapped networks), όπως αυτά που απαιτούνται σε ορισμένες περιπτώσεις από πολιτικές ασφάλειας πληροφοριών.[53]

Ollama: Πρόκειται για ένα εργαλείο ανοιχτού κώδικα που επιτρέπει την τοπική εκτέλεση LLMs σε προσωπικούς υπολογιστές. Το Ollama αναλαμβάνει τη διαχείριση των πόρων του συστήματος (CPU/GPU) και παρέχει ένα REST API για την επικοινωνία με την Python εφαρμογή [54]. Η χρήση του διασφαλίζει ότι κανένα δεδομένο δεν εγκαταλείπει την υποδομή του οργανισμού, ικανοποιώντας την απαίτηση για εμπιστευτικότητα [55].

Llama 3 (Meta AI): Χρησιμοποιήθηκε το μοντέλο Llama 3 8B (8 δισεκατομμύρια παράμετροι). Πρόκειται για ένα μοντέλο αρχιτεκτονικής Transformer [56], το οποίο έχει εκπαιδευτεί σε τεράστιο όγκο δεδομένων και έχει βελτιστοποιηθεί για την κατανόηση και παραγωγή κειμένου. Η έκδοση 8B επιλέχθηκε λόγω της ισορροπίας μεταξύ ακρίβειας και απαιτήσεων υλικού, επιτρέποντας την εκτέλεση σε τυπικούς υπολογιστές γραφείου χωρίς την ανάγκη εξειδικευμένων καρτών γραφικών (Data Center GPUs) [57].

5.2.1 Δυναμική Κατασκευή Διεπαφής (Context Processors)

Η διεπαφή του χρήστη με το Ollama και έπειτα ε το Llama 3 8B χρειάζεται δυναμικά στοιχεία σε κάθε σελίδα, όπως το μενού επιλογών. Το Django χρησιμοποιεί πολύπλοκους μηχανισμούς (Template Tags). Το Flask προσφέρει μια πιο άμεση λύση: τους context_processors. Στο app.py, χρησιμοποιήσαμε τη συνάρτηση inject_helpers. Αυτή η συνάρτηση στέλνει αυτόματα δεδομένα, όπως τις επιλογές του μενού (schema_choices), σε όλα τα πρότυπα HTML. Έτσι, ο κώδικας παραμένει καθαρός και συντηρήσιμος, καθώς η λογική της διεπαφής διαχωρίζεται από τη λογική των δεδομένων.[57]



Εικόνα 17: Λογική Context proccesors

Η τεχνολογία Ollama λειτουργεί ως ενδιάμεσο επίπεδο (middleware) ανάμεσα στην εφαρμογή Flask και στο ίδιο το γλωσσικό μοντέλο, προσφέροντας ένα απλό και ελεγχόμενο API για την υποβολή prompts και τη λήψη απαντήσεων. Η αρχιτεκτονική αυτή επιτρέπει την αντικατάσταση ή την αναβάθμιση του υποκείμενου μοντέλου (π.χ. χρήση διαφορετικών παραλλαγών του Llama 3 ή άλλων ανοικτών LLMs) χωρίς αλλαγές στον κώδικα της web εφαρμογής. Επιπλέον, η τοπική εκτέλεση σημαίνει ότι οι κλήσεις προς το LLM δεν εξαρτώνται από την διαθεσιμότητα εξωτερικών υπηρεσιών, αυξάνοντας την ανθεκτικότητα του συστήματος και επιτρέποντας τη λειτουργία του ακόμη και σε απομονωμένα περιβάλλοντα (air-gapped networks), όπως αυτά που απαιτούνται σε ορισμένες περιπτώσεις από πολιτικές ασφάλειας πληροφοριών.[57]

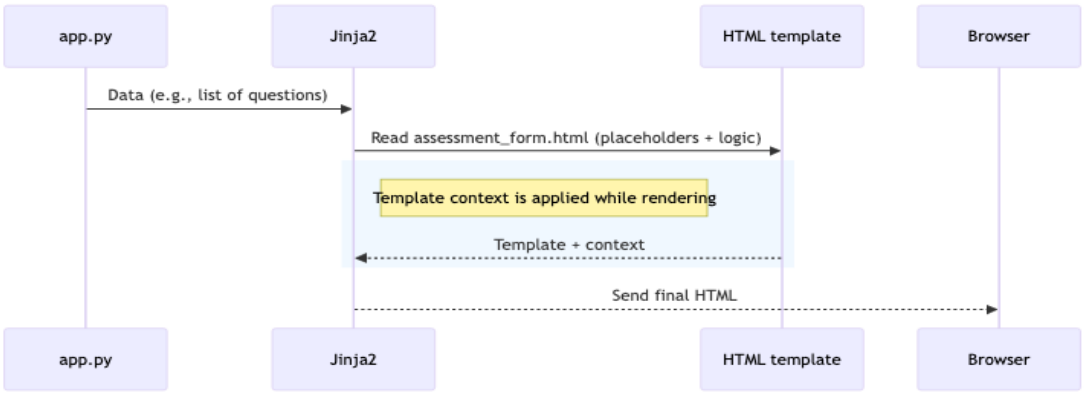
5.3 Τεχνολογίες Διεπαφής (Frontend) και Templating

Η διεπαφή χρήστη (User Interface – UI) αποτελεί το σημείο επαφής του ανθρώπου με τη μηχανή. Στον "GDPR ASSESSOR", ο σχεδιασμός της διεπαφής δεν αφορούσε μόνο την αισθητική. Στόχος ήταν η δημιουργία ενός λειτουργικού περιβάλλοντος που καθοδηγεί τον χρήστη, ακόμα και αν δεν διαθέτει εξειδικευμένες τεχνικές γνώσεις. Για την επίτευξη αυτού του στόχου, χρησιμοποιήθηκε ένας συνδυασμός σταθερών προτύπων ιστού και δυναμικής επεξεργασίας από την πλευρά του διακομιστή.[57]

Η τεχνολογία Ollama λειτουργεί ως ενδιάμεσο επίπεδο (middleware) ανάμεσα στην εφαρμογή Flask και στο ίδιο το γλωσσικό μοντέλο, προσφέροντας ένα απλό και ελεγχόμενο API για την υποβολή prompts και τη λήψη απαντήσεων. Η αρχιτεκτονική αυτή επιτρέπει την αντικατάσταση ή την αναβάθμιση του υποκείμενου μοντέλου (π.χ. χρήση διαφορετικών παραλλαγών του Llama 3 ή άλλων ανοικτών LLMs) χωρίς αλλαγές στον κώδικα της web εφαρμογής. Επιπλέον, η τοπική εκτέλεση σημαίνει ότι οι κλήσεις προς το LLM δεν εξαρτώνται από την διαθεσιμότητα εξωτερικών υπηρεσιών, αυξάνοντας την ανθεκτικότητα του συστήματος και επιτρέποντας τη λειτουργία του ακόμη και σε απομονωμένα περιβάλλοντα (air-gapped networks), όπως αυτά που απαιτούνται σε ορισμένες περιπτώσεις από πολιτικές ασφάλειας πληροφοριών.[57]

5.3.1 Δυναμική Σύνθεση Σελίδων (Jinja Templating)

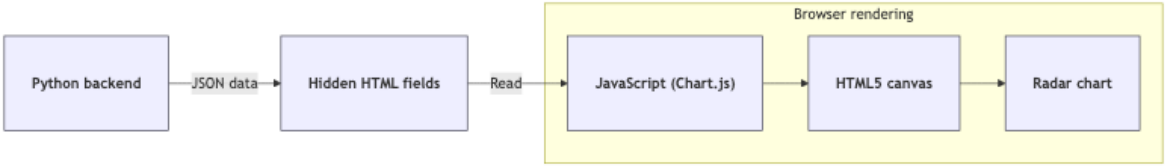
Η καρδιά της διεπαφής είναι η μηχανή προτύπων Jinja2. Το Flask δεν στέλνει έτοιμες, στατικές σελίδες HTML στον χρήστη. Αντίθετα, "συναρμολογεί" τις σελίδες εκείνη τη στιγμή. Στο αρχείο app.py, βλέπουμε εντολές όπως render_template("assessment_form.html", ...). Το Jinja2 επιτρέπει την εισαγωγή λογικής μέσα στο HTML. Για παράδειγμα, χρησιμοποιούμε βρόχους (for loops) για να εμφανίσουμε τις ερωτήσεις του DPIA μία προς μία. Χρησιμοποιούμε επίσης συνθήκες (if statements) για να κρύψουμε ή να εμφανίσουμε τμήματα της σελίδας ανάλογα με την πρόοδο του χρήστη. Αυτό καθιστά την εφαρμογή "ζωντανή" και προσαρμοστική.[57]



Εικόνα 18: Διαδρομή σύνθεσης σελίδας

5.3.2 Οπτικοποίηση Δεδομένων (Chart.js)(Ανάλυση όλων των Διαγραμμάτων)

Μια εικόνα αξίζει όσο χίλιες λέξεις, ειδικά όταν πρόκειται για πολύπλοκα δεδομένα συμμόρφωσης. Για την παρουσίαση των αποτελεσμάτων, επιλέχθηκε η βιβλιοθήκη JavaScript Chart.js. Στη σελίδα των αποτελεσμάτων (results.html), τα δεδομένα δεν παρουσιάζονται μόνο ως αριθμοί. Μετατρέπονται σε διαδραστικά γραφήματα. Συγκεκριμένα, χρησιμοποιούνται διάφορα διαγράμματα τα οποία ακολουθούν παρόμοια λογική με το διάγραμμα τύπου "Radar" (Ραντάρ) το οποίο αναλύεται και στο παρακάτω διάγραμμα (5.4.2). Αυτό επιτρέπει στον DPO να δει με μια ματιά την ισορροπία μεταξύ διαφορετικών τομέων, όπως η Ασφάλεια και τα Δικαιώματα Υποκειμένων. Η επεξεργασία γίνεται στον φυλλομετρητή του χρήστη (client-side), ελαφρύνοντας τον φόρτο του διακομιστή.

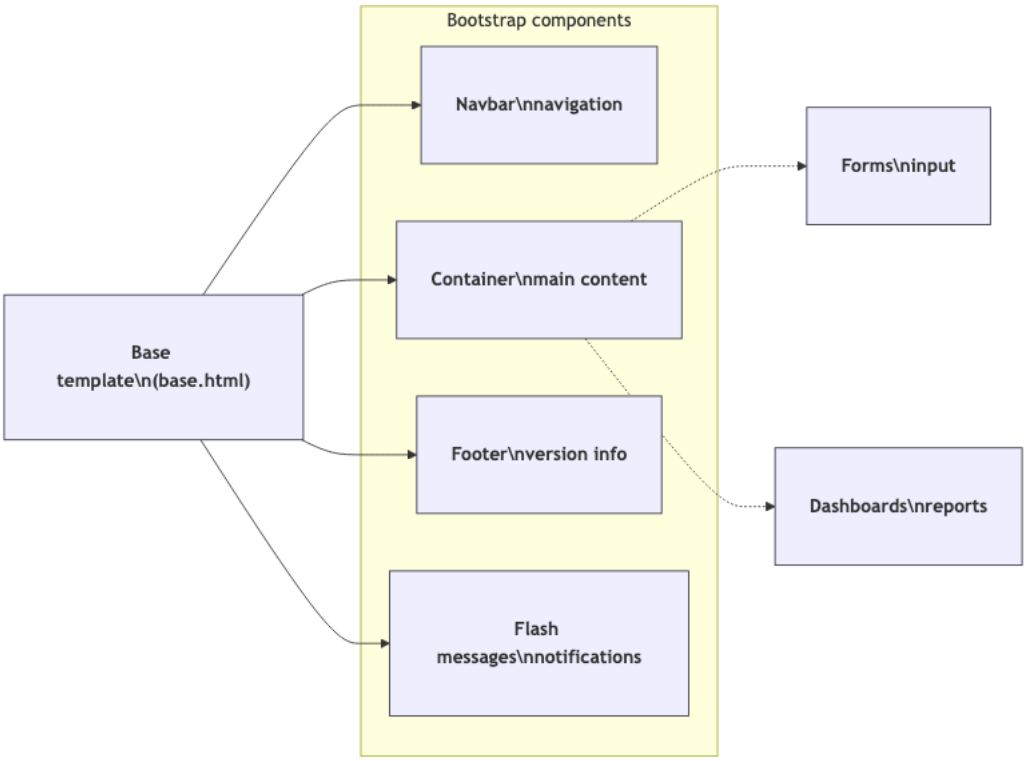


Εικόνα 19: Διαδρομή δεδομένων πριν τη σύνθεση της σελίδας

5.3.3 Σχεδιαστική Συνέπεια και Προσαρμοστικότητα (CSS & Bootstrap)

Η εμφάνιση της εφαρμογής πρέπει να είναι καθαρή και επαγγελματική. Για τον σκοπό αυτό, χρησιμοποιήθηκε το πλαίσιο Bootstrap. Το Bootstrap παρέχει ένα σύστημα "πλέγματος" (grid system). Αυτό διασφαλίζει ότι η εφαρμογή φαίνεται σωστά σε οθόνες διαφορετικών διαστάσεων (Responsive Design). Είτε ο χρήστης εργάζεται σε μεγάλο monitor γραφείου είτε σε laptop, τα

στοιχεία της φόρμας και τα κουμπιά προσαρμόζονται αυτόματα. Επιπλέον, χρησιμοποιήθηκαν πρότυπα CSS για τη δημιουργία μιας οπτικής ταυτότητας που εμπνέει εμπιστοσύνη, χρησιμοποιώντας ουδέτερα χρώματα και ευανάγνωστες γραμματοσειρές, κατάλληλα για εταιρικό περιβάλλον.



Εικόνα 20: Διάγραμμα Προσαρμοστικότητας σύνθεσης της σελίδας

Η χρήση της βιβλιοθήκης Chart.js για την οπτικοποίηση των αποτελεσμάτων προσφέρει μια ισορροπία ανάμεσα στην απλότητα υλοποίησης και στην εκφραστική δύναμη των διαγραμμάτων. Τα radar charts, οι πίνακες κινδύνου και τα διαγράμματα συσχέτισης επιτρέπουν στον DPO να αντιληφθεί γρήγορα τις περιοχές αυξημένου ρίσκου και να ιεραρχήσει τις ενέργειες συμμόρφωσης. Από τεχνικής πλευράς, η επιλογή client-side οπτικοποίησης σημαίνει ότι ο διακομιστής αποστέλλει μόνο τα επεξεργασμένα δεδομένα, αφήνοντας τη δουλειά της γραφικής απόδοσης στο πρόγραμμα περιήγησης. Αυτό μειώνει το φόρτο του server και διευκολύνει την μελλοντική προσαρμογή ή αντικατάσταση των γραφημάτων χωρίς αλλαγές στον πυρήνα της εφαρμογής.

5.4 Αποθήκευση Δεδομένων: JSON (NoSQL Approach)

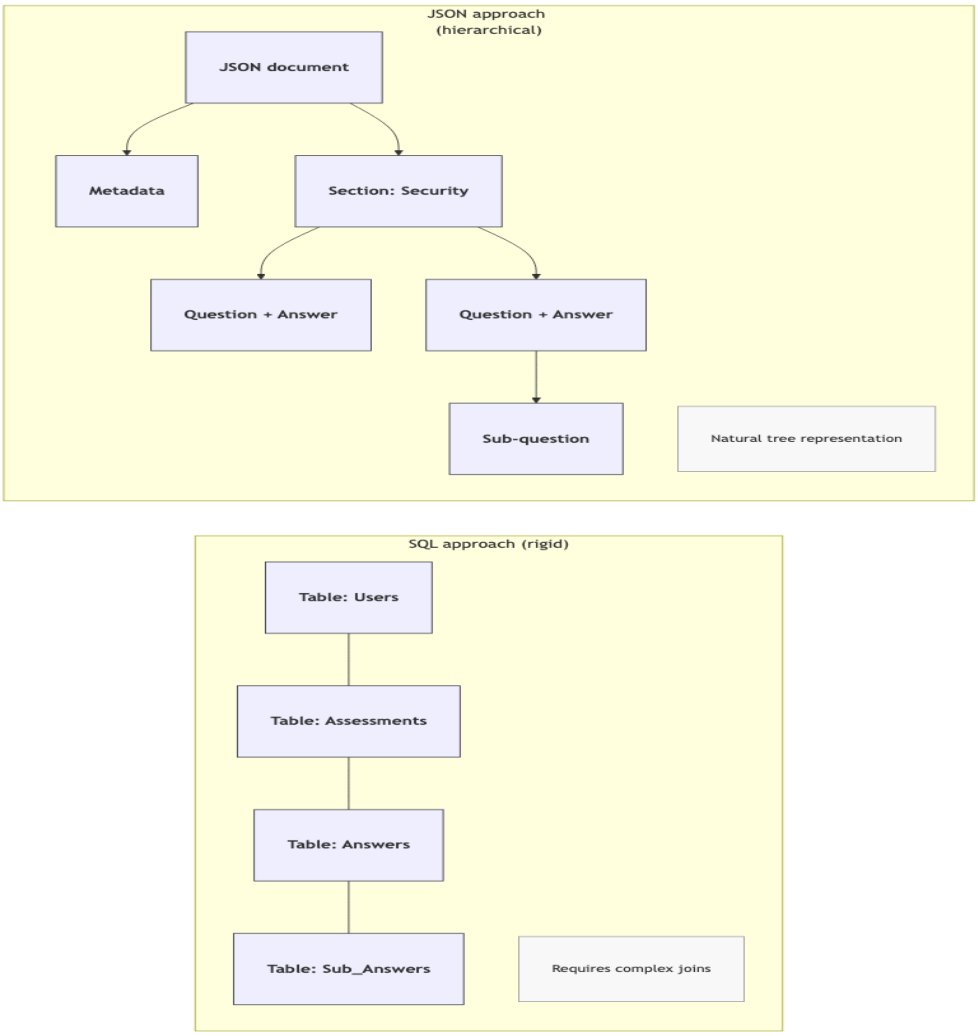
Για το επίπεδο αποθήκευσης δεδομένων (Persistence Layer), το σύστημα "GDPR ASSESSOR" απορρίπτει το παραδοσιακό μοντέλο των Σχεσιακών Βάσεων Δεδομένων (RDBMS), όπως η MySQL ή η PostgreSQL. Αντ' αυτού, υιοθετεί μια αρχιτεκτονική βασισμένη σε έγγραφα (Document-Oriented), χρησιμοποιώντας το πρότυπο JSON (JavaScript Object Notation). Αυτή η απόφαση δεν ελήφθη για λόγους ευκολίας, αλλά για να εξυπηρετήσει την ιεραρχική φύση των δεδομένων αξιολόγησης και τις απαιτήσεις φορητότητας του GDPR.[57]

Η επιλογή χρήσης JSON ως πρωτεύοντος μέσου αποθήκευσης δεδομένων συνδέεται τόσο με τεχνικούς όσο και με ρυθμιστικούς παράγοντες. Σε τεχνικό επίπεδο, η NoSQL προσέγγιση επιτρέπει την αποθήκευση ετερογενών δομών δεδομένων (schemas, απαντήσεις, πολιτικές, logs)

χωρίς την ανάγκη περίπλοκης σχεδίασης σχεσιακού σχήματος. Αυτό είναι ιδιαίτερα χρήσιμο σε ένα ερευνητικό έργο, όπου τα ερωτηματολόγια και οι δομές ενδέχεται να αλλάξουν πολλές φορές. Σε ρυθμιστικό επίπεδο, η αποθήκευση σε απλά αρχεία JSON διευκολύνει την εξαγωγή δεδομένων για τις ανάγκες άσκησης δικαιωμάτων από τα υποκείμενα (π.χ. δικαίωμα πρόσβασης) και ενισχύει τη διαφάνεια, αφού τα δεδομένα είναι αναγνώσιμα και επιθεωρήσιμα χωρίς εξειδικευμένα εργαλεία βάσεων δεδομένων.[57]

5.4.1 Ιεραρχική Δομή και Ευελιξία Σχήματος

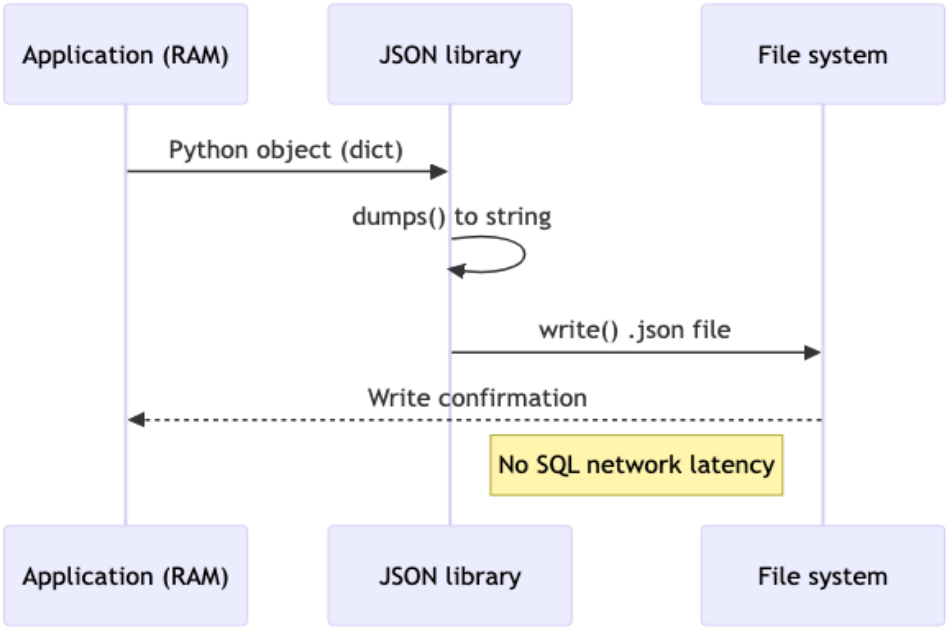
Τα δεδομένα μιας Εκτίμησης Αντικτύπου (DPIA) δεν είναι επίπεδα. Είναι δενδρικά. Μια ερώτηση μπορεί να έχει υπο-ερωτήσεις, οι οποίες εμφανίζονται μόνο αν πληρούνται συγκεκριμένες συνθήκες. Σε μια βάση SQL, η αποθήκευση τέτοιων δεδομένων θα απαιτούσε πολύπλοκες συνδέσεις πινάκων (Joins). Με το JSON, αποθηκεύουμε ολόκληρη τη δομή σε ένα αρχείο. Στο αρχείο gdpr_wizard.py, η κλάση SchemaBundle φορτώνει απευθείας αυτή τη δομή. Αν αύριο η Αρχή Προστασίας Δεδομένων αλλάξει το ερωτηματολόγιο, δεν χρειάζεται να αλλάξουμε τη δομή της βάσης (Schema Migration). Απλώς ενημερώνουμε το αρχείο JSON.[57]



Εικόνα 21: Σύγκριση Μοντέλων Δεδομένων json/sql

5.4.2 Σειριοποίηση και Επιδόσης (Serialization)

Η Python διαθέτει ενσωματωμένη υποστήριξη για JSON, γεγονός που καθιστά την επεξεργασία εξαιρετικά γρήγορη. Στο αρχείο app.py, η λειτουργία export_assessment χρησιμοποιεί τη βιβλιοθήκη json για να μετατρέψει τα αντικείμενα της μνήμης σε κείμενο (serialization) και το αντίστροφο. Επειδή δεν υπάρχει μεσολάβηση διακομιστή βάσης δεδομένων (Database Server overhead), η ανάγνωση και εγγραφή γίνονται σχεδόν ακαριαία. Τα δεδομένα γράφονται απευθείας στον δίσκο, στους φακέλους που ορίζονται στο config.py (όπως το OUTPUT_BASE), εξασφαλίζοντας την άμεση διαθεσιμότητά τους.[57]



Εικόνα 22: Ροή Εγγραφής Δεδομένων

5.5 Περιβάλλον Ανάπτυξης και Διαχείριση Κώδικα

- **Visual Studio Code** (VS Code): Χρησιμοποιήθηκε ως το κύριο περιβάλλον ανάπτυξης (IDE), λόγω της εξαιρετικής υποστήριξης για Python και των εργαλείων debugging.
- **Git & GitHub:** Η χρήση του Git επέτρεψε την καταγραφή της ιστορικότητας των αλλαγών (commits).

Συνοψίζοντας, η επιλογή των εργαλείων έγινε με γνώμονα τη δημιουργία ενός συστήματος που είναι ασφαλές (Local AI), ευέλικτο (Flask, JSON) και βιώσιμο (Python Ecosystem), καλύπτοντας πλήρως τις απαιτήσεις μιας σύγχρονης λύσης κανονιστικής συμμόρφωσης.

5.6 Σύνοψη Κεφαλαίου

Στο κεφάλαιο αυτό παρουσιάστηκαν τα βασικά εργαλεία και οι τεχνολογίες που αξιοποιεί το «GDPR ASSESSOR» για να υλοποιήσει τις λειτουργικές και μη λειτουργικές απαιτήσεις που τέθηκαν στα προηγούμενα κεφάλαια. Η Python και το Flask αποτέλεσαν τον πυρήνα της εφαρμογής, προσφέροντας ευελιξία, διαφάνεια και δυνατότητα τοπικής ανάπτυξης. Η χρήση του

Ollama και του Llama 3 επέτρεψε την υλοποίηση μιας μηχανής παραγωγικής συμμόρφωσης (Generative Compliance) με σεβασμό στην ιδιωτικότητα, ενώ τα εργαλεία Jinja2 και Chart.js συνέβαλαν στη δημιουργία μιας δυναμικής, φιλικής προς τον χρήστη διεπαφής και στην αποτελεσματική οπτικοποίηση των αποτελεσμάτων. Τέλος, η επιλογή αποθήκευσης σε JSON και η προσεκτική διαχείριση του συστήματος αρχείων ενίσχυσαν την επεκτασιμότητα, τη συντηρησιμότητα και τη συμβατότητα του συστήματος με τις αρχές του GDPR.[57]

Συνδυαστικά, οι τεχνολογικές επιλογές του Κεφαλαίου 5 υποστηρίζουν άμεσα τα ερευνητικά ερωτήματα της εργασίας, προσφέροντας μια συγκεκριμένη, υλοποιημένη απάντηση στο πώς μπορεί να σχεδιαστεί ένα σύστημα που καθοδηγεί βήμα προς βήμα τη διαδικασία συμμόρφωσης και ενσωματώνει με ασφαλή τρόπο την τοπική τεχνητή νοημοσύνη στην παραγωγή πολιτικών.[57]

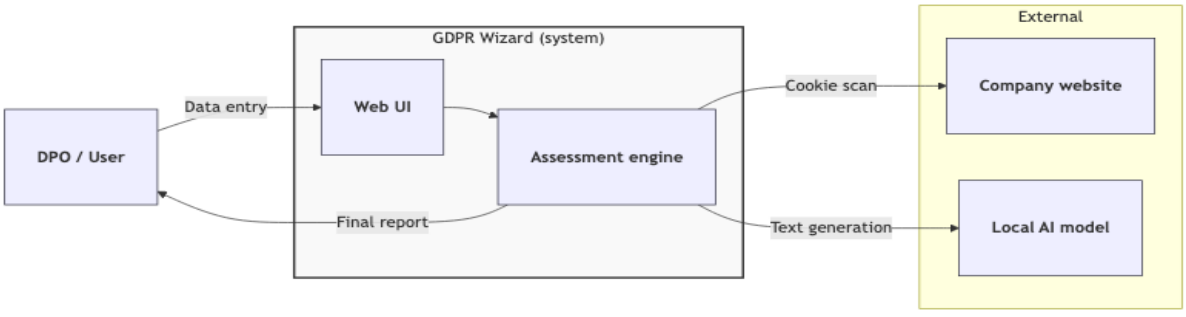
6 *Το Σύστημα*

Στο παρόν κεφάλαιο περιγράφεται η πρακτική υλοποίηση του πληροφοριακού συστήματος «GDPR ASSESSOR», όπως αυτή προκύπτει από τις αρχιτεκτονικές επιλογές και τα εργαλεία που παρουσιάστηκαν στα προηγούμενα κεφάλαια. Η ανάλυση εστιάζει στη λειτουργία των βασικών υποσυστημάτων (Κεντρικός Πίνακας Ελέγχου, Υποσύστημα Αξιολογήσεων DPIA/Gap, Μηχανισμός Ελέγχου Ιστοσελίδας, Ενότητα Αναλυτικών Στοιχείων και Μηχανισμός Παραγωγής Πολιτικών), δίνοντας έμφαση στη ροή των δεδομένων, στη συμπεριφορά του συστήματος από την πλευρά του χρήστη και στον τρόπο με τον οποίο υλοποιούνται στην πράξη οι στόχοι της παραγωγικής συμμόρφωσης (Generative Compliance).[57]

Ο κύριος στόχος του συστήματος είναι η υποστήριξη του Υπευθύνου Προστασίας Δεδομένων (DPO). Η συμμόρφωση με τον GDPR είναι συχνά μια χαοτική διαδικασία. Απαιτεί τη διαχείριση νομικών κειμένων, τεχνικών ελέγχων και διοικητικών εγγράφων. Το "GDPR ASSESSOR" ενοποιεί αυτές τις εργασίες σε μία πλατφόρμα. Λειτουργεί ως ένας "ψηφιακός συνεργάτης". Δεν καταγράφει απλώς πληροφορίες. Συμμετέχει ενεργά στη διαδικασία, εκτελώντας τεχνικούς ελέγχους και συντάσσοντας κείμενα μέσω Τεχνητής Νοημοσύνης.[57]

Η σχεδίαση του συστήματος εστίασε στην εμπειρία του χρήστη (User Experience). Η πολυπλοκότητα του κώδικα και των αλγορίθμων παραμένει "κρυφή" στο παρασκήνιο. Ο χρήστης αλληλεπιδρά με ένα καθαρό και φιλικό περιβάλλον. Αυτό επιτρέπει ακόμα και σε χρήστες χωρίς εξειδικευμένες τεχνικές γνώσεις να εκτελέσουν σύνθετους ελέγχους ασφαλείας και να παράγουν ολοκληρωμένες αναφορές συμμόρφωσης.

Για την καλύτερη κατανόηση της θέσης του συστήματος στο επιχειρησιακό περιβάλλον, παρατίθεται το ακόλουθο διάγραμμα πλαισίου.



Εικόνα 23: Ροή διεργασιών στο Επιχειρησιακό Περιβάλλον

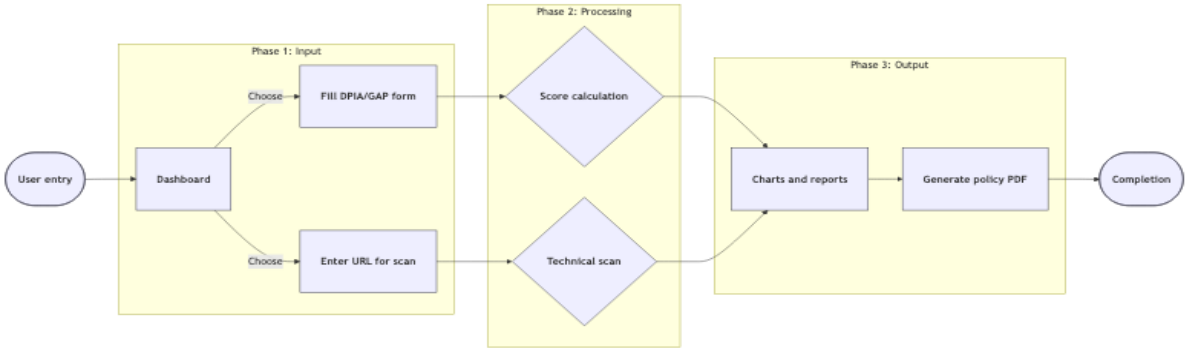
6.1 Επισκόπηση Ροής

Η εφαρμογή λειτουργεί ως μια διαδικτυακή πλατφόρμα (Web Application). Η δομή της είναι απλή και αυστηρά ιεραρχική. Στόχος του σχεδιασμού ήταν η αποφυγή πολύπλοκων μενού που αποπροσανατολίζουν τον χρήστη. Όλη η δραστηριότητα ξεκινά και καταλήγει σε ένα κεντρικό σημείο αναφοράς: τον Πίνακα Ελέγχου (Dashboard).

Η «καρδιά» της εφαρμογής, όπως ορίζεται στο αρχείο app.py, οργανώνει τη ροή εργασίας σε τρεις διακριτές φάσεις. Κάθε φάση εξυπηρετεί έναν συγκεκριμένο σκοπό στην αλυσίδα της συμμόρφωσης:

1. Φάση Εισαγωγής (Input): Ο χρήστης τροφοδοτεί το σύστημα με δεδομένα. Αυτό επιτυγχάνεται μέσω των διαδραστικών ερωτηματολογίων (για DPIA και Gap Analysis) ή μέσω της εισαγωγής URL για τον τεχνικό έλεγχο ιστοσελίδας.[57]
2. Φάση Επεξεργασίας (Processing): Το σύστημα αναλαμβάνει δράση στο παρασκήνιο. Υπολογίζει βαθμολογίες συμμόρφωσης, εντοπίζει κενά ασφαλείας και εκτελεί σαρώσεις για ιχνηλάτες (cookies).
3. Φάση Εξαγωγής (Output): Η διαδικασία ολοκληρώνεται με την παραγωγή αξίας για τον χρήστη. Το σύστημα συνθέτει τα ευρήματα σε οπτικά γραφήματα και παράγει αυτόματα τα τελικά νομικά κείμενα πολιτικής.[57]

Για την οπτική κατανόηση αυτής της διαδικασίας, ακολουθεί το διάγραμμα ροής ενεργειών του χρήστη.



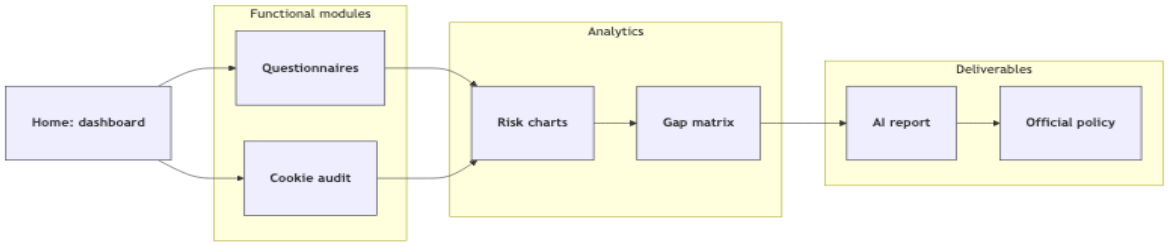
Εικόνα 24: Ροή Ενεργειών Χρήστη (User Action Flow)

6.1.1 Αρχιτεκτονική Πληροφορίας (Sitemap)

Η πλοήγηση μέσα στην εφαρμογή σχεδιάστηκε ώστε να είναι γραμμική. Ο χρήστης δεν χρειάζεται να μαντέψει το επόμενο βήμα. Οι διαδρομές (routes) του κώδικα στο app.py αντικατοπτρίζουν αυτή τη λογική.

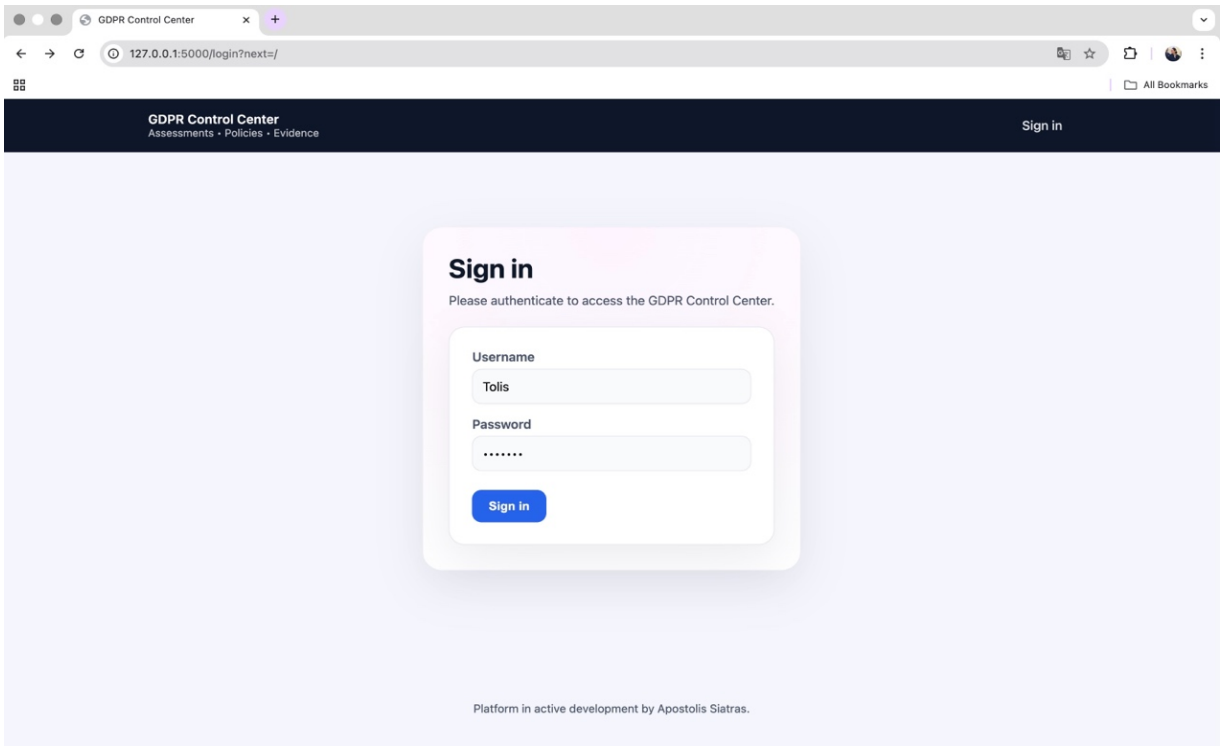
- **Dashboard (/):** Η σελίδα επισκόπησης. Ενημερώνει τον χρήστη για το ποσοστό ολοκλήρωσης των εργασιών.
- **Assessment (/assessment/<mode>): Ο** χώρος εργασίας. Εδώ ο χρήστης απαντά στις ερωτήσεις ανά θεματική ενότητα.
- **Results (/results):** Η σελίδα απολογισμού. Εδώ συγκεντρώνονται όλα τα ευρήματα.
- **Policy (/official-policy):** Το τελικό στάδιο. Εδώ γίνεται η σύνθεση του εγγράφου με τη βοήθεια της Τεχνητής Νοημοσύνης.

Το παρακάτω διάγραμμα χαρτογραφεί τις οθόνες της εφαρμογής και τον τρόπο που συνδέονται μεταξύ τους.



Εικόνα 25: Διάγραμμα διαμοιρασμού πληροφοριών προς τον χρήστη

Η πρώτη εντύπωση που αποκομίζει ο χρήστης από το σύστημα είναι η οθόνη εισόδου. Παρόλο που ο "GDPR ASSESOR σχεδιάστηκε για να λειτουργεί τοπικά (local deployment) ή σε εσωτερικό δίκτυο (intranet), η ασφάλεια της πρόσβασης δεν παραμελήθηκε. Τα δεδομένα που διαχειρίζεται το σύστημα, όπως οι ευπάθειες ασφαλείας μιας εταιρείας, είναι εμπιστευτικά. Επομένως, η ανεξέλεγκτη πρόσβαση θα αποτελούσε κίνδυνο.[57]



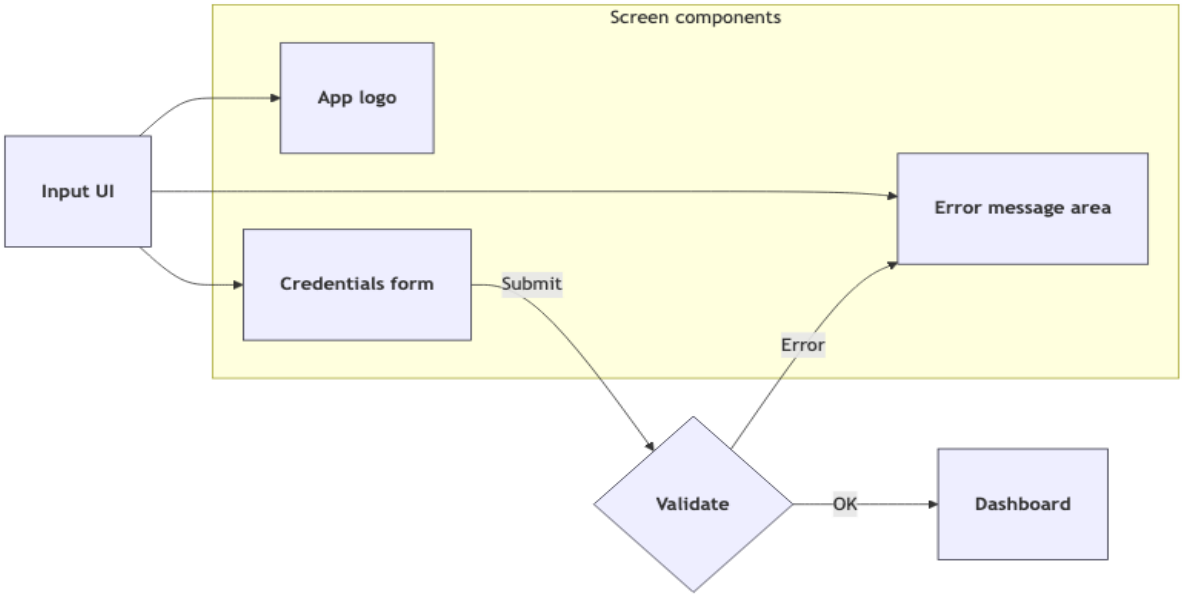
Εικόνα 26: Οθόνη Αυθεντικοποίησης

6.1.2 Μηχανισμός Αυθεντικοποίησης

Για την προστασία της εφαρμογής, υλοποιήθηκε ένας μηχανισμός ελέγχου ταυτότητας βασισμένος σε συνεδρίες (session-based authentication). Όπως φαίνεται στο αρχείο app.py, η διαδρομή /login διαχειρίζεται τη διαδικασία. Ο χρήστης καλείται να εισάγει ένα όνομα χρήστη και έναν κωδικό πρόσβασης.

6.1.3 Σχεδιασμός Διεπαφής

Η οθόνη εισόδου (login.html) σχεδιάστηκε λιτά, ώστε να μην αποσπά την προσοχή. Στο κέντρο δεσπόζει η φόρμα εισαγωγής στοιχείων. Χρησιμοποιήθηκαν ευδιάκριτα πεδία και ξεκάθαρα μηνύματα σφάλματος (π.χ. "Λανθασμένος κωδικός"). Στόχος ήταν η διαδικασία εισόδου να είναι γρήγορη και διαισθητική, επιτρέποντας στον DPO να προχωρήσει άμεσα στην εργασία του.



Εικόνα 27: Δομή Σελίδας Εισόδου

6.2 Κεντρικός Πίνακας Ελέγγου (Dashboard)

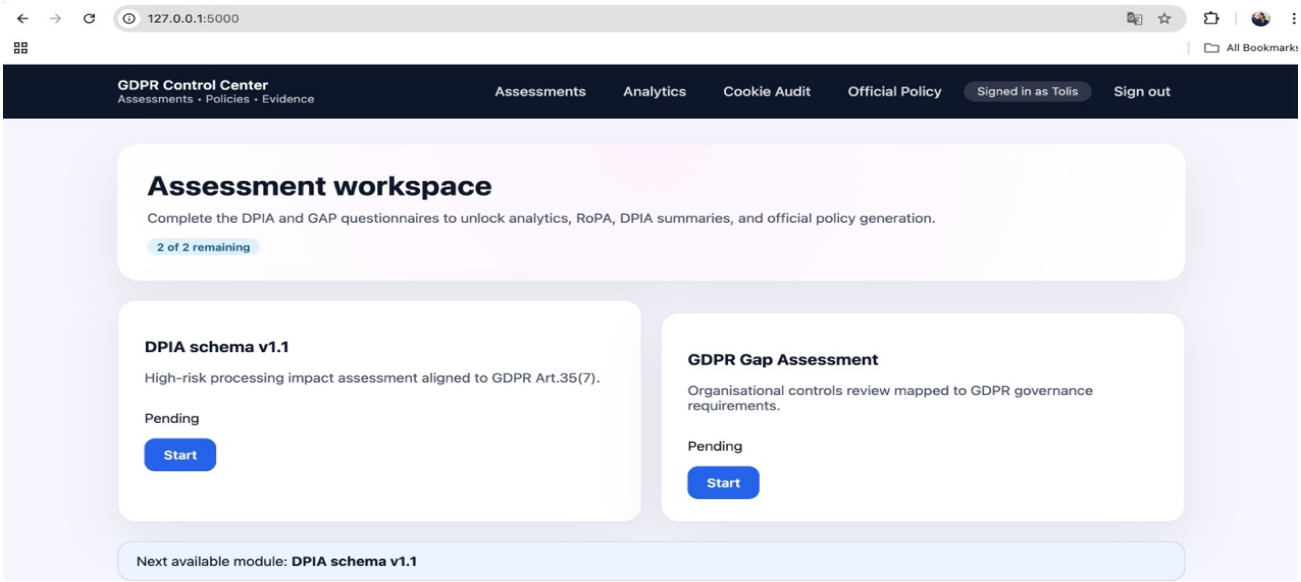
Μετά την επιτυχή είσοδο, ο χρήστης μεταφέρεται στον Κεντρικό Πίνακα Ελέγχου (Workspace). Αυτή η οθόνη αποτελεί το κέντρο επιχειρήσεων της εφαρμογής. Σχεδιάστηκε με γνώμονα την άμεση πληροφόρηση. Ο χρήστης δεν χρειάζεται να ψάξει για να βρει τι πρέπει να κάνει. Το σύστημα του παρουσιάζει μια συνοπτική εικόνα της κατάστασης συμμόρφωσης με μια ματιά.

Ο Κεντρικός Πίνακας Ελέγχου λειτουργεί ουσιαστικά ως «νοητικός χάρτης» της συμμόρφωσης του οργανισμού. Ο χρήστης δεν χρειάζεται να αναζητά ξεχωριστά τις επιμέρους λειτουργίες, αλλά βλέπει συγκεντρωμένα την πρόοδο και τα αποτελέσματα των αξιολογήσεων, τα ευρήματα από τους τεχνικούς ελέγχους και τις διαθέσιμες ενέργειες. Με τον τρόπο αυτό, το σύστημα υποστηρίζει την αρχή της διαφάνειας και της έγκαιρης ενημέρωσης, καθώς ο DPO μπορεί να εντοπίσει άμεσα τις περιοχές με τη χαμηλότερη βαθμολογία και να οργανώσει ανάλογα τις επόμενες ενέργειες συμμόρφωσης.

6.2.1 Δυναμικές Κάρτες Εργασιών (Task Cards)

Ο Πίνακας Ελέγχου δεν είναι μια στατική σελίδα. Προσαρμόζεται δυναμικά ανάλογα με την πρόοδο του χρήστη. Στο αρχείο app.py, η συνάρτηση home ελέγχει τη συνεδρία (session) για να δει ποιες αξιολογήσεις έχουν ολοκληρωθεί.

Βάσει αυτού του ελέγχου, η διεπαφή οργανώνεται σε "Κάρτες" (Cards). Κάθε κάρτα αντιστοιχεί σε μια λειτουργική ενότητα, όπως το DPIA ή το Gap Analysis. Οι κάρτες αλλάζουν κατάσταση αυτόματα.[57]



Εικόνα 28: Dashboard Πληροφοριακού Συστήματος

Όπως φαίνεται στην Εικόνα 2, το Dashboard περιλαμβάνει δυναμικές κάρτες (Cards) για κάθε διαθέσιμη αξιολόγηση. Κάθε κάρτα ενημερώνει τον χρήστη για το εάν έχει ολοκλήρωθεί και την τρέχουσα βαθμολογία (Score), για την άμεση αναγνώριση του επιπέδου κινδύνου. Αυτή η οπτική πληροφορία επιτρέπει την ιεράρχηση ενεργειών, εστιάζοντας πρώτα στους τομείς με τη χαμηλότερη ωριμότητα.

6.3 Υποσύστημα Αξιολογήσεων (DPIA & Gap Analysis)

Η καρδιά της εφαρμογής είναι ο μηχανισμός των ερωτηματολογίων. Εδώ ο χρήστης εισάγει τα δεδομένα που θα καθορίσουν το επίπεδο συμμόρφωσης του οργανισμού. Επιλέγοντας μια κάρτα από το Dashboard (π.χ. "DPIA schema v1.1"), ο χρήστης εισέρχεται στο περιβάλλον της αξιολόγησης.[57]

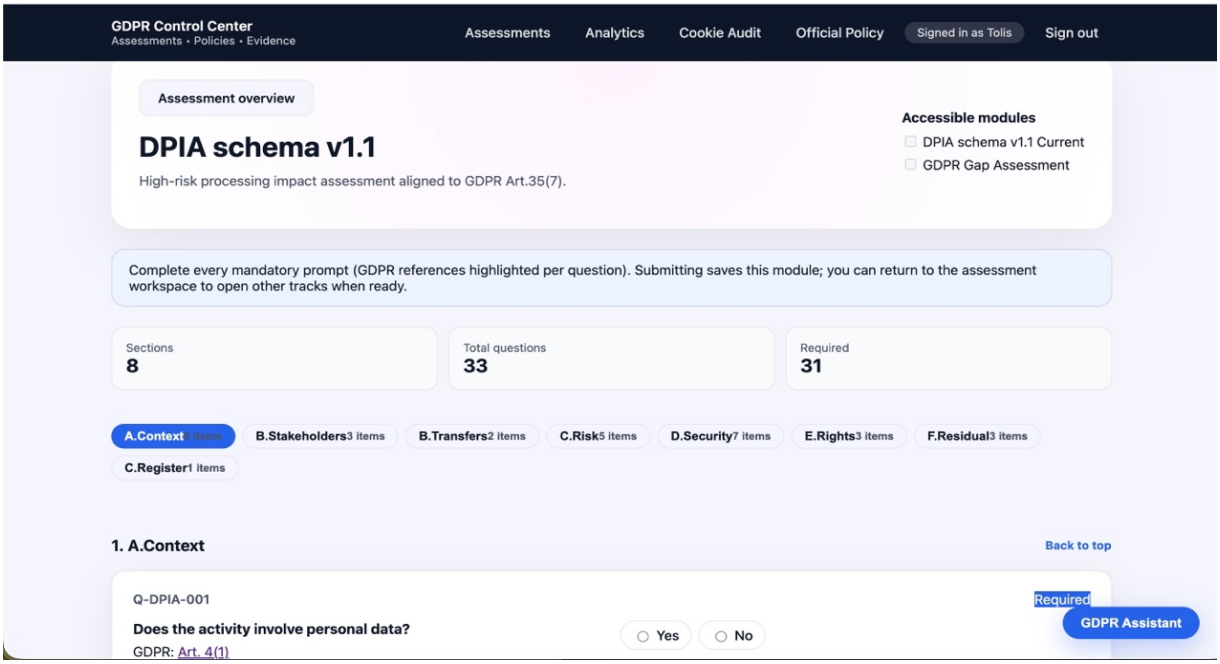
Αυτό το υποσύστημα δεν είναι μια απλή, στατική φόρμα HTML. Είναι ένας δυναμικός μηχανισμός που προσαρμόζεται σε πραγματικό χρόνο. Στηρίζεται στην κλάση SchemaBundle του αρχείου gdpr_wizard.py, η οποία φορτώνει τη δομή των ερωτήσεων από εξωτερικά αρχεία JSON. Αυτό σημαίνει ότι η λογική των ερωτήσεων είναι διαχωρισμένη από τον κώδικα της εφαρμογής, επιτρέποντας εύκολες ενημερώσεις όταν αλλάζει η νομοθεσία.[57]

6.3.1 Δυναμική Δομή και Λογική

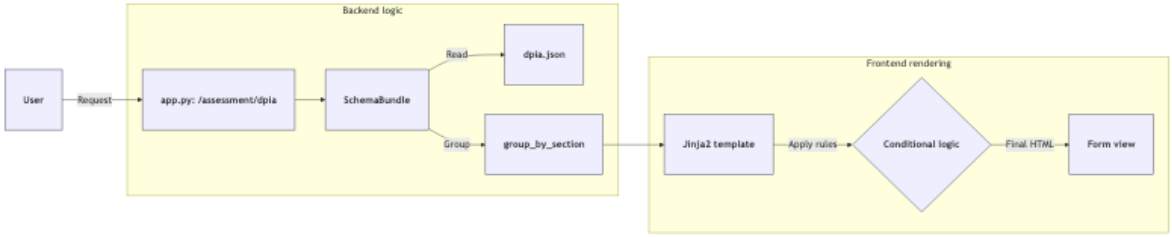
Το ερωτηματολόγιο "χτίζεται" δυναμικά τη στιγμή που το ζητάει ο χρήστης. Στο app.py, η συνάρτηση assessment_form ομαδοποιεί τις ερωτήσεις σε θεματικές ενότητες (Sections).

Χρησιμοποιώντας τη μηχανή προτύπων Jinja2, το σύστημα εφαρμόζει λογική εμφάνισης/απόκρυψης (Conditional Logic). Για παράδειγμα, αν ο χρήστης απαντήσει "Όχι" στην ερώτηση για χρήση νέων τεχνολογιών, οι επόμενες ερωτήσεις που αφορούν τεχνικές λεπτομέρειες

μπορεί να παραλειφθούν αυτόματα. Αυτό μειώνει τον κόπο συμπλήρωσης και εστιάζει την προσοχή στα ουσιώδη σημεία.



Εικόνα 29: Οθόνη χρήσης για αξιολόγηση βάση DPIA



Εικόνα 30:Ροή Δημιουργίας Ερωτηματολογίου

Κάθε ερώτηση συνοδεύεται από:

- Σαφή διατύπωση: Βασισμένη στο κείμενο του GDPR.
- Επεξηγηματικό Πλαίσιο (Context): Πεδίο όπου ο χρήστης μπορεί να προσθέσει σχόλια ή αποδεικτικά στοιχεία.
- Αναφορά Νομοθεσίας: Ετικέτες που συνδέουν την ερώτηση με συγκεκριμένα άρθρα του κανονισμού (π.χ. Art. 35(7)), ενισχύοντας τη διαφάνεια και την εκπαιδευτική αξία του εργαλείου.[57]

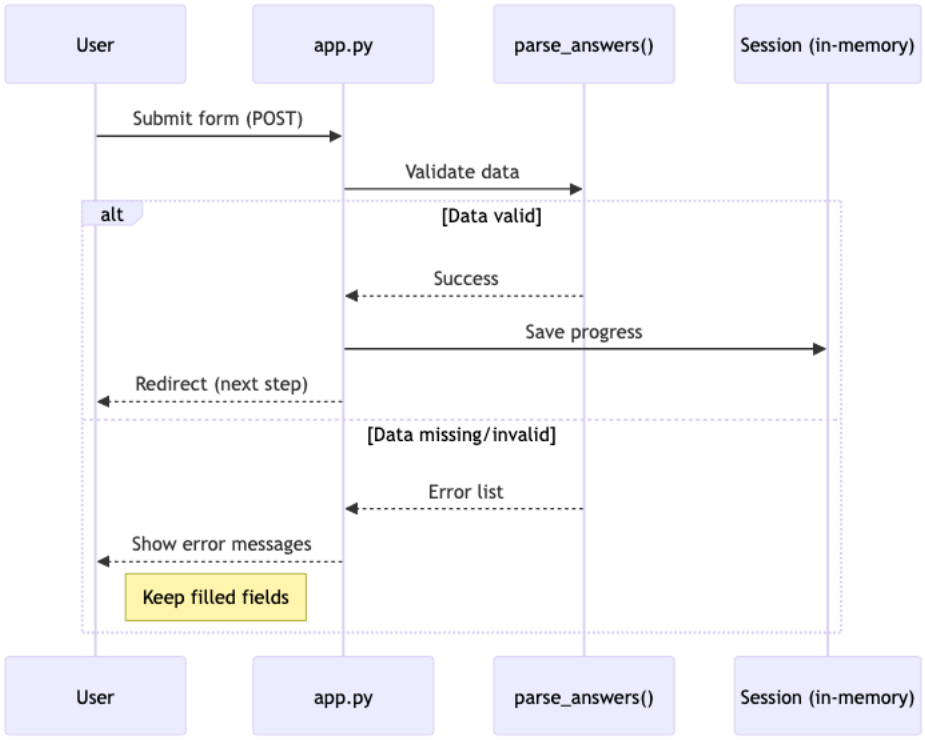
Μέσα από τον συνδυασμό δομημένων ερωτηματολογίων και δυναμικής απόδοσης, το υποσύστημα αξιολογήσεων λειτουργεί ως «γνωστικός οδηγός» για τον χρήστη. Αντί ο DPO να ξεκινά κάθε φορά από ένα κενό έγγραφο ή ένα γενικό πρότυπο, το σύστημα τον οδηγεί μέσα από μια αλληλουχία στοχευμένων ερωτήσεων, οι οποίες καλύπτουν τόσο νομικές απαιτήσεις όσο και τεχνικές και οργανωτικές πτυχές της επεξεργασίας. Η προσθήκη επεξηγηματικών πεδίων και αναφορών σε συγκεκριμένα άρθρα του GDPR βοηθά τον χρήστη να κατανοήσει το «γιατί» πίσω από κάθε ερώτηση, μετατρέποντας τη συμπλήρωση της φόρμας σε διαδικασία μάθησης και όχι απλώς σε τυπική υποχρέωση.[57]

6.3.2 Μηχανισμός Επικύρωσης και Αποθήκευσης (Validation & State)

Η ακεραιότητα των δεδομένων είναι κρίσιμη για τη σωστή παραγωγή των νομικών κειμένων. Το σύστημα δεν αποθηκεύει τυφλά ό,τι γράφει ο χρήστης. Στο αρχείο app.py, η συνάρτηση parse_answers εκτελεί αυστηρούς ελέγχους εγκυρότητας (Validation) κάθε φορά που ο χρήστης πατάει "Αποθήκευση" ή "Επόμενο".

Οι έλεγχοι περιλαμβάνουν:

- **Υποχρεωτικά Πεδία**: Ελέγχει αν έχουν απαντηθεί όλες οι κρίσιμες ερωτήσεις.
- **Έλεγχος Επιλογών:** Επιβεβαιώνει ότι οι απαντήσεις ανήκουν στις επιτρεπτές τιμές (q.enum), αποτρέποντας την παραποίηση των δεδομένων.
    - **Διαχείριση Κατάστασης (State):** Αν υπάρξουν λάθη, το σύστημα διατηρεί τις απαντήσεις που δόθηκαν σωστά (form_state), ώστε ο χρήστης να μην χρειαστεί να τα ξαναγράψει από την αρχή.

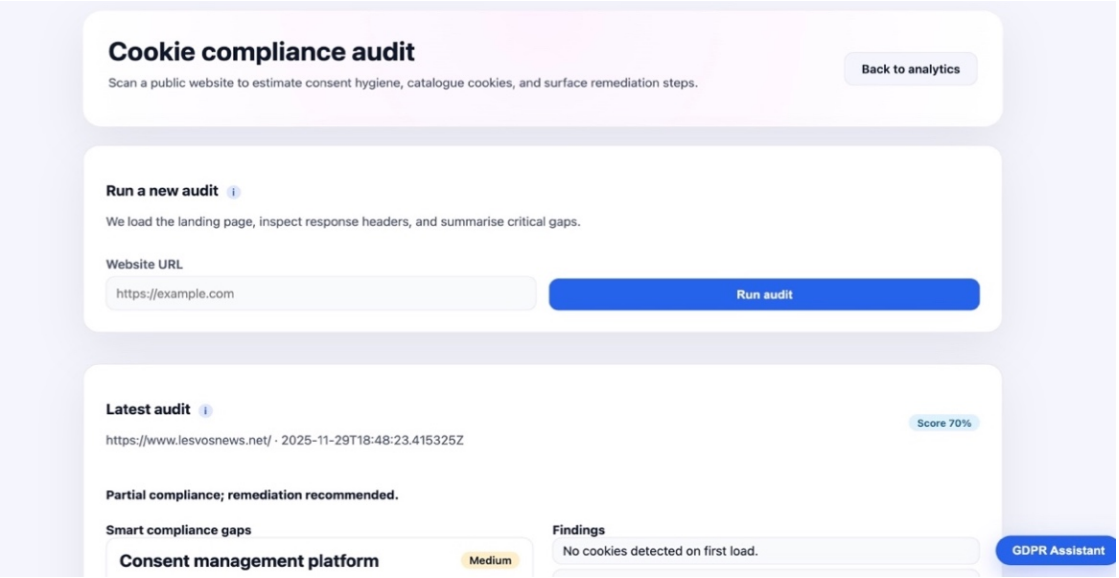


Εικόνα 31: Διαδικασία Υποβολής και Ελέγχου

6.4 Μηχανισμός Ελέγχου Ιστοσελίδας (Cookie Audit)

Ο Μηχανισμός Ελέγχου Ιστοσελίδας αποτελεί μια διακριτή λειτουργική μονάδα του συστήματος. Λειτουργεί συμπληρωματικά προς τα ερωτηματολόγια. Ενώ τα ερωτηματολόγια καταγράφουν τη "θεωρητική" συμμόρφωση (τι πιστεύει ο οργανισμός ότι κάνει), ο μηχανισμός ελέγχου εξετάζει την "πρακτική" εφαρμογή (τι συμβαίνει πραγματικά στον ιστότοπο).

Η υλοποίηση δεν βασίζεται σε πλήρη εξομοίωση προγράμματος περιήγησης (headless browser), καθώς κάτι τέτοιο θα αύξανε δραματικά τις απαιτήσεις πόρων. Αντ' αυτού, επιλέχθηκε η μέθοδος της Στατικής Ανάλυσης (Static Analysis). Το σύστημα ανακτά τον πηγαίο κώδικα και τις κεφαλίδες της ιστοσελίδας και τα εξετάζει βάσει προκαθορισμένων κανόνων.



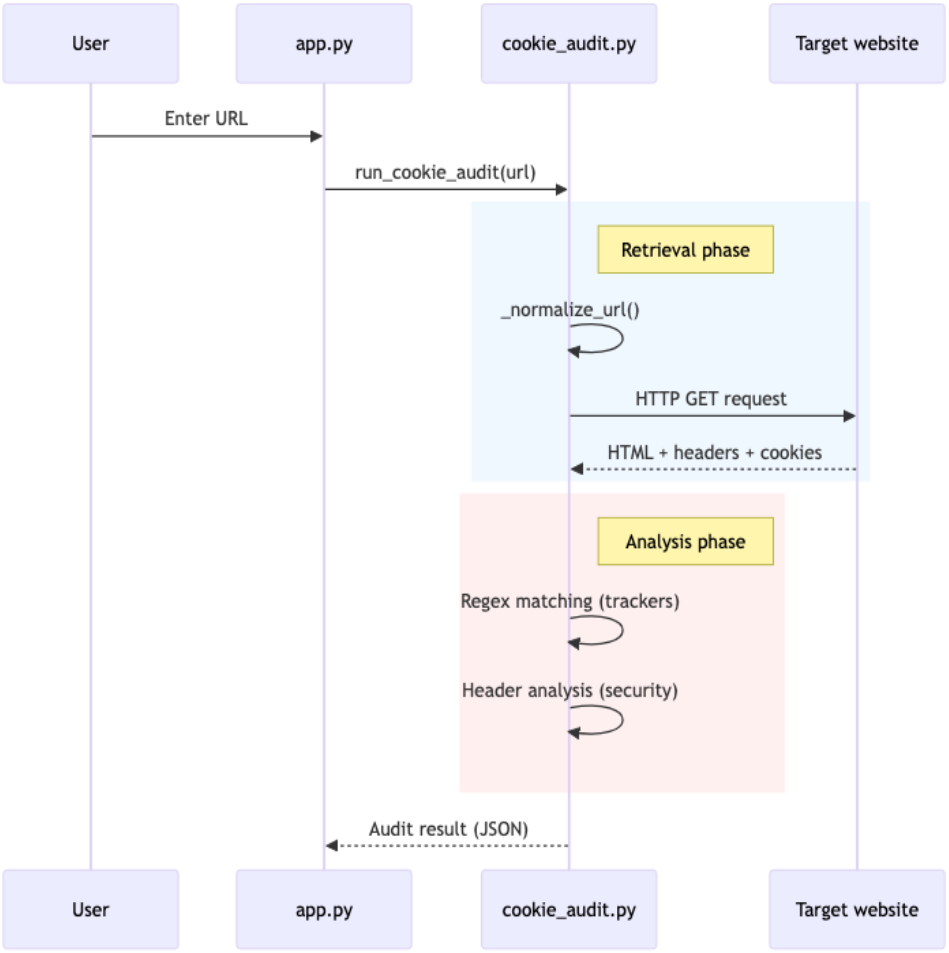
Εικόνα 32: Cookie Audit landing Page

6.4.1 Μηχανισμός Αξιολόγησης (Assessment Engine)

Η διαδικασία ξεκινά όταν ο χρήστης εισάγει ένα URL στη φόρμα ελέγχου. Το πρώτο βήμα είναι η εξασφάλιση ότι το URL είναι έγκυρο. Η συνάρτηση _normalize_url αναλαμβάνει να διορθώσει τη μορφή της διεύθυνσης, προσθέτοντας το πρωτόκολλο https:// εάν αυτό λείπει.

Στη συνέχεια, εκτελείται η ανάκτηση των δεδομένων μέσω της βιβλιοθήκης requests. Το σύστημα "κατεβάζει" το περιεχόμενο της σελίδας (response.text) και τα μεταδεδομένα της σύνδεσης (response.headers). Σε αυτό το στάδιο, καταγράφονται επίσης τα cookies που αποστέλλει ο διακομιστής πριν δώσει ο χρήστης τη συγκατάθεσή του, κάτι που αποτελεί κρίσιμη ένδειξη για την παραβίαση της αρχής "Privacy by Default".[57]

Ο μηχανισμός ελέγχου ιστοσελίδας έχει σχεδιαστεί ως ένα «ελαφρύ» εργαλείο πρώτου επιπέδου (first-level check), το οποίο δεν φιλοδοξεί να υποκαταστήσει εξειδικευμένα, εμπορικά scanners, αλλά να δώσει μια άμεση, προσανατολιστική εικόνα της πρακτικής συμμόρφωσης. Η στατική ανάλυση HTML και headers, παρότι δεν μπορεί να εντοπίσει όλα τα δυναμικά φορτωμένα cookies ή scripts, αρκεί για να αναδειχθούν προφανείς παραβάσεις της αρχής της συγκατάθεσης (π.χ. τοποθέτηση cookies πριν το banner). Η σαφής αποτύπωση των ορίων αυτής της προσέγγισης στην υλοποίηση είναι σημαντική, ώστε το εργαλείο να χρησιμοποιείται ως συμπληρωματικό βοήθημα και όχι ως μοναδικό σημείο αναφοράς για την αξιολόγηση της συμμόρφωσης ενός ιστότοπου.



Εικόνα 33: Ροή Εκτέλεσης Σάρωσης (cookie audit)

6.5 Αναλυτικά Στοιχεία και Οπτικοποίηση (Analytics)

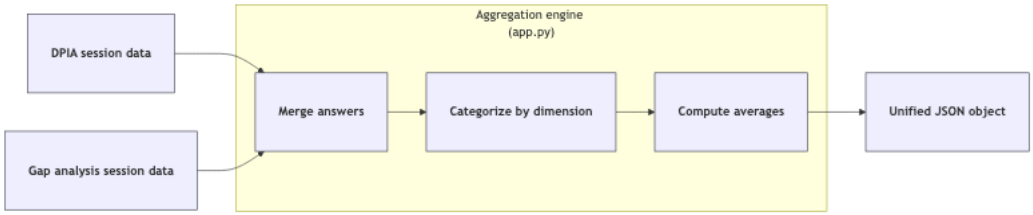
Η ενότητα των Αναλυτικών Στοιχείων αποτελεί το κέντρο λήψης αποφάσεων της εφαρμογής. Μόλις ολοκληρωθούν οι αξιολογήσεις (DPIA ή Gap Analysis), το σύστημα ενεργοποιεί τη μηχανή οπτικοποίησης. Η σελίδα αποτελεσμάτων (/results) δεν είναι μια στατική αναφορά. Είναι ένας διαδραστικός πίνακας που συνθέτει ποσοτικά και ποιοτικά δεδομένα.[57]

Η αρχιτεκτονική της οπτικοποίησης βασίζεται στην επεξεργασία των δεδομένων στον διακομιστή (Server-side processing) μέσω Python και την τελική απεικόνιση στον φυλλομετρητή (Client-side rendering) μέσω της βιβλιοθήκης Chart.js.

6.5.1 Μηχανισμός Συσχέτισης Δεδομένων (Data Aggregation)

Πριν παραχθεί οποιοδήποτε γράφημα, το σύστημα πρέπει να ενοποιήσει τα δεδομένα. Στο αρχείο app.py, η συνάρτηση combined_summary αναλαμβάνει αυτόν τον ρόλο. Αντλεί τα δεδομένα από τις συνεδρίες του DPIA και του Gap Analysis. Υπολογίζει τον μέσο όρο συμμόρφωσης και αθροίζει τα κενά ασφαλείας (Coverage Gaps).[57]

Επιπλέον, η συνάρτηση _collect_field_scores ομαδοποιεί τις ερωτήσεις σε έξι στρατηγικούς άξονες, όπως "Ασφάλεια", "Δικαιώματα" και "Διακυβέρνηση". Αυτή η κατηγοριοποίηση επιτρέπει τη σύγκριση διαφορετικών ερωτηματολογίων κάτω από κοινές θεματικές ομπρέλες.

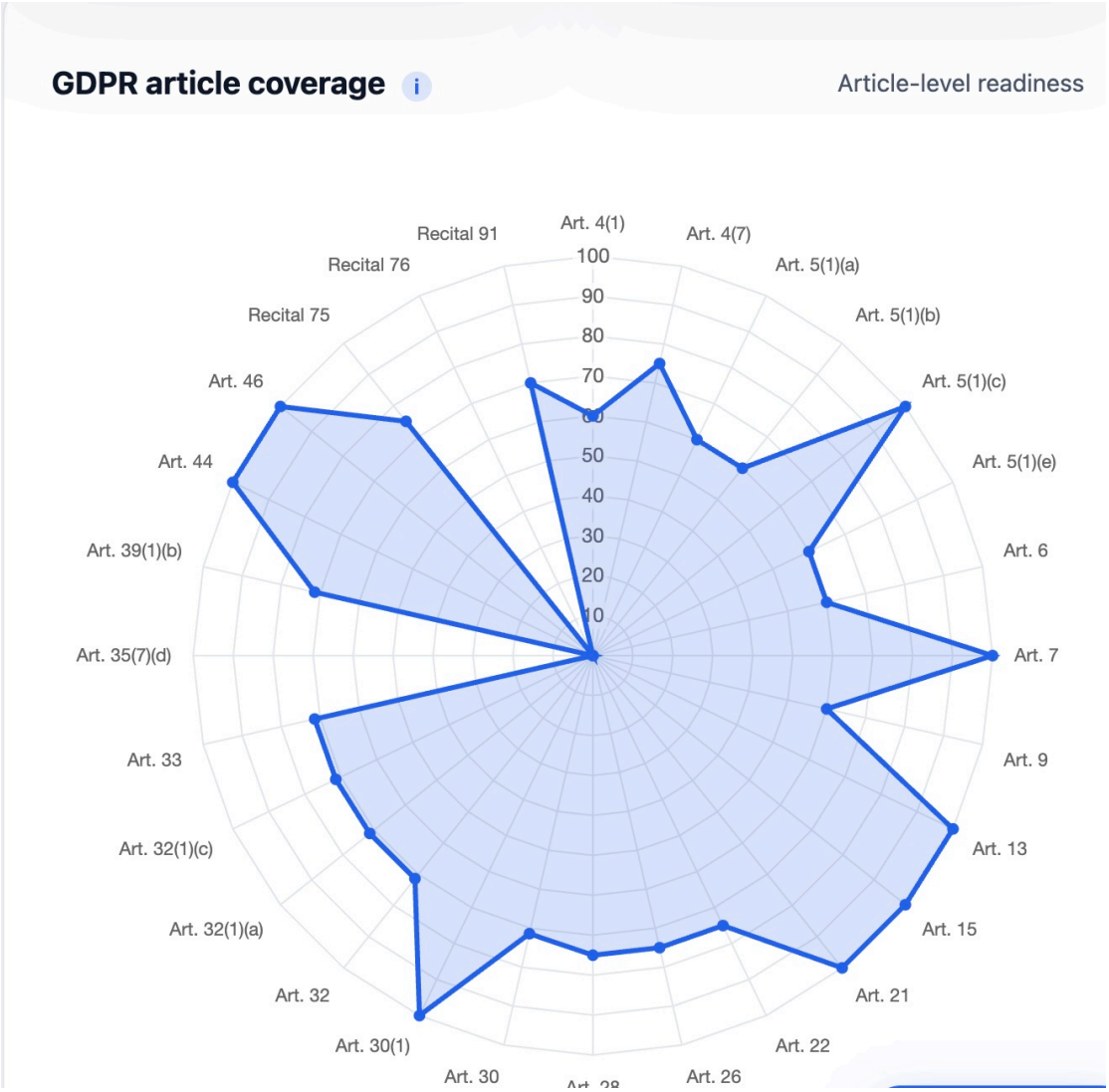


Εικόνα 34: Ροή Ενοποίησης Δεδομένων

Η οπτικοποίηση περιλαμβάνει:

1. Radar Chart: Ένα πολυγωνικό γράφημα που αποτυπώνει την ωριμότητα του οργανισμού σε 4 βασικούς άξονες Αυτό επιτρέπει τη γρήγορη σύγκριση μεταξύ της τρέχουσας κατάστασης και του επιθυμητού στόχου.

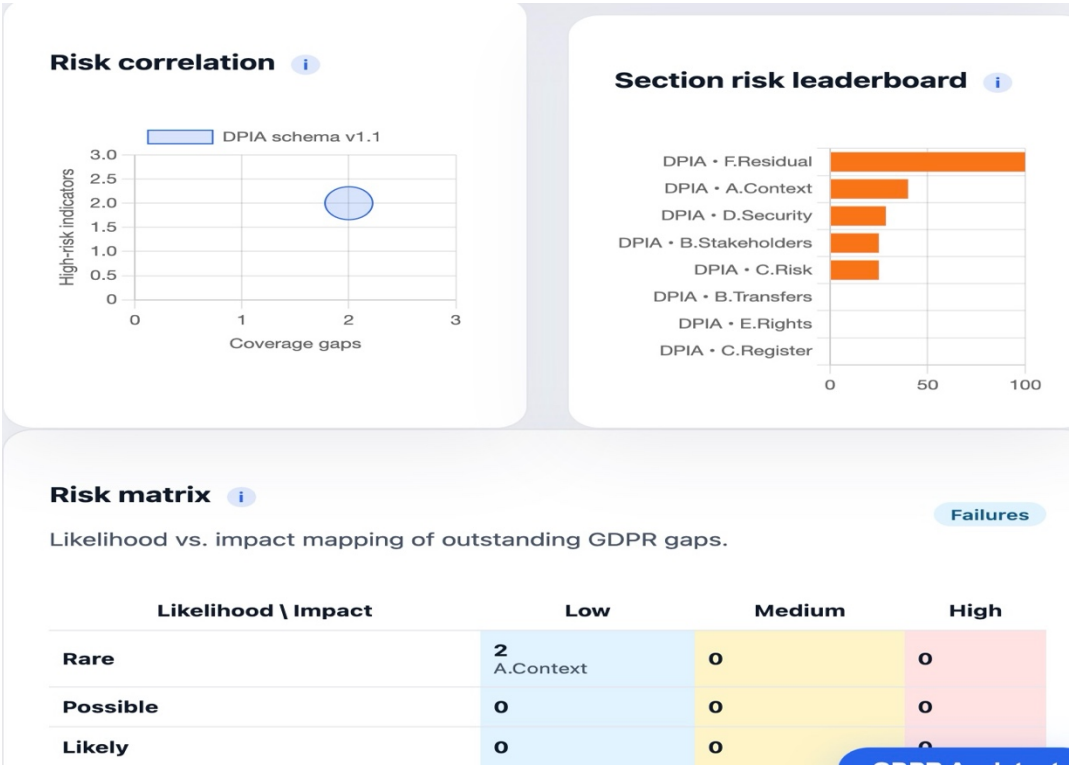
Εικόνα 35: Radar/Risk Matrix



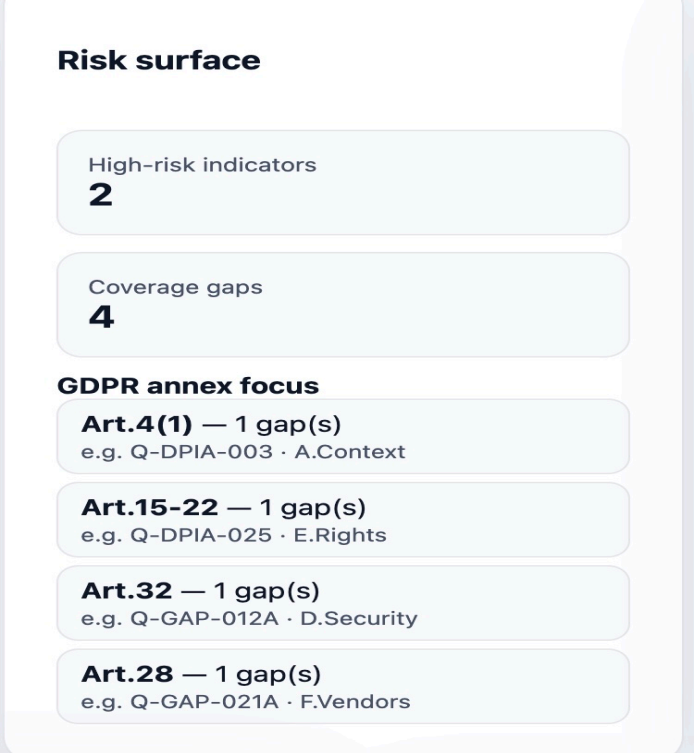
Εικόνα 36: Radar / Coverage per Article

2. Risk Matrix: Ένας πίνακας που χαρτογραφεί τα ευρήματα βάσει Πιθανότητας (Likelihood) και Επιπτώσεων (Impact), βοηθώντας τον DPO να ιεραρχήσει τις διορθωτικές ενέργειες.

Εικόνα 37: Correlation Matrix



Τα αναλυτικά στοιχεία που παράγει το σύστημα δεν έχουν στόχο μόνο να απεικονίσουν αισθητικά τα δεδομένα, αλλά να υποστηρίξουν τη λήψη αποφάσεων. Για παράδειγμα, η απεικόνιση της ωριμότητας ανά θεματική ενότητα επιτρέπει στον DPO να σχεδιάσει στοχευμένες παρεμβάσεις (π.χ. προτεραιοποίηση μέτρων ασφαλείας σε τομείς με χαμηλό σκορ), ενώ η μήτρα κινδύνου βοηθά στη σύνδεση της πιθανότητας με την ένταση των επιπτώσεων. Η δυνατότητα εξαγωγής των αποτελεσμάτων σε μορφές φιλικές προς επεξεργασία (π.χ. CSV, JSON) διευκολύνει επιπλέον την ενσωμάτωση των ευρημάτων σε εσωτερικές αναφορές ή άλλα συστήματα διαχείρισης κινδύνων.



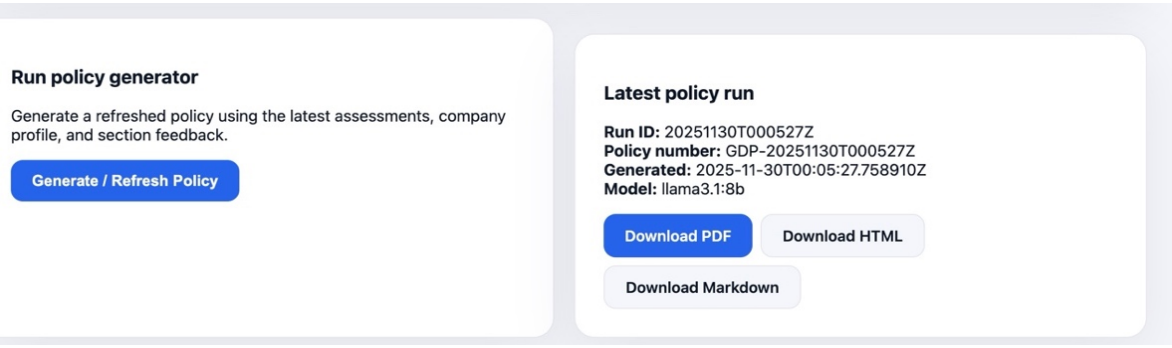
Εικόνα 38: Gap List

6.6 Δομή του Πληροφοριακού συστήματος

Η κορωνίδα του συστήματος είναι η δυνατότητα αυτόματης σύνταξης κειμένων. Στην οθόνη "Official Policy", ο χρήστης μπορεί να παραμετροποιήσει το περιεχόμενο της πολιτικής που επιθυμεί (π.χ. προσθέτοντας το όνομα της εταιρείας και του DPO).[57]

Κρίσιμο στοιχείο της υλοποίησης είναι ότι το παραγόμενο κείμενο δεν θεωρείται «τελικό» αλλά «σχέδιο προς έλεγχο». Η διεπαφή επιτρέπει στον χρήστη να δει το αποτέλεσμα σε μορφή Markdown, να το επεξεργαστεί, να το προσαρμόσει στη γλώσσα και την ορολογία του οργανισμού και, μόνο όταν είναι ικανοποιημένος, να το εξαγάγει σε PDF για επίσημη χρήση. Με αυτόν τον τρόπο, ο ανθρώπινος παράγοντας παραμένει στο κέντρο της διαδικασίας, ενώ το LLM λειτουργεί ως επιταχυντής παραγωγής κειμένου. Η υλοποίηση αυτή ενσωματώνει στην πράξη την αρχή του human-in-the-loop και διασφαλίζει ότι η τεχνητή νοημοσύνη δεν λαμβάνει αυτόνομες κανονιστικές αποφάσεις, αλλά υποστηρίζει τη δουλειά του DPO.[57]

Πατώντας "Generate", το σύστημα συλλέγει τα δομημένα δεδομένα από το JSON (dpia.json, gap.json) και τα διοχετεύει στο τοπικό μοντέλο Llama 3. Το μοντέλο, καθοδηγούμενο



από εξειδικευμένες εντολές (System Prompts), συντάσσει ένα συνεκτικό κείμενο σε φυσική γλώσσα.[57]

Εικόνα 39: Οθόνη Παραγωγής Πολιτικής

Το τελικό αποτέλεσμα παρέχεται σε δύο μορφές:

- Markdown: Για εύκολη επεξεργασία από τεχνικούς.
- PDF: Ως επίσημο έγγραφο έτοιμο για υπογραφή και διανομή.
- HTML : Ωμή (raw) Μορφή του Policy

Η διαδικασία αυτή μειώνει τον χρόνο συγγραφής από ημέρες σε λίγα λεπτά, ενώ η χρήση τοπικού AI διασφαλίζει ότι καμία πληροφορία για τα κενά ασφαλείας της εταιρείας δεν διαρρέει στο διαδίκτυο.

Ένα επιπλέον πλεονέκτημα της υλοποίησης είναι η παραμετροποίηση των prompts μέσω εξωτερικών αρχείων. Τα αρχεία που καθορίζουν το ύφος, τη δομή και το περιεχόμενο των παραγόμενων πολιτικών μπορούν να αναθεωρηθούν χωρίς τροποποίηση του κώδικα, επιτρέποντας την προσαρμογή τους σε διαφορετικούς κλάδους, γλώσσες ή νομικές ιδιαιτερότητες. Μελλοντικά, ο μηχανισμός αυτός μπορεί να αξιοποιηθεί για τη δημιουργία «πακέτων προτύπων» (templates packs) ανά κλάδο (π.χ. υγεία, εκπαίδευση, e-commerce), ενισχύοντας τη χρηστικότητα και την προστιθέμενη αξία του συστήματος[57]

6.7 Συζήτηση επί της Υλοποίησης

Η διαδικασία ανάπτυξης του λογισμικού «GDPR ASSESSOR» αποτέλεσε πεδίο δοκιμασίας για τις αρχιτεκτονικές επιλογές που περιγράφηκαν στα προηγούμενα κεφάλαια. Η μετάβαση από τον θεωρητικό σχεδιασμό στην πρακτική εφαρμογή ανέδειξε σημαντικά τεχνικά ζητήματα. Στην παρούσα ενότητα αναλύονται οι κρίσιμες πτυχές της υλοποίησης. Εξετάζεται η αποδοτικότητα της αρθρωτής αρχιτεκτονικής, η συμπεριφορά του τοπικού γλωσσικού μοντέλου και η στρατηγική διαχείρισης δεδομένων.[57]

Συνολικά, η υλοποίηση του «GDPR ASSESSOR» επιβεβαίωσε ότι είναι εφικτό να συνδυαστούν σε ένα ενιαίο σύστημα διαφορετικοί τύποι ελέγχων (οργανωτικοί, νομικοί, τεχνικοί) και παραγωγική τεχνητή νοημοσύνη, χωρίς να απαιτείται ιδιαίτερα πολύπλοκη υποδομή. Ωστόσο, η ανάπτυξη ανέδειξε και συγκεκριμένους περιορισμούς, όπως η χρονική καθυστέρηση κατά την παραγωγή μεγάλων κειμένων πολιτικής σε τυπικό hardware και η ανάγκη για προσεκτικό σχεδιασμό των prompts ώστε να περιορίζονται οι πιθανότητες παραγωγής ψευδών πληροφοριών. Οι περιορισμοί αυτοί δεν αναιρούν τη χρησιμότητα του συστήματος, αλλά ορίζουν ένα σαφές πλαίσιο εντός του οποίου πρέπει να γίνεται η χρήση του και ταυτόχρονα υποδεικνύουν συγκεκριμένες κατευθύνσεις για βελτίωση σε μελλοντικές εκδόσεις.[57]

6.7.1 Αξιολόγηση της Αρχιτεκτονικής «Βάσει Σχήματος» (Schema-Driven Architecture)

Η κεντρική σχεδιαστική επιλογή ήταν η αποσύνδεση της λογικής του κώδικα από το περιεχόμενο των ερωτηματολογίων. Αυτή η προσέγγιση, γνωστή ως Schema-Driven Development, υλοποιήθηκε μέσω της κλάσης SchemaBundle. Τα ερωτηματολόγια δεν ενσωματώθηκαν στον πηγαίο κώδικα (hard-coded). Αντιθέτως, φορτώνονται δυναμικά από εξωτερικά αρχεία JSON (π.χ. dpia.json).[57]

Η υλοποίηση αυτή προσέφερε εξαιρετική ευελιξία. Επέτρεψε την τροποποίηση των ερωτήσεων χωρίς την ανάγκη αλλαγής της ροής του προγράμματος ή επανεκκίνησης του εξυπηρετητή. Κατά τη διάρκεια των δοκιμών, η προσθήκη νέων πεδίων ελέγχου για την ασφάλεια (Security Controls) πραγματοποιήθηκε αποκλειστικά μέσω επεξεργασίας του αρχείου JSON. Ο μηχανισμός AssessmentBuilder απέδειξε την ανθεκτικότητά του, προσαρμόζοντας αυτόματα τον υπολογισμό του σκορ στα νέα δεδομένα. Συνεπώς, η συντηρησιμότητα (maintainability) του συστήματος κρίνεται ιδιαίτερα υψηλή.

6.7.2 Ενσωμάτωση Τοπικής Τεχνητής Νοημοσύνης και Από

Η διασύνδεση με το τοπικό μοντέλο Llama 3 μέσω της υπηρεσίας Ollama αποτέλεσε το πιο απαιτητικό τμήμα της υλοποίησης. Η συνάρτηση run_ollama σχεδιάστηκε να λειτουργεί σύγχρονα (synchronous execution) για την απλοποίηση της ροής. Ωστόσο, παρατηρήθηκε ότι η παραγωγή κειμένου είναι μια χρονοβόρα διαδικασία.[57]

Σε τυπικό υλικό (hardware) γραφείου, η δημιουργία μιας πλήρους πολιτικής μπορεί να διαρκέσει από 30 έως 60 δευτερόλεπτα. Αυτή η καθυστέρηση (latency) αποτελεί εγγενές χαρακτηριστικό της τοπικής εκτέλεσης (inference) σε CPU. Παρά την καθυστέρηση, η ποιότητα του παραγόμενου κειμένου κρίθηκε ικανοποιητική. Η χρήση συγκεκριμένων προτύπων (templates), όπως το official_policy_overview_en.txt, περιόρισε τις «παραγωγές ψευδών πληροφοριών» του μοντέλου. Το σύστημα λειτούργησε αποτελεσματικά ως μηχανισμός συμπλήρωσης κειμένου (text completion) βάσει αυστηρού πλαισίου (context), επιβεβαιώνοντας την αξία της μεθόδου Retrieval-Augmented Generation (RAG) σε απλουστευμένη μορφή.[57]

6.7.3 Διαχείριση Κατάστασης Χωρίς Βάση Δεδομένων (Stateless design)

Η απόφαση να αποφευχθεί η χρήση σχεσιακής βάσης δεδομένων (SQL) υπέρ της αποθήκευσης σε αρχεία JSON (Session Stores) απλοποίησε δραματικά την ανάπτυξη. Το σύστημα διατηρεί την κατάσταση κάθε συνεδρίας στο φάκελο output/.

Αυτή η επιλογή αποδείχθηκε ιδανική για τον σκοπό της εφαρμογής, η οποία προορίζεται για χρήση από έναν DPO ή μια μικρή ομάδα. Εξασφαλίζει την πλήρη φορητότητα των δεδομένων (Data Portability). Ο χρήστης μπορεί να λάβει ένα αρχείο ZIP με όλες τις απαντήσεις του και να το μεταφέρει σε άλλο μηχάνημα. Ωστόσο, η υλοποίηση αυτή θέτει περιορισμούς στην ταυτόχρονη επεξεργασία από πολλούς χρήστες (concurrency). Σε σενάριο μαζικής χρήσης, το σύστημα αρχείων θα μπορούσε να αποτελέσει σημείο συμφόρησης (bottleneck). Για τα δεδομένα μεγέθη μιας Μικρομεσαίας Επιχείρησης, ωστόσο, η απόδοση κρίνεται επαρκής.[57]

6.7.4 Αυτοματοποίηση Τεχνικών Ελέγχων (Web Scraping)

Η ενσωμάτωση του μηχανισμού cookie_audit.py ανέδειξε τη δυσκολία ελέγχου δυναμικών ιστοσελίδων. Η χρήση της βιβλιοθήκης requests επιτρέπει τον γρήγορο έλεγχο των HTTP κεφαλίδων και των στατικών cookies. Παρ' όλα αυτά, η ανίχνευση cookies που τοποθετούνται μέσω JavaScript απαιτεί πιο σύνθετες τεχνικές (headless browser).

Η παρούσα υλοποίηση εστιάζει στην ανάλυση του HTML κώδικα για τον εντοπισμό ιχνών (signatures) γνωστών εργαλείων παρακολούθησης (π.χ. Google Analytics). Ο αλγόριθμος που

αναπτύχθηκε, βασισμένος σε κανονικές εκφράσεις (Regex), επέτυχε υψηλό ποσοστό ακρίβειας στον εντοπισμό δημοφιλών υπηρεσιών. Αποδείχθηκε ότι η στατική ανάλυση μπορεί να προσφέρει μια γρήγορη, πρώτη εικόνα συμμόρφωσης, χωρίς την πολυπλοκότητα ενός πλήρους crawler.

Συμπερασματικά, η υλοποίηση του «GDPR ASSESSOR» πέτυχε την ισορροπία μεταξύ λειτουργικότητας και πολυπλοκότητας. Η επιλογή της Python και του Flask επέτρεψε την ταχεία ανάπτυξη (rapid prototyping). Η αρχιτεκτονική του συστήματος είναι αρθρωτή και επεκτάσιμη, επιτρέποντας τη μελλοντική ενσωμάτωση νέων κανονιστικών απαιτήσεων με ελάχιστο κόστος ανακατασκευής.[57]

7 *Συζήτηση*

Στο παρόν κεφάλαιο πραγματοποιείται κριτική αποτίμηση του συστήματος «GDPR ASSESSOR» υπό το πρίσμα αφενός της σχετικής βιβλιογραφίας και αφετέρου των ερευνητικών ερωτημάτων που διατυπώθηκαν στην Εισαγωγή της παρούσας εργασίας. Η συζήτηση δεν περιορίζεται σε μια περιγραφική αποτύπωση των λειτουργιών της πλατφόρμας, αλλά εστιάζει στα πλεονεκτήματα και στους περιορισμούς της επιλεγμένης αρχιτεκτονικής, στη συμπεριφορά του τοπικά εκτελούμενου Μεγάλου Γλωσσικού Μοντέλου σε ρεαλιστικά σενάρια παραγωγής πολιτικών απορρήτου, καθώς και στον τρόπο με τον οποίο ο ανθρώπινος παράγοντας ενσωματώνεται ως μηχανισμός ελέγχου και λογοδοσίας μέσα στο προτεινόμενο πλαίσιο παραγωγικής συμμόρφωσης (Generative Compliance). Υπό αυτή την οπτική, το ζητούμενο δεν είναι μόνο η τεχνική ορθότητα των επιμέρους υποσυστημάτων, αλλά η συνολική αξιοπιστία της ροής από δομημένα δεδομένα αξιολόγησης προς συνεκτικό κείμενο πολιτικής, καθώς και οι συνθήκες υπό τις οποίες μια τέτοια ροή μπορεί να θεωρηθεί ασφαλής και εφαρμόσιμη στην πράξη.[57]

Παράλληλα, η αποτίμηση επιχειρεί να τοποθετήσει το «GDPR ASSESSOR» στο ευρύτερο επιστημονικό και τεχνολογικό πλαίσιο της Υπολογιστικής Νομικής και της Κανονιστικής Τεχνολογίας. Με άλλα λόγια, το ενδιαφέρον δεν εξαντλείται στο εάν η πλατφόρμα «λειτουργεί» ως πρωτότυπο, αλλά επεκτείνεται στο πώς διαφοροποιείται από τις παραδοσιακές προσεγγίσεις συμμόρφωσης που βασίζονται σε στατικές φόρμες, πρότυπα εγγράφων και χειροκίνητη συγγραφή. Ιδιαίτερη έμφαση δίνεται στο πώς αξιοποιούνται οι δυνατότητες των Μεγάλων Γλωσσικών Μοντέλων για παραγωγή κειμένου (και ειδικότερα πολιτικής απορρήτου), χωρίς να αίρεται η ανάγκη ανθρώπινης εποπτείας, και στο ποιο ρόλο μπορεί να διαδραματίσει ένα τέτοιο εργαλείο τόσο στην αγορά—ιδίως ως ελαφριά και οικονομικά προσιτή λύση για ΜΜΕ—όσο και στην ερευνητική κοινότητα ως αναπαραγώγιμο παράδειγμα εφαρμογής ελεγχόμενης παραγωγικής τεχνητής νοημοσύνης σε κανονιστικά περιβάλλοντα.[57]

7.1 Αξιολόγηση της Αρχιτεκτονικής Local AI

Η κεντρική καινοτομία της παρούσας διατριβής, όπως προκύπτει από την κριτική αποτίμηση, ήταν η συνειδητή επιλογή τοπικής εκτέλεσης του μοντέλου Llama 3 μέσω του Ollama, αντί της αξιοποίησης cloud υπηρεσιών ευρείας χρήσης (π.χ. OpenAI API). Από αξιολογική σκοπιά, η επιλογή αυτή τεκμηριώνεται ως βέλτιστη πρακτική για σενάρια όπου το ζητούμενο είναι η παραγωγή κειμένων πολιτικής απορρήτου με βάση πληροφορίες που δύνανται να είναι ευαίσθητες για τον οργανισμό. Η τοπική εκτέλεση περιορίζει δραστικά την έκθεση δεδομένων σε τρίτους παρόχους και, συνεπώς, μειώνει τον κίνδυνο διαρροής εμπιστευτικών εταιρικών πληροφοριών ή δεδομένων που σχετίζονται με τη συμμόρφωση, στοιχείο που έχει ιδιαίτερη βαρύτητα σε περιβάλλοντα όπου η εμπιστευτικότητα αποτελεί προϋπόθεση για την υιοθέτηση εργαλείων παραγωγικής τεχνητής νοημοσύνης [11].

Επιπλέον, η επιλογή της Local AI δεν πρέπει να ιδωθεί αποκλειστικά ως τεχνική βελτιστοποίηση, αλλά και ως ρυθμιστική/οργανωσιακή απόφαση. Από τη σκοπιά του GDPR, η αποφυγή αποστολής δεδομένων σε εξωτερικούς παρόχους συνεπάγεται απλούστερη χαρτογράφηση ροών δεδομένων και περιορισμό των εμπλεκόμενων τρίτων (ιδίως ως προς ρόλους «εκτελούντος την επεξεργασία»), γεγονός που διευκολύνει τη λογοδοσία και τη διαφάνεια της επεξεργασίας. Με άλλα λόγια, η αρχιτεκτονική επιλογή συνδέεται άμεσα με τις κανονιστικές αρχές που συζητήθηκαν στα προηγούμενα κεφάλαια: ελαχιστοποίηση διαμοιρασμού, περιορισμός πρόσβασης και ενίσχυση της διακυβέρνησης των δεδομένων εντός του οργανισμού.[11]

Ωστόσο, η ίδια επιλογή ενσωματώνει ένα σαφές κόστος, το οποίο είναι κρίσιμο να αποτυπωθεί με ρεαλιστικούς όρους. Η τοπική εκτέλεση μεταφέρει το υπολογιστικό βάρος στον οργανισμό, ο οποίος καλείται να διαθέτει επαρκή υποδομή (hardware) και να διαχειρίζεται το περιβάλλον λειτουργίας (ενημερώσεις, ασφάλεια, ρυθμίσεις). Η παρούσα εργασία δείχνει ότι, για το συγκεκριμένο use case—δηλαδή την παραγωγή κειμένων πολιτικής απορρήτου και συναφών τυποποιημένων τμημάτων—το Llama 3 8B είναι λειτουργικά επαρκές. Η επάρκεια αυτή ερμηνεύεται ως αποτέλεσμα του «περιορισμένου» χαρακτήρα του προβλήματος: το σύστημα δεν ζητά από το μοντέλο να παράγει πρωτότυπη νομική ερμηνεία, αλλά να μετασχηματίσει δομημένες εισροές (JSON) σε συνεκτικό κείμενο πολιτικής, υπό αυστηρά διαμορφωμένα system prompts (constrained generation). Κατ’ επέκταση, η ποιότητα του παραγόμενου κειμένου εξαρτάται περισσότερο από την ορθότητα και πληρότητα των εισροών και από τη δομή του prompt, παρά από «βαθιά» νομική συλλογιστική.[11]

Παράλληλα, είναι σημαντικό να αναγνωριστεί ότι τα μικρότερα ανοιχτά μοντέλα έχουν περιορισμούς σε καθήκοντα σύνθετης, πολυβηματικής νομικής συλλογιστικής. Συγκριτικές αξιολογήσεις έχουν δείξει ότι, παρότι μοντέλα όπως το Llama 3 έχουν βελτιωθεί σημαντικά, εξακολουθούν να υστερούν έναντι κλειστών frontier μοντέλων (όπως το GPT-4) σε tasks multi-step reasoning [58]. Υπό την οπτική της παρούσας διπλωματικής, αυτό το εύρημα δεν αναιρεί τη χρησιμότητα της προσέγγισης, αλλά οριοθετεί τον χώρο ασφαλούς εφαρμογής της: η Local AI αρχιτεκτονική λειτουργεί ιδιαίτερα αποτελεσματικά όταν το ζητούμενο είναι η παραγωγή πολιτικής απορρήτου με βάση δομημένα δεδομένα και πρότυπα ενότητες (templated sections), ενώ η επέκταση σε πιο σύνθετες νομικές χρήσεις (π.χ. λεπτή στάθμιση βάσεων επεξεργασίας ή διατύπωση εξαιρέσεων σε ειδικά σενάρια) θα απαιτούσε προσεκτική στάθμιση μεταξύ ιδιωτικότητας, υπολογιστικής επάρκειας και προσδοκώμενης ακρίβειας.

Τέλος, από κριτική σκοπιά, η αρχιτεκτονική Local AI δεν μπορεί να παρουσιαστεί ως «ασημένια σφαίρα». Παρότι μεγιστοποιεί την προστασία δεδομένων και ενισχύει τη διαφάνεια της επεξεργασίας, εισάγει πρόσθετες ευθύνες συντήρησης και λειτουργικής ασφάλειας στο εσωτερικό του οργανισμού, ενώ η επιλογή μικρότερων μοντέλων συνεπάγεται περιορισμούς στην κλίμακα και στο βάθος νομικής συλλογιστικής. Συνεπώς, η προσέγγιση της παρούσας εργασίας αποτιμάται ως συνειδητή και τεκμηριωμένη ανταλλαγή (trade-off): προτάσσει την ιδιωτικότητα, τον έλεγχο και την κανονιστική απλότητα, αποδεχόμενη ρεαλιστικά όρια σε απόδοση και ευκολία υποδομής, τα οποία όμως—για τον στόχο της παραγωγής πολιτικών απορρήτου—κρίνονται διαχειρίσιμα και πρακτικά αποδεκτά.[58]

7.2 Κίνδυνος της παραγωγής ψευδών πληροφοριών (Hallucinations) Στη Νομική Τεχνολογία

Ένα από τα πλέον σταθερά ευρήματα της πρόσφατης βιβλιογραφίας (2024) είναι ότι τα Μεγάλα Γλωσσικά Μοντέλα εμφανίζουν συστηματική τάση παραγωγής «π ψευδών πληροφοριών» (hallucinations), δηλαδή νομικά αβάσιμων ή φανταστικών πληροφοριών, με ποσοστά που σε γενικές νομικές ερωτήσεις αναφέρονται από 17% έως και 58% [59]. Από κριτική σκοπιά, το ζήτημα αυτό είναι ιδιαίτερα σοβαρό στη νομική τεχνολογία, επειδή δεν αφορά μόνο την ακρίβεια ενός αποσπάσματος κειμένου, αλλά τον κίνδυνο το μοντέλο να παράγει απαντήσεις με υψηλό βαθμό «ρητορικής βεβαιότητας», οι οποίες μπορεί να οδηγήσουν τον χρήστη σε εσφαλμένες αποφάσεις ή σε ψευδή αίσθηση συμμόρφωσης.

Στην πράξη, οι πιθανότητες παραγωγής ψευδών πληροφοριών στη νομική χρήση μπορούν να εκδηλωθούν με περισσότερους από έναν τρόπους. Μπορεί να εμφανιστούν ως ανύπαρκτες ή λανθασμένες παραπομπές σε άρθρα και κανονιστικά κείμενα, ως υπεραπλουστευμένες γενικεύσεις σε ζητήματα που απαιτούν λεπτή στάθμιση, ή ως «σιωπηρές» παρερμηνείες, όπου το κείμενο είναι γλωσσικά εύλογο αλλά νομικά προβληματικό. Η τελευταία κατηγορία είναι ίσως η πιο επικίνδυνη: το μοντέλο δεν δίνει προφανώς παράλογη απάντηση, αλλά μετατοπίζει διακριτές έννοιες και προϋποθέσεις σε ένα ενιαίο, «ομαλό» αφήγημα, το οποίο δημιουργεί ψευδή ασφάλεια. Επομένως, η συζήτηση για τις hallucinations στη νομική τεχνολογία αφορά ταυτόχρονα την ορθότητα, την ερμηνευτική ακρίβεια και—κυρίως—τη διαχείριση της εμπιστοσύνης του χρήστη απέναντι σε ένα σύστημα που μπορεί να φαίνεται πειστικό ακόμη και όταν σφάλει.[59]

Στο «GDPR ASSESSOR», ο κίνδυνος αυτός αντιμετωπίστηκε με μια απλουστευμένη λογική Retrieval-Augmented Generation (RAG), όχι υπό την πλήρη μορφή ανάκτησης από εξωτερικές βάσεις γνώσης, αλλά ως αυστηρή «δέσμευση» του μοντέλου σε συγκεκριμένα πραγματολογικά δεδομένα που προκύπτουν από τα ερωτηματολόγια του χρήστη. Με αυτόν τον σχεδιασμό, το LLM δεν χρησιμοποιείται ως ανεξάρτητη πηγή νομικής γνώσης, αλλά ως μηχανισμός σύνθεσης και διατύπωσης: η παραγωγή πολιτικής απορρήτου βασίζεται στα δηλωμένα χαρακτηριστικά του οργανισμού (σκοποί, κατηγορίες δεδομένων, αποδέκτες, μέτρα κ.λπ.), με αποτέλεσμα το μοντέλο να λειτουργεί περισσότερο ως «συντάκτης» και λιγότερο ως «νομικός σύμβουλος». Η προσέγγιση αυτή περιορίζει σημαντικά τις πιθανότητες παραγωγής ψευδών πληροφοριών που σχετίζονται με τα πραγματικά δεδομένα του οργανισμού, επειδή τα κρίσιμα facts δεν επιτρέπεται να "εφευρεθούν", αλλά εισάγονται ως δομημένο πλαίσιο (context injection).[59]

Ωστόσο, από αξιολογική σκοπιά, η απλουστευμένη RAG προσέγγιση δεν εξαφανίζει το πρόβλημα· το μετατοπίζει. Ακόμη και αν το μοντέλο δεν «επινοεί» οργανωσιακά δεδομένα, μπορεί να παρανοήσει το κανονιστικό πλαίσιο μέσα στο οποίο αυτά εντάσσονται ή να υπερ-γενικεύσει ως προς τις νομικές συνέπειες και τις κατάλληλες διατυπώσεις. Επιπλέον, παραμένει υπαρκτός ο κίνδυνος λανθασμένων παραπομπών ή μη ακριβών αναφορών σε άρθρα, κάτι που στην περίπτωση κειμένων πολιτικής απορρήτου είναι κρίσιμο, διότι επηρεάζει τόσο την τεκμηρίωση λογοδοσίας όσο και την αξιοπιστία του τελικού εγγράφου. Για τον λόγο αυτό, ο τελικός ανθρώπινος έλεγχος από DPO ή νομικό ειδικό παραμένει αναγκαία προϋπόθεση, όχι ως τυπική επιφύλαξη, αλλά ως βασική δικλείδα ασφάλειας απέναντι σε «σιωπηρές» νομικές αστοχίες [12].

Με βάση τα παραπάνω, η αντιμετώπιση των hallucinations στην παρούσα εργασία πρέπει να ερμηνευθεί ως μια λειτουργική στρατηγική μετριασμού κινδύνου και όχι ως οριστική λύση. Η

εμπειρία από την υλοποίηση υποδεικνύει ότι μελλοντική έρευνα θα ήταν σκόπιμο να εξετάσει πιο εξελιγμένες τεχνικές RAG, όπως ελεγχόμενη εισαγωγή αποσπασμάτων από επίσημες πηγές (π.χ. κανονιστικό κείμενο, οδηγίες αρχών), καθώς και μηχανισμούς επαλήθευσης παραπομπών πριν την εξαγωγή τελικού εγγράφου. Σε κάθε περίπτωση, το βασικό συμπέρασμα που προκύπτει είναι ότι ένα τέτοιο σύστημα πρέπει να αντιμετωπίζεται ως εργαλείο υποβοήθησης της παραγωγής πολιτικής απορρήτου—δηλαδή ως επιταχυντής συγγραφής και οργάνωσης περιεχομένου—και όχι ως πηγή δεσμευτικής νομικής ερμηνείας.[12]

7.3 Αναγκαιότητα του "Human-in-the-loop"

Η κριτική ανάλυση της βιβλιογραφίας και του κανονιστικού πλαισίου συγκλίνει στο συμπέρασμα ότι η «πλήρης αυτοματοποίηση» της συμμόρφωσης δεν είναι ούτε νομικά ούτε ηθικά ασφαλής επιλογή. Σε επίπεδο θεμελιωδών αρχών, το Άρθρο 22 του GDPR θεσπίζει προστασία των υποκειμένων έναντι αποφάσεων που λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, υπογραμμίζοντας ότι, σε κρίσιμες διαδικασίες που επηρεάζουν δικαιώματα και ελευθερίες, η ανθρώπινη κρίση δεν μπορεί να παρακαμφθεί [GDPR Article 22]. Παράλληλα, στο αναδυόμενο ρυθμιστικό πλαίσιο της Ε.Ε. για την τεχνητή νοημοσύνη, ο EU AI Act ενισχύει περαιτέρω αυτή τη λογική, εισάγοντας ως κεντρική απαίτηση την ανθρώπινη εποπτεία (Human Oversight) ιδίως για συστήματα υψηλού ρίσκου, ώστε να διασφαλίζεται έλεγχος, δυνατότητα παρέμβασης και λογοδοσία [60]. Από αξιολογική σκοπιά, τα δύο αυτά σημεία λειτουργούν ως σαφής «οροφή» στο τι μπορεί να θεωρηθεί αποδεκτό επίπεδο αυτοματοποίησης σε διαδικασίες συμμόρφωσης.

Μέσα σε αυτό το πλαίσιο, η αρχιτεκτονική του «GDPR ASSESSOR» αποτυπώνει μια συνειδητή και ρεαλιστική κατανομή ρόλων μεταξύ μηχανής και ανθρώπου. Το σύστημα αναλαμβάνει όσα μπορούν να τυποποιηθούν με σχετική ασφάλεια—τη συλλογή και οργάνωση των εισροών, την αποθήκευση και επεξεργασία των απαντήσεων, καθώς και την αρχική σύνθεση/δομημένη διατύπωση ενός προσχεδίου πολιτικής απορρήτου και συναφών κειμένων. Ο άνθρωπος, αντιθέτως, διατηρεί τον κρίσιμο ρόλο της αξιολόγησης επάρκειας, της ερμηνευτικής στάθμισης, της προσαρμογής της γλώσσας στα ειδικά χαρακτηριστικά του οργανισμού και, τελικά, της λήψης αποφάσεων. Υπό αυτή την έννοια, η τεχνητή νοημοσύνη δεν τοποθετείται ως «αυτόματος πιλότος», αλλά ως «συνοδηγός» (co-pilot) που επιταχύνει τη συγγραφή και μειώνει το διοικητικό βάρος, χωρίς να μεταφέρει την ευθύνη της συμμόρφωσης εκτός ανθρώπινου ελέγχου.[60]

Η επιλογή αυτή υλοποιείται πρακτικά μέσω της σχεδιαστικής αρχής Human-in-the-Loop (HITL). Ο χρήστης (DPO) καλείται να επικυρώσει τα ευρήματα της αξιολόγησης πριν από την παραγωγή της αναφοράς, ενώ προβλέπεται δυνατότητα επεξεργασίας του τελικού κειμένου (π.χ. σε μορφή Markdown) πριν την εξαγωγή/οριστικοποίηση. Από αξιολογική άποψη, αυτή η ροή ενισχύει δύο κρίσιμα στοιχεία: αφενός, περιορίζει τον κίνδυνο η τελική πολιτική απορρήτου να ενσωματώσει ακούσια σφάλματα ή ακατάλληλες γενικεύσεις του μοντέλου· αφετέρου, διατηρεί τη λογοδοσία στον ανθρώπινο ρόλο που θεσμικά φέρει την ευθύνη. Έτσι, η τεχνολογία λειτουργεί ως εργαλείο ενίσχυσης (augmentation) και όχι ως υποκατάστατο της ανθρώπινης κρίσης [61].

Ωστόσο, η εισαγωγή εργαλείων παραγωγικής τεχνητής νοημοσύνης σε διαδικασίες συμμόρφωσης συνοδεύεται από έναν πρόσθετο κίνδυνο που δεν είναι καθαρά τεχνικός: την υπερεμπιστοσύνη (automation bias). Οι χρήστες μπορεί να τείνουν να αποδέχονται άκριτα τις προτάσεις του συστήματος, ειδικά όταν αυτές εμφανίζονται γλωσσικά πειστικές και τεχνικά «καλοστημένες». Από κριτική σκοπιά, αυτό το φαινόμενο είναι ιδιαίτερα σημαντικό στην παραγωγή πολιτικής απορρήτου, επειδή το κείμενο μπορεί να δημιουργεί εντύπωση πληρότητας ακόμη και όταν υπάρχουν κενά, ασάφειες ή ακατάλληλες διατυπώσεις για το συγκεκριμένο οργανωσιακό πλαίσιο. Η παρούσα υλοποίηση επιχειρεί να μετριάσει τον κίνδυνο μέσω σχεδιαστικών επιλογών (π.χ. σαφής επισήμανση ότι το κείμενο αποτελεί «draft», δυνατότητα επεξεργασίας πριν την οριστικοποίηση, ένταξη σημείων ελέγχου), όμως η πλήρης αντιμετώπιση δεν μπορεί να στηριχθεί μόνο στον σχεδιασμό διεπαφής. Απαιτείται συμπληρωματικά οργανωτική θωράκιση: κατάλληλη εκπαίδευση χρηστών, σαφείς εσωτερικές οδηγίες για το πότε και πώς χρησιμοποιείται το εργαλείο, και διαδικασίες ελέγχου/έγκρισης που διατηρούν την τελική ευθύνη στον DPO ή στο νομικό τμήμα. Με αυτόν τον τρόπο, το «GDPR ASSESSOR» μπορεί να ενταχθεί σε μια πρακτική και κανονιστικά συνεπή λογική χρήσης της παραγωγικής τεχνητής νοημοσύνης, όπου το όφελος είναι η μείωση του διοικητικού φόρτου και η επιτάχυνση της σύνταξης πολιτικών, χωρίς να διακινδυνεύεται η ουσία της λογοδοσίας και της ανθρώπινης εποπτείας.[61]

7.4 Σύγκριση με Υπάρχουσες Λύσεις

Σε σύγκριση με τις εμπορικές πλατφόρμες που εξετάστηκαν στο Κεφάλαιο 2 (ενδεικτικά, λύσεις τύπου OneTrust), το «GDPR ASSESSOR» εμφανίζει πλεονεκτήματα που είναι ιδιαίτερα κρίσιμα για το προφίλ και τους περιορισμούς των μικρομεσαίων επιχειρήσεων. Πρώτον, σε επίπεδο κόστους, η απουσία αδειών χρήσης και συνδρομών cloud μεταφράζεται σε χαμηλό ή μηδενικό λειτουργικό κόστος, κάτι που, από πρακτική σκοπιά, αποτελεί συχνά προϋπόθεση για να υιοθετηθεί οποιοδήποτε εργαλείο συμμόρφωσης από ΜΜΕ. Δεύτερον, ως προς την ιδιωτικότητα, η αρχιτεκτονική τοπικής εκτέλεσης και ο πλήρης έλεγχος της ροής δεδομένων ενισχύουν την έννοια της κυριαρχίας δεδομένων (Data Sovereignty), περιορίζοντας τις εξαρτήσεις από τρίτους παρόχους και μειώνοντας τους κινδύνους που συνδέονται με την αποστολή ευαίσθητων πληροφοριών εκτός οργανισμού. Τρίτον, ως προς την επιχειρησιακή ταχύτητα, η δυνατότητα άμεσης παραγωγής πρώτων προσχεδίων (first drafts) πολιτικών απορρήτου συνιστά πρακτικό όφελος υψηλής αξίας: μεταφέρει την προσπάθεια από τη χειροκίνητη συγγραφή στην επιμέλεια και στην τελική προσαρμογή, μειώνοντας τον χρόνο που απαιτείται για να παραχθεί ένα συνεκτικό κείμενο.[61]

Από την άλλη πλευρά, η κριτική σύγκριση αναδεικνύει ότι το «GDPR ASSESSOR» υστερεί έναντι των enterprise λύσεων σε πεδία που σχετίζονται με την κλιμάκωση και τη διαχείριση πολυπλοκότητας. Οι μεγάλες πλατφόρμες GRC/Privacy Management έχουν σχεδιαστεί για οργανισμούς με πολλαπλές οντότητες, περίπλοκες ιεραρχίες, διαφορετικές γεωγραφικές δικαιοδοσίες και υψηλές απαιτήσεις ενοποίησης με εταιρικά συστήματα. Αντιθέτως, η παρούσα υλοποίηση είναι πιο κατάλληλη για σενάρια με σαφέστερη δομή και περιορισμένο οργανωτικό εύρος, καθώς δεν ενσωματώνει ακόμη μηχανισμούς enterprise governance, multi-tenant ρυθμίσεις, ή εκτεταμένη αυτοματοποίηση ενημερώσεων κανονιστικού περιεχομένου. Επιπλέον, η εξάρτηση από τοπικά μοντέλα και τοπικό περιβάλλον συνεπάγεται ανάγκη χειροκίνητης επικαιροποίησης (τόσο στο επίπεδο του μοντέλου όσο και στο επίπεδο των templates/σχημάτων), κάτι που μειώνει

την «αυτοματοποιημένη επικαιρότητα» που υπόσχονται οι εμπορικές λύσεις με συνεχή ενημέρωση περιεχομένου και ενσωματωμένη νομική βάση γνώσης [62].

Ωστόσο, το πιο ουσιαστικό συμπέρασμα από τη σύγκριση δεν είναι ότι το «GDPR ASSESSOR» «κερδίζει» ή «χάνει» απέναντι στα enterprise συστήματα, αλλά ότι τοποθετείται σε διαφορετικό σημείο του οικοσυστήματος. Δεν επιχειρεί να ανταγωνιστεί άμεσα το πλήρες εύρος λειτουργιών ενός μεγάλου GRC, αλλά να καλύψει ένα πρακτικό κενό που αναδείχθηκε στη χαρτογράφηση του Κεφαλαίου 2: την παραγωγική υποστήριξη της συγγραφής, με έμφαση στην πολιτική απορρήτου, σε μια ελαφριά, οικονομικά προσιτή και τεχνικά διαφανή στοίβα. Από αυτή την οπτική, η συμβολή του μπορεί να χαρακτηριστεί περισσότερο συμπληρωματική παρά υποκατάστατη. Για τις ΜΜΕ, μπορεί να λειτουργήσει ως αυτόνομο εργαλείο που μειώνει άμεσα το διοικητικό βάρος και παρέχει γρήγορα αξιοποιήσιμα προσχέδια πολιτικών. Για μεγαλύτερους οργανισμούς, μπορεί να λειτουργήσει ως «sandbox» πειραματισμού με Local AI και controlled generation, προσφέροντας έναν χαμηλού ρίσκου τρόπο να διερευνηθεί η αξία της παραγωγικής τεχνητής νοημοσύνης στην παραγωγή κειμένων συμμόρφωσης πριν από επένδυση σε βαριές εμπορικές πλατφόρμες.[62]

7.5 Περιορισμοί της έρευνας

Σε μεθοδολογικό επίπεδο, ένας βασικός περιορισμός είναι ότι η αξιολόγηση της χρηστικότητας και της αποτελεσματικότητας του συστήματος στηρίχθηκε κυρίως σε ελεγχόμενα σενάρια και στην κριτική εκτίμηση του ερευνητή, ενδεχομένως με τη συνδρομή περιορισμένου αριθμού χρηστών. Δεν πραγματοποιήθηκε ακόμη μια ευρείας κλίμακας μελέτη χρηστικότητας με μεγάλο και στατιστικά αντιπροσωπευτικό δείγμα DPOs, ούτε μακροχρόνια παρακολούθηση της ενσωμάτωσης του εργαλείου σε πραγματικές ροές εργασίας. Συνεπώς, τα συμπεράσματα για την πρακτική αξία του συστήματος μπορούν να θεωρηθούν ισχυρές ενδείξεις, με την προϋπόθεση ότι θα ενισχυθούν περαιτέρω από μελλοντικές δοκιμές πεδίου.

Πέρα από τη μεθοδολογία, προκύπτουν και ορισμένοι λειτουργικοί περιορισμοί που είναι αναμενόμενοι για μια Local AI προσέγγιση και μπορούν να αντιμετωπιστούν σταδιακά. Πρώτον, ως προς τη γλωσσική απόδοση, το Llama 3 έχει εκπαιδευτεί κυρίως σε αγγλικά δεδομένα, οπότε στην παραγωγή ελληνικών νομικών κειμένων ενδέχεται να εμφανιστούν περιστασιακά αγγλισμοί ή λιγότερο «φυσικές» διατυπώσεις. Στην πράξη, αυτό δεν ακυρώνει τη χρησιμότητα του εργαλείου, αλλά ενισχύει τον ρόλο του DPO ως επιμελητή: το σύστημα παράγει ένα ποιοτικό πρώτο προσχέδιο, το οποίο στη συνέχεια γυαλίζεται γλωσσικά και προσαρμόζεται στον συγκεκριμένο οργανισμό. Δεύτερον, ο χρονικός ορίζοντας γνώσης (knowledge cutoff) σημαίνει ότι το μοντέλο δεν «γνωρίζει» νεότερες οδηγίες ή αποφάσεις μετά την εκπαίδευσή του, συνεπώς η περιοδική επικαιροποίηση (μέσω ενημερώσεων του μοντέλου ή/και των templates) παραμένει χρήσιμη πρακτική για τη διατήρηση της επικαιρότητας [63]. Τρίτον, η ταχύτητα παραγωγής εξαρτάται από το διαθέσιμο hardware: σε τυπικό σύγχρονο εξοπλισμό η εμπειρία είναι ικανοποιητική, ενώ σε παλαιότερα μηχανήματα μπορεί να εμφανιστεί μεγαλύτερο latency. Αυτό, όμως, είναι ακριβώς το αναμενόμενο trade-off της τοπικής εκτέλεσης, το οποίο αντισταθμίζεται από το όφελος της ιδιωτικότητας και του ελέγχου των δεδομένων.

Επιπλέον, από την ίδια την εμπειρία υλοποίησης προέκυψαν ορισμένοι «περιορισμοί σχεδιασμού» που λειτουργούν περισσότερο ως σαφείς άξονες βελτίωσης παρά ως αδυναμίες. Η ποιότητα της παραγόμενης πολιτικής απορρήτου εξαρτάται από την πληρότητα και τη συνοχή των εισροών του χρήστη: όσο πιο καθαρά και δομημένα είναι τα δεδομένα που συλλέγονται μέσω των ερωτηματολογίων, τόσο πιο στοχευμένο και αξιοποιήσιμο είναι το τελικό κείμενο. Με την ίδια λογική, η χειροκίνητη επικαιροποίηση των schemas/prompts αποτελεί σήμερα μια πρακτική ανάγκη, αλλά ταυτόχρονα είναι και πλεονέκτημα της schema-driven αρχιτεκτονικής, καθώς επιτρέπει γρήγορη προσαρμογή χωρίς ανασχεδιασμό του κώδικα.[63]

Τέλος, είναι χρήσιμο να αναφερθεί με ισορροπημένο τρόπο ότι το ρυθμιστικό πλαίσιο για την ΤΝ στην Ε.Ε. εξελίσσεται (AI Act), και πιθανόν να ενισχύσει απαιτήσεις όπως logging, τεκμηρίωση και διαχείριση κινδύνου για συστήματα που ενσωματώνουν LLMs. Η εργασία το λαμβάνει υπόψη θεωρητικά, ενώ η υλοποίηση μπορεί να εμπλουτιστεί σταδιακά με πρόσθετα στοιχεία τεκμηρίωσης και ελέγχου, ώστε να παραμένει ευθυγραμμισμένη με τις απαιτήσεις που θα σταθεροποιηθούν στο προσεχές διάστημα. Overall, τα παραπάνω δεν μειώνουν τη συμβολή του «GDPR ASSESSOR», αλλά περιγράφουν ρεαλιστικά το πεδίο στο οποίο μια λειτουργική πλατφόρμα μπορεί να ωριμάσει περαιτέρω μέσω πιλοτικών εφαρμογών, γλωσσικής εξειδίκευσης και ενίσχυσης των μηχανισμών τεκμηρίωσης.[63]

8

Συμπεράσματα της Μελέτης

Βάσει της υλοποίησης του συστήματος «GDPR ASSESSOR» και της ανάλυσης που προηγήθηκε στα Κεφάλαια 1–3, οι απαντήσεις στα ερευνητικά ερωτήματα διατυπώνονται με τρόπο που αντιστοιχεί άμεσα στο αρχικό ερευνητικό κενό (research gap) που εντοπίστηκε: την απουσία μιας ενιαίας, οικονομικά προσιτής λύσης που να συνδυάζει δομημένη συλλογή πληροφοριών, τεχνικό έλεγχο και ασφαλή παραγωγή κειμένου πολιτικής/τεκμηρίωσης μέσω τοπικών LLMs, υπό ανθρώπινη εποπτεία. Με αυτή την έννοια, κάθε απάντηση παρακάτω δεν αξιολογεί απλώς «αν λειτουργεί» ένα υποσύστημα, αλλά αν το σύνολο της προσέγγισης καλύπτει το "τελευταίο μίλι" που λείπει από την αγορά και τη βιβλιογραφία: τη μετατροπή δομημένων ευρημάτων σε συνεκτικό και προσαρμοσμένο κείμενο, χωρίς να θυσιάζεται η ασφάλεια και η επαναληψιμότητα.[63]

8.1 Τα ερευνητικά ερωτήματα και απαντήσεις

Συνολικά, τα ευρήματα υποστηρίζουν ότι το σύστημα καλύπτει σε μεγάλο βαθμό το αρχικό research gap: (α) μετατρέπει τη συλλογή πληροφορίας από «στατική καταγραφή» σε δομημένη, ιχνηλάσιμη διαδικασία αξιολόγησης, (β) γεφυρώνει το «κενό παραγωγής» μέσω ελεγχόμενης παραγωγής κειμένων πολιτικής από τοπικό LLM, (γ) αντιμετωπίζει το privacy paradox μέσω local execution, και (δ) μειώνει την αποσπασματικότητα ενσωματώνοντας τεχνικό έλεγχο στη συνολική ροή. Ταυτόχρονα, αναγνωρίζεται ότι η πλήρης επιβεβαίωση—ιδίως ως προς χρηστικότητα, υιοθέτηση και οικονομικό όφελος σε πραγματικές ΜΜΕ—αποτελεί επόμενο βήμα και σαφή κατεύθυνση για μελλοντική έρευνα.[63]

8.1.1 Ερευνητικό ερώτημα 1

«Σε ποιο βαθμό είναι εφικτό να σχεδιαστεί ένα πληροφοριακό σύστημα που να καθοδηγεί τον χρήστη βήμα προς βήμα στη διενέργεια DPIA και Gap Analysis, αξιοποιώντας δομημένα ερωτηματολόγια τα οποία συνδέονται άμεσα με συγκεκριμένα άρθρα του GDPR;»[63]

Η υλοποίηση του Assessment Engine έδειξε ότι είναι εφικτό να μετατραπεί η DPIA/Gap Analysis από «άτυπη» διαδικασία (συνεντεύξεις, έγγραφα Word, εμπειρικές σημειώσεις) σε τυποποιημένη ακολουθία βημάτων με σαφή δομή και ιχνηλασιμότητα. Η χρήση schema-driven αρχείων JSON (dpia.json, gap.json) και η λειτουργία της AssessmentBuilder επέτρεψαν: (α) θεματική ομαδοποίηση και σταδιακή καθοδήγηση του χρήστη, (β) συστηματική συλλογή πληροφοριών με έλεγχο εγκυρότητας, και (γ) άμεση σύνδεση πεδίων/ενοτήτων με νομικές αναφορές (gdpr_refs), ώστε ο χρήστης να κατανοεί «γιατί» ζητείται κάθε πληροφορία. Αυτό απαντά στο πρώτο τμήμα του αρχικού ερευνητικού κενού (structured, traceable data capture): αντί για απλή καταγραφή, δημιουργείται αναπαραγώγιμο σύνολο δομημένων δεδομένων που μπορεί να χρησιμοποιηθεί ως βάση για παραγωγή κειμένου. Συνεπώς, το ερώτημα απαντάται καταφατικά ως προς τη δυνατότητα συστηματικής καθοδήγησης και χαρτογράφησης απαιτήσεων, με την

επισήμανση ότι η πλήρης αποτίμηση της εργονομίας και της κατανόησης από τελικούς χρήστες απαιτεί ευρύτερη αξιολόγηση με DPOs.[63]

8.1.2 Ερευνητικό ερώτημα 2

«Πώς μπορεί να ενσωματωθεί ένα τοπικά εκτελούμενο Μεγάλο Γλωσσικό Μοντέλο, ώστε να συνθέτει κείμενα πολιτικής απορρήτου και διαδικασιών ασφαλείας, ελαχιστοποιώντας ταυτόχρονα τις νομικά επικίνδυνες παραγωγές ψευδών πληροφοριών ς;»[63]

Η ενσωμάτωση του Llama 3 μέσω Ollama επιβεβαίωσε ότι ένα LLM μπορεί να χρησιμοποιηθεί λειτουργικά ως «μηχανή κειμενοποίησης» για πολιτικές απορρήτου και συναφείς διαδικασίες, υπό την προϋπόθεση ότι η χρήση του είναι αυστηρά περιορισμένη και "context-aware". Το κρίσιμο στοιχείο εδώ—που απαντά στον πυρήνα του research gap για «Generative Compliance/Generative Policy Writing»—είναι ότι το μοντέλο δεν τροφοδοτείται με ασαφή, ελεύθερη περιγραφή, αλλά με δομημένες εισροές που προέρχονται από τα schemas και τα αποτελέσματα της αξιολόγησης (DPIA/Gap και τεχνικά ευρήματα). Η χρήση system prompts, ο αποκλεισμός της «ελεύθερης συνομιλίας» και η προ-επεξεργασία των inputs (noise reduction) λειτουργούν ως μηχανισμοί μείωσης της παραγωγής ψευδών πληροφοριών, επειδή περιορίζουν τον χώρο «δημιουργικής συμπλήρωσης» του μοντέλου σε πληροφορίες που έχουν δηλωθεί ή ελεγχθεί από τον χρήστη/σύστημα. Παράλληλα, η τοπική εκτέλεση καλύπτει το δεύτερο κρίσιμο σκέλος του αρχικού κενού (privacy-by-design in AI usage): μειώνει ουσιαστικά την έκθεση εισροών σε τρίτους παρόχους. Παρότι δεν είναι ρεαλιστικό να υποστηριχθεί πλήρης εξάλειψη του κινδύνου ανακριβών διατυπώσεων, τα αποτελέσματα δείχνουν ότι η ελεγχόμενη, δομημένη και τοπική χρήση ενός LLM μπορεί να υποστηρίξει παραγωγή πολιτικών με αποδεκτή αξιοπιστία, υπό ρητή προϋπόθεση human-in-the-loop έγκρισης.[63]

8.1.3 Ερευνητικό ερώτημα 3

«Ποια αρχιτεκτονικά πρότυπα (π.χ. schema-driven development, αποθήκευση σε JSON, modular σχεδίαση) διευκολύνουν την προσαρμογή του συστήματος σε μελλοντικές αλλαγές του κανονιστικού πλαισίου;»

Η υλοποίηση έδειξε ότι ο συνδυασμός schema-driven development, modular αρχιτεκτονικής και αποθήκευσης ερωτηματολογίων σε JSON αποτελεί πρακτικά αποτελεσματική βάση προσαρμογής. Η προσθήκη νέων ενοτήτων, η αλλαγή πεδίων και η ενσωμάτωση νέων νομικών παραπομπών πραγματοποιήθηκαν χωρίς μεταβολές στον πυρήνα της ροής της εφαρμογής, γεγονός που μειώνει το κόστος συντήρησης και αυξάνει την ανθεκτικότητα σε αλλαγές απαιτήσεων. Αυτό απαντά στο τρίτο σκέλος του αρχικού κενού που προκύπτει στην αγορά: οι enterprise πλατφόρμες είναι «βαριές» και δύσκολα παραμετροποιούνται χωρίς συμβούλους, ενώ οι απλές λύσεις είναι στατικές. Αντίθετα, η διάκριση "content vs logic" (JSON vs Python) και η οργάνωση σε modules (gdpr_wizard, policy_engine, site_inspector) επιτρέπουν εξέλιξη του συστήματος χωρίς πλήρη ανασχεδιασμό. Συνεπώς, το ερώτημα απαντάται με τη διαπίστωση ότι τα συγκεκριμένα πρότυπα αποτελούν κατάλληλη αρχιτεκτονική στρατηγική για επέκταση, τόσο εντός GDPR (οδηγίες Αρχών, νέες απαιτήσεις τεκμηρίωσης) όσο και σε γειτονικά πλαίσια (π.χ. AI Act), υπό την προϋπόθεση ότι θα προστεθούν αντίστοιχα schemas/κανόνες.[63]

8.1.4 Ερευνητικό ερώτημα 4

«Σε ποιον βαθμό ένα τέτοιο σύστημα μπορεί να αποτελέσει ρεαλιστική, οικονομικά προσιτή εναλλακτική για ΜΜΕ σε σχέση με τις υφιστάμενες, βαριές και υψηλού κόστους πλατφόρμες συμμόρφωσης;»

Η επιλογή ανοικτών τεχνολογιών, η απουσία εξάρτησης από εμπορικές cloud υπηρεσίες AI και η δυνατότητα εκτέλεσης σε τυπικό hardware υποστηρίζουν ότι το σύστημα μπορεί να λειτουργήσει ως ρεαλιστική εναλλακτική για ΜΜΕ, ακριβώς στο σημείο όπου το research gap είναι πιο έντονο: μια «μεσαία λύση» ανάμεσα στις enterprise πλατφόρμες και στις στατικές/συμβουλευτικές πρακτικές. Η αυτοματοποίηση της παραγωγής κειμένων πολιτικής (και η ενσωμάτωση τεχνικών ευρημάτων ιστοσελίδας) μειώνει τον επαναλαμβανόμενο χρόνο συγγραφής/επικαιροποίησης, ενώ η modular απλότητα (Flask, JSON, local LLM) περιορίζει τις απαιτήσεις σε εξειδικευμένο προσωπικό. Ωστόσο, για να απαντηθεί πλήρως το ερώτημα με όρους του αρχικού ερευνητικού κενού (πρακτική υιοθέτηση/απόδοση σε πραγματική οικονομία), απαιτείται εκτενέστερη εμπειρική αξιολόγηση σε οργανισμούς ΜΜΕ: μετρήσεις χρόνου/κόστους πριν και μετά, αξιολόγηση χρηστικότητας από μη τεχνικούς χρήστες, και ανάλυση κόστους–οφέλους σε βάθος χρόνου. Συνεπώς, το ερώτημα απαντάται καταφατικά ως προς τη θεωρητική και τεχνική βιωσιμότητα, με ρητή αναγνώριση ότι η εξωτερική εγκυρότητα απαιτεί μεγαλύτερη κλίμακα δοκιμών.[63]

8.1.5 Συνολική Σύνδεση με το Αρχικό Ερευνητικό Κενό

Σε γενικές γραμμές, το ερευνητικό κενό που εντοπίστηκε στα προηγούμενα κεφάλαια μπορεί να θεωρηθεί ότι απαντάται σε μεγάλο βαθμό από τη σχεδίαση και την υλοποίηση του «GDPR ASSESSOR», υπό την έννοια ότι η εργασία δεν μένει σε θεωρητική πρόταση αλλά παρουσιάζει μια λειτουργική μεθοδολογία που γεφυρώνει ακριβώς τα σημεία όπου η βιβλιογραφία και η αγορά εμφανίζουν αδυναμίες. Συγκεκριμένα, το σύστημα υλοποιεί τον συνδυασμό δομημένων εισροών (schema-driven ερωτηματολόγια DPIA/Gap) με παραγωγή προσαρμοσμένου κειμένου (policy generation) μέσω LLM, καλύπτοντας το «τελευταίο μίλι» που συνήθως παραμένει χειροκίνητο: τη μετατροπή των ευρημάτων και των απαντήσεων σε συνεκτικό νομικό κείμενο πολιτικής. Επιπλέον, η επιλογή τοπικής εκτέλεσης του μοντέλου (Local AI μέσω Ollama/Llama 3) αντιμετωπίζει ευθέως το privacy paradox που αναδείχθηκε, καθώς μειώνει την ανάγκη αποστολής δεδομένων σε cloud υπηρεσίες. Τέλος, η ενσωμάτωση τεχνικού ελέγχου ιστοσελίδας (cookies/trackers) μέσα στην ίδια ροή εργασίας μειώνει την αποσπασματικότητα (siloed compliance) σε ό,τι αφορά τουλάχιστον το πεδίο της πολιτικής απορρήτου και της τεχνικής τεκμηρίωσης για web περιβάλλοντα, προσφέροντας μια πιο ενοποιημένη προσέγγιση από τις συνήθεις «λύσεις-σιλό».[63]

Παρά τα παραπάνω, είναι σημαντικό να σημειωθεί ότι η απάντηση του ερευνητικού κενού είναι ισχυρότερη σε επίπεδο αρχιτεκτονικής, υλοποίησης και αρχικής τεκμηρίωσης, και λιγότερο σε επίπεδο πλήρους εμπειρικής επικύρωσης. Δηλαδή, η εργασία δείχνει ότι το προτεινόμενο μοντέλο είναι τεχνικά εφικτό και λειτουργικά συνεκτικό, αλλά η πλήρης επιβεβαίωση ότι αποτελεί ώριμη, καθολικά εφαρμόσιμη λύση—ιδίως για ΜΜΕ—απαιτεί ευρύτερη αξιολόγηση σε πραγματικά περιβάλλοντα. Αυτό περιλαμβάνει δοκιμές χρηστικότητας με DPOs/χρήστες, ποσοτικές μετρήσεις εξοικονόμησης χρόνου/κόστους, και αξιολόγηση της ποιότητας/νομικής ακρίβειας των παραγόμενων πολιτικών από ειδικούς. Επομένως, το ερευνητικό κενό μπορεί να

χαρακτηριστεί ότι «καλύπτεται» σε μεγάλο βαθμό από τη συμβολή της παρούσας εργασίας, με σαφή ένδειξη πρακτικής εφαρμοσιμότητας, αλλά με ταυτόχρονη αναγνώριση ότι η τελική ωρίμανση της απάντησης προϋποθέτει περαιτέρω εμπειρική επικύρωση και συγκριτική αξιολόγηση στο πεδίο.[63]

8.2 Συμπεράσματα επί των αποτελεσμάτων

Στο πλαίσιο των αποτελεσμάτων της παρούσας διπλωματικής, προκύπτει ότι η κύρια συμβολή της εργασίας εντοπίζεται στην τεκμηριωμένη μετάβαση από την «καταγραφή» της συμμόρφωσης προς την παραγωγική υποστήριξη της συγγραφής, με κεντρικό σημείο αναφοράς την αυτόματη δημιουργία πολιτικής απορρήτου. Ειδικότερα, η εργασία ανέδειξε ότι το πραγματικό επιχειρησιακό βάρος για οργανισμούς—και ιδιαίτερα για μικρομεσαίες επιχειρήσεις—δεν περιορίζεται στη συμπλήρωση φορμών ή στη διατήρηση αρχείων (record keeping), αλλά στη συνεχή σύνθεση, επικαιροποίηση και συνεκτικοποίηση κειμένων πολιτικής που πρέπει να είναι κατανοητά, προσαρμοσμένα στον οργανισμό και συμβατά με το κανονιστικό πλαίσιο. Υπό αυτή την οπτική, η ανάπτυξη του «GDPR ASSESSOR» λειτουργεί ως εμπειρική απόδειξη ότι η παραγωγή κειμένων πολιτικής απορρήτου μπορεί να ενταχθεί σε μια ελεγχόμενη, επαναλήψιμη και τεχνικά ασφαλή ροή εργασίας.[63]

Τα αποτελέσματα δείχνουν ότι η χρήση δομημένων ερωτηματολογίων (DPIA και Gap Analysis) ως πρωτογενούς μηχανισμού συλλογής και τυποποίησης πληροφορίας παρέχει ένα αξιόπιστο υπόστρωμα για τη δημιουργία πολιτικής απορρήτου. Η schema-driven προσέγγιση (αρχεία JSON) επιτρέπει την αντιστοίχιση των εισροών σε σαφείς ενότητες περιεχομένου (π.χ. σκοποί επεξεργασίας, κατηγορίες δεδομένων, αποδέκτες, χρονικά όρια τήρησης, μέτρα ασφάλειας), με αποτέλεσμα η πολιτική να μην παράγεται ως γενικό «πρότυπο», αλλά ως κείμενο που αντανακλά τις δηλωμένες πρακτικές του οργανισμού. Επιπλέον, η ενσωμάτωση μεταδεδομένων και νομικών παραπομπών στα σχήματα ενισχύει την ιχνηλασιμότητα του τελικού κειμένου, καθώς καθιστά σαφές ποια τμήματα της πολιτικής αντιστοιχούν σε συγκεκριμένες κανονιστικές απαιτήσεις.[63]

Κρίσιμο εύρημα της υλοποίησης είναι ότι η ενσωμάτωση ενός τοπικά εκτελούμενου Μεγάλου Γλωσσικού Μοντέλου (Llama 3 μέσω Ollama) μπορεί να λειτουργήσει αποτελεσματικά ως μηχανισμός «κειμενοποίησης» για πολιτικές απορρήτου, όταν η λειτουργία του περιορίζεται αυστηρά σε δομημένο πλαίσιο. Η χρήση system prompts, η αποφυγή ελεύθερης συνομιλίας και η τροφοδότηση του μοντέλου αποκλειστικά με τα δομημένα δεδομένα που παρήχθησαν από τα ερωτηματολόγια (context injection) συνέβαλαν στη μείωση της πιθανότητας παραγωγής ανακριβών ή αυθαίρετων διατυπώσεων. Με τον τρόπο αυτό, η παραγωγή πολιτικής απορρήτου αναβαθμίζεται από μια χειροκίνητη, χρονοβόρα διαδικασία σε μια ημι-αυτοματοποιημένη ροή, όπου ο άνθρωπος διατηρεί τον ρόλο του τελικού ελεγκτή (human-in-the-loop), ενώ το σύστημα αναλαμβάνει την αρχική σύνθεση και τη δομική οργάνωση του περιεχομένου.[63]

Παράλληλα, η επιλογή τοπικής εκτέλεσης ενισχύει ουσιαστικά τη διάσταση της ιδιωτικότητας σε επίπεδο αρχιτεκτονικής, αντιμετωπίζοντας το παράδοξο που αναδείχθηκε στη βιβλιογραφία για την χρήση cloud-based AI σε σενάρια ευαίσθητων δεδομένων. Η μη αποστολή εισροών σε τρίτους παρόχους συνιστά σημαντικό πλεονέκτημα για οργανισμούς που επιδιώκουν διακυβέρνηση και κυριαρχία δεδομένων (data sovereignty) [64]. Ταυτόχρονα, η ενσωμάτωση τεχνικού ελέγχου ιστοσελίδας (cookie/trackers audit) προσθέτει ένα επίπεδο πρακτικής

επαλήθευσης που μπορεί να τροφοδοτήσει με πιο αντικειμενικά δεδομένα τα σχετικά τμήματα της πολιτικής απορρήτου (π.χ. τεχνολογίες παρακολούθησης), μειώνοντας την απόκλιση μεταξύ «δηλωμένων» πρακτικών και πραγματικής συμπεριφοράς του web περιβάλλοντος.

Ωστόσο, τα αποτελέσματα ανέδειξαν και συγκεκριμένους περιορισμούς που επηρεάζουν κυρίως την ποιότητα της παραγόμενης πολιτικής σε σύνθετα σενάρια. Τα μικρότερα τοπικά μοντέλα (π.χ. 8B παραμέτρων) εμφανίζουν μειωμένη ικανότητα σε σύνθετη νομική συλλογιστική και λεπτές διατυπώσεις, σε σύγκριση με εμπορικά frontier models, γεγονός που μπορεί να οδηγήσει σε περισσότερο γενικευμένες ή λιγότερο ακριβείς διατυπώσεις όταν το πλαίσιο επεξεργασίας είναι πολύπλοκο [65]. Αυτό υποδηλώνει ότι, παρότι η τοπική εκτέλεση ισχυροποιεί την ασφάλεια, η επίτευξη υψηλής ποιότητας πολιτικής απορρήτου εξαρτάται από τη σωστή ισορροπία μεταξύ μοντέλου, δομημένων εισροών και ανθρώπινης επιμέλειας. Συνεπώς, η τεχνολογία λειτουργεί καταλληλότερα ως εργαλείο ενίσχυσης και επιτάχυνσης της συγγραφής, παρά ως υποκατάστατο της νομικής κρίσης.

Συμπερασματικά, τα αποτελέσματα της εργασίας καταδεικνύουν ότι η παραγωγή πολιτικής απορρήτου μπορεί να τεθεί στο κέντρο μιας ενοποιημένης, ελεγχόμενης και ασφαλούς διαδικασίας, η οποία συνδέει δομημένη αποτύπωση πρακτικών (DPIA/Gap), τεχνική επιβεβαίωση (web audit) και παραγωγική σύνθεση κειμένου (local LLM). Η παρούσα υλοποίηση προσφέρει ένα αναπαραγώγιμο παράδειγμα που υποστηρίζει εμπειρικά τη δυνατότητα μιας «Παραγωγικής» προσέγγισης στη συμμόρφωση, με σαφή πρακτική αξία για οργανισμούς περιορισμένων πόρων, υπό την προϋπόθεση ότι η τελική ευθύνη και ο έλεγχος παραμένουν στον ανθρώπινο παράγοντα.[65]

8.3 Συμπεράσματα επί της μεθοδολογίας

Από την οπτική μιας συνολικής αποτίμησης, η επιλογή της Design Science Research (DSR) κρίνεται κατάλληλη για το ερευνητικό αντικείμενο της εργασίας, επειδή το πρόβλημα που τίθεται δεν είναι μόνο θεωρητικό αλλά πρωτίστως πρακτικό: η υπέρμετρη γραφειοκρατική επιβάρυνση γύρω από τον GDPR και, ειδικότερα, η δυσκολία παραγωγής και διαρκούς συντήρησης κειμένων όπως η πολιτική απορρήτου. Η DSR, ως μεθοδολογία που στοχεύει στη δημιουργία και τεκμηρίωση λειτουργικών τεχνουργημάτων, ευθυγραμμίζεται με τη βασική επιδίωξη της εργασίας: να προτείνει μια εφαρμόσιμη λύση και να δείξει, μέσω υλοποίησης, ότι η λύση αυτή μπορεί να λειτουργήσει ως ρεαλιστικό εργαλείο υποστήριξης του DPO, αντί να περιοριστεί σε αφηρημένες περιγραφές ή σε «γενικές» κατευθύνσεις συμμόρφωσης.[65]

Ως θετικό στοιχείο της εφαρμογής της μεθοδολογίας, η αρθρωτή (modular) σχεδίαση αξιολογείται ως ιδιαίτερα αποτελεσματική επιλογή. Η διάσπαση του συστήματος σε διακριτά υποσυστήματα—ιδίως το Audit Module και το Policy Engine—επέτρεψε την ανεξάρτητη ανάπτυξη, τον στοχευμένο έλεγχο και τη σταδιακή ολοκλήρωση κρίσιμων λειτουργιών. Αυτό μείωσε τη συνολική πολυπλοκότητα και ενίσχυσε την επαληθευσιμότητα της υλοποίησης, καθώς κάθε υποσύστημα μπορούσε να αξιολογηθεί με βάση συγκεκριμένες εισροές και αναμενόμενα αποτελέσματα. Επιπλέον, η δομή αυτή υποστηρίζει άμεσα την κεντρική υπόθεση της εργασίας: ότι η παραγωγή πολιτικής απορρήτου μπορεί να στηριχθεί σε ελεγχόμενες και δομημένες εισροές, οι οποίες προκύπτουν από διαδικασίες αξιολόγησης (DPIA/Gap) και τεχνικά ευρήματα (π.χ. cookies/trackers).[65]

Παράλληλα, η βασική αδυναμία που προκύπτει αφορά το σκέλος της αξιολόγησης και, ειδικότερα, την εξωτερική εγκυρότητα των συμπερασμάτων. Η αξιολόγηση βασίστηκε κυρίως σε use cases και συνθετικά δεδομένα, κάτι που είναι εύλογο σε επίπεδο πρωτοτύπου, αλλά δεν επαρκεί για να επιβεβαιωθεί πλήρως ότι το σύστημα θα αποδώσει με τον ίδιο τρόπο σε περιβάλλον παραγωγής, με πραγματικούς DPOs, πραγματικές οργανωτικές διαδικασίες και πραγματικούς περιορισμούς χρόνου/τεχνικής ωριμότητας. Σε αυτό το σημείο, είναι πιθανό να υπάρχουν πρακτικά ζητήματα χρηστικότητας (UX), ενσωμάτωσης στη ροή εργασίας και αποδοχής/εμπιστοσύνης που δεν αναδεικνύονται σε εργαστηριακές συνθήκες. Συνεπώς, η μεθοδολογία επιτυγχάνει ισχυρή τεκμηρίωση της τεχνικής εφικτότητας και της συνοχής της προσέγγισης, αλλά αφήνει ως αναγκαίο επόμενο βήμα την ευρείας κλίμακας πιλοτική αξιολόγηση.

Ως προς τα τέσσερα ερευνητικά ερωτήματα, η συνολική εικόνα είναι κατά βάση θετική, με σαφείς προϋποθέσεις.

- Για το πρώτο ερώτημα, τα αποτελέσματα δείχνουν ότι είναι εφικτό να σχεδιαστεί ένα σύστημα που καθοδηγεί βήμα-προς-βήμα τη διενέργεια DPIA και Gap Analysis. Ο συνδυασμός schema-driven ερωτηματολογίων, θεματικής ομαδοποίησης και σύνδεσης με άρθρα του GDPR συγκροτεί μια δομημένη, επαναχρησιμοποιήσιμη διαδικασία που μειώνει την πιθανότητα παράλειψης κρίσιμων σημείων και δημιουργεί εισροές κατάλληλες για περαιτέρω αξιοποίηση. [65]
- Για το δεύτερο ερώτημα, η ενσωμάτωση τοπικού LLM (Llama 3 μέσω Ollama) τεκμηριώνει ότι η παραγωγή κειμένων πολιτικής—με κέντρο βάρους την πολιτική απορρήτου—μπορεί να αυτοματοποιηθεί σε σημαντικό βαθμό όταν το μοντέλο λειτουργεί σε αυστηρά ελεγχόμενο πλαίσιο και τροφοδοτείται με δομημένα δεδομένα. Εδώ η ανθρώπινη εποπτεία παραμένει κρίσιμη, όχι ως αδυναμία αλλά ως αναγκαία συνθήκη για νομικά δεσμευτικά κείμενα, ενώ τα αποτελέσματα υποστηρίζουν ότι ο χρόνος σύνταξης και αναθεώρησης μπορεί να μειωθεί αισθητά. [65]
- Για το τρίτο ερώτημα, η υλοποίηση καταδεικνύει ότι η modular αρχιτεκτονική, ο διαχωρισμός περιεχομένου–λογικής και η αποθήκευση των ερωτηματολογίων σε JSON διευκολύνουν την προσαρμογή σε μελλοντικές αλλαγές χωρίς ριζικό ανασχεδιασμό, ενισχύοντας τη συντηρησιμότητα και την επεκτασιμότητα.
- Για το τέταρτο ερώτημα, τα ευρήματα υποδηλώνουν ότι το σύστημα μπορεί να αποτελέσει ρεαλιστική και οικονομικά προσιτή εναλλακτική για ΜΜΕ, τουλάχιστον σε επίπεδο πρωτοτύπου, λόγω της χρήσης ανοικτού κώδικα και της τοπικής εκτέλεσης που περιορίζει τόσο το λειτουργικό κόστος όσο και την εξάρτηση από εμπορικές cloud υπηρεσίες. Ωστόσο, η πλήρης επιβεβαίωση αυτού του συμπεράσματος απαιτεί πιλοτική εφαρμογή σε πραγματικούς οργανισμούς και συγκριτική αποτίμηση κόστους–οφέλους, ώστε να αξιολογηθεί η βιωσιμότητα, η αποδοχή και η λειτουργική ένταξη στο καθημερινό περιβάλλον εργασίας.

Συνολικά, η εργασία οδηγεί σε ένα ισορροπημένο συμπέρασμα: τα ερευνητικά ερωτήματα απαντώνται θετικά σε μεγάλο βαθμό σε επίπεδο σχεδιασμού, υλοποίησης και αρχικής τεκμηρίωσης, ενώ τα όρια της απάντησης σχετίζονται κυρίως με την ανάγκη ευρύτερης εμπειρικής αξιολόγησης στο πεδίο. Με άλλα λόγια, η εργασία δείχνει πειστικά ότι η παραγωγή πολιτικής απορρήτου μπορεί να μετατραπεί από χειροκίνητη, γραφειοκρατική εργασία σε ελεγχόμενη, υποβοηθούμενη

διαδικασία, όπου το LLM λειτουργεί ως επιταχυντής συγγραφής και ο άνθρωπος ως τελικός κριτής, με επόμενο βήμα την επιβεβαίωση της ωριμότητας της λύσης σε πραγματικές συνθήκες χρήσης.[65]

8.4 Συμπεράσματα επί των εργαλείων

Από τη σκοπιά της αξιολόγησης των τεχνολογικών επιλογών, η απόφαση να βασιστεί η υλοποίηση σε εργαλεία ανοικτού κώδικα φαίνεται να δικαιώνεται από το τελικό αποτέλεσμα, τόσο ως προς τη λειτουργικότητα όσο και ως προς τη στρατηγική στόχευση της εργασίας (προσιτή, αναπαραγώγιμη λύση με κέντρο την παραγωγή πολιτικής απορρήτου). [65]

Πρώτον, το πλαίσιο Flask ανταποκρίθηκε επαρκώς στις απαιτήσεις μιας «ελαφριάς» εφαρμογής, επιτρέποντας γρήγορη υλοποίηση της ροής εργασίας, καθαρό διαχωρισμό υποσυστημάτων και απλή ενσωμάτωση των μηχανισμών δυναμικής απόδοσης και εξαγωγής παραδοτέων. Υπό αυτή την έννοια, η επιλογή του Flask ενισχύει το επιχείρημα ότι για εφαρμογές τύπου RegTech/PrivacyTech, όπου προτεραιότητα είναι η ταχύτητα, η ευελιξία και η μικρή υπολογιστική επιβάρυνση, μια ελαφριά web αρχιτεκτονική μπορεί να είναι αποτελεσματικότερη από «βαριές» στοίβες λογισμικού [66].

Δεύτερον, το Ollama αναδεικνύεται ως κρίσιμο τεχνολογικό σημείο της εργασίας, επειδή κατέστησε εφικτή την τοπική εκτέλεση ενός LLM σε συμβατικό hardware, άρα υποστήριξε έμπρακτα τη βασική υπόθεση της εργασίας ότι η παραγωγή πολιτικής απορρήτου μπορεί να γίνει χωρίς cloud εξάρτηση. Με αυτόν τον τρόπο, η υλοποίηση δεν περιορίζεται σε θεωρητική επίκληση της “local AI” αρχής, αλλά δείχνει πρακτικά ότι προηγμένες δυνατότητες παραγωγής κειμένου μπορούν να γίνουν προσβάσιμες σε οργανισμούς περιορισμένων πόρων, μειώνοντας το φράγμα εισόδου σε τεχνολογίες που, μέχρι πρόσφατα, συνδέονταν με υποδομές υψηλής κλίμακας [54].

Τρίτον, η επιλογή αποθήκευσης των ερωτηματολογίων σε JSON (και γενικότερα η schema-driven λογική)αποδείχθηκε λειτουργική ως μηχανισμός ευελιξίας και συντηρησιμότητας: η ενσωμάτωση νέων ενοτήτων ή ρυθμιστικών οδηγιών μπορεί να πραγματοποιηθεί με αλλαγές στο επίπεδο περιεχομένου/σχήματος, χωρίς αναδιάρθρωση βάσης δεδομένων ή τροποποίηση του πυρήνα της εφαρμογής. Αυτό είναι ιδιαίτερα κρίσιμο σε κανονιστικά περιβάλλοντα, όπου οι απαιτήσεις τεκμηρίωσης εξελίσσονται και η δυνατότητα γρήγορης προσαρμογής αποτελεί πρακτικό κριτήριο βιωσιμότητας του εργαλείου. [54]

Συνολικά, οι επιλογές ανοικτού κώδικα δεν λειτουργούν μόνο ως «τεχνολογική προτίμηση», αλλά ως συνεπές μέσο υλοποίησης της κεντρικής επιδίωξης της εργασίας: μια ενοποιημένη, οικονομικά προσιτή και τεχνικά ασφαλής πλατφόρμα που υποστηρίζει την παραγωγή πολιτικής απορρήτου σε πραγματικές συνθήκες χρήσης.[54]

8.5 Προοπτικές / Επόμενα βήματα

Από την οπτική μιας συνολικής αξιολόγησης, τα παραπάνω καταδεικνύουν ότι η παρούσα εργασία δεν συνιστά ένα κλειστό και στατικό τεχνούργημα, αλλά μια αφετηρία για μια ευρύτερη ερευνητική και τεχνολογική πορεία στον χώρο της κανονιστικής τεχνολογίας και της παραγωγικής τεχνητής νοημοσύνης, με κεντρικό άξονα την αξιόπιστη παραγωγή και συντήρηση πολιτικών απορρήτου. Η υλοποίηση του «GDPR ASSESSOR» παρέχει ήδη ένα λειτουργικό παράδειγμα του πώς δομημένα ευρήματα (DPIA/Gap και τεχνικά audits) μπορούν να μετασχηματιστούν σε συνεκτικό κείμενο πολιτικής υπό ανθρώπινη εποπτεία· συνεπώς, οι μελλοντικές προεκτάσεις που προτείνονται δεν

αποτελούν «πρόσθετες ιδέες», αλλά φυσική συνέχιση των ορίων που ανέδειξε η αξιολόγηση: ανάγκη υψηλότερης ακρίβειας σε τοπικές δικαιοδοσίες, ανάγκη κάλυψης νέων κανονιστικών υποχρεώσεων, και ανάγκη ισχυρότερης εμπειρικής επικύρωσης στο πεδίο.[54]

Μία πρώτη και ιδιαίτερα ουσιαστική κατεύθυνση είναι η τοπικοποίηση του γλωσσικού μοντέλου μέσω fine-tuning σε σώμα κειμένων της Ελληνικής Αρχής Προστασίας Δεδομένων. Από αξιολογική σκοπιά, η πρόταση αυτή στοχεύει σε ένα κρίσιμο σημείο για την ποιότητα των παραγόμενων πολιτικών απορρήτου: ακόμη και όταν η παραγωγή γίνεται με αυστηρά δομημένο context, τα γενικά μοντέλα συχνά αποδίδουν καλύτερα σε "γενικές" διατυπώσεις παρά σε λεπτές ερμηνευτικές απαιτήσεις, ειδικά όταν αυτές διαμορφώνονται από τοπικές κατευθυντήριες γραμμές και πρακτικές. Η βιβλιογραφία υποστηρίζει ότι η εξειδίκευση σε συγκεκριμένες δικαιοδοσίες μπορεί να αυξήσει σημαντικά την ακρίβεια και τη χρησιμότητα σε νομικά σενάρια, κάτι που μεταφράζεται πρακτικά σε λιγότερη χειροκίνητη επιμέλεια και σε πιο συνεπή κείμενα πολιτικής [61]. Υπό αυτή την έννοια, το fine-tuning δεν αφορά απλώς «καλύτερο μοντέλο», αλλά πιο αξιόπιστη και τοπικά ευθυγραμμισμένη παραγωγή πολιτικής απορρήτου.

Μια δεύτερη κατεύθυνση αφορά την επέκταση του συστήματος ώστε να καλύψει απαιτήσεις του Ευρωπαϊκού Κανονισμού για την Τεχνητή Νοημοσύνη (AI Act), ο οποίος καθίσταται σταδιακά υποχρεωτικός έως το 2026. Από τη σκοπιά της RegTech, η κίνηση αυτή είναι στρατηγικά συνεπής: οι οργανισμοί που χρησιμοποιούν ή αναπτύσσουν συστήματα ΤΝ θα κληθούν να παράγουν νέα τεκμήρια και πολιτικές, ενώ σε πολλά πραγματικά σενάρια οι υποχρεώσεις του AI Act θα συνυπάρχουν με τις υποχρεώσεις που υπάρχουν στις πολιτικές απορρήτων. Η αναφορά στην ανάγκη εναρμόνισης και στη δημιουργία ζήτησης για ενιαία εργαλεία ελέγχου μέσω ενός ευρύτερου "Digital Omnibus" πλαισίου υπογραμμίζει ότι το μέλλον της συμμόρφωσης δεν είναι μονο-κανονιστικό αλλά πολυ-κανονιστικό, άρα απαιτεί εργαλεία που μπορούν να ενοποιούν διαδικασίες και παραδοτέα [67]. Για το «GDPR ASSESSOR», αυτό πρακτικά σημαίνει επέκταση των schemas, των ελέγχων και—κυρίως—των παραγόμενων κειμένων πολιτικής απορρήτου, ώστε η παραγωγή πολιτικών να παραμένει συνεπής και με τις δύο κανονιστικές σφαίρες.

Τρίτη κατεύθυνση είναι η διερεύνηση agentic AI, δηλαδή η μετάβαση από ένα μοντέλο που κυρίως παράγει κείμενο σε πράκτορες που μπορούν να εκτελούν ενέργειες υπό ανθρώπινη εποπτεία. Από αξιολογική σκοπιά, αυτή η προέκταση έχει υψηλό δυναμικό γιατί μετατοπίζει το σύστημα από «παραγωγή εγγράφων» προς «συνεχή συμμόρφωση» (continuous compliance): για παράδειγμα, ένας πράκτορας θα μπορούσε να προτείνει ή να εφαρμόζει αλλαγές ρυθμίσεων ασφαλείας, να ενεργοποιεί ελέγχους, ή να εισηγείται αυτόματη επικαιροποίηση τμημάτων της πολιτικής όταν αλλάζει το κανονιστικό πλαίσιο. Ωστόσο, ακριβώς επειδή οι πράκτορες εισάγουν ενεργητικές λειτουργίες με πραγματικές επιχειρησιακές συνέπειες, απαιτούνται ισχυρότερες δικλείδες λογοδοσίας, αυστηρό human-in-the-loop, και λεπτομερής καταγραφή ενεργειών, ώστε να αποφεύγονται μη αναστρέψιμα σφάλματα ή μη ελεγχόμενες παρεμβάσεις [68]. Επομένως, η agentic προσέγγιση αποτελεί γόνιμο ερευνητικό πεδίο, αλλά προϋποθέτει προσεκτική, σταδιακή υλοποίηση.

Τέλος, ανεξάρτητα από τις τεχνολογικές επεκτάσεις, μια καθοριστική κατεύθυνση μελλοντικής έρευνας είναι η συστηματική αξιολόγηση του εργαλείου σε πραγματικά περιβάλλοντα ΜΜΕ. Από θέση κριτή, αυτό είναι το βήμα που θα ενισχύσει αποφασιστικά την εξωτερική εγκυρότητα των συμπερασμάτων: θα επιτρέψει να αξιολογηθούν η χρηστικότητα, η αποδοχή, η

πραγματική μείωση χρόνου παραγωγής πολιτικής απορρήτου, καθώς και η ποιότητα των παραγόμενων κειμένων υπό πραγματικές οργανωτικές συνθήκες. Με αυτό τον τρόπο, οι προτεινόμενες προεκτάσεις δεν εμφανίζονται ως γενικές μελλοντικές ιδέες, αλλά ως στοχευμένες απαντήσεις στα επόμενα λογικά βήματα ωρίμανσης μιας πλατφόρμας που έχει ήδη τοποθετήσει την παραγωγή πολιτικής απορρήτου στο κέντρο μιας ελεγχόμενης, τοπικής και αναπαραγώγιμης ροής συμμόρφωσης.[68]

Βιβλιογραφία

[1] EU 2016/679, "General Data Protection Regulation," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Accessed: Jan. 28, 2026.

[2] DLA Piper, "GDPR Fines and Data Breach Survey: January 2024," 2024. [Online]. Available: https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024. Accessed: Jan. 28, 2026.

[3] Minaee et al., "Large Language Models: A Survey," 2024. [Online]. Available: https://arxiv.org/abs/2402.06196. Accessed: Jan. 28, 2026. doi:10.48550/arXiv.2402.06196.

[4] FRIL White Paper, "Simplifying Compliance through Explainable Intelligent Automation," 2024. [Online]. Available: https://strathprints.strath.ac.uk/89572/1/FRIL-WPS-2024-Simplifying-Compliance-Through-Explainable-Intelligent-Automation.pdf. Accessed: Jan. 28, 2026.

[5] Liu & Wongsosaputro, "Compliance Redefined: Using GenAI to Navigate a Complex Regulatory Landscape," 2024. [Online]. Available: https://www.ingentaconnect.com/content/hsp/jdb001/2024/00000008/00000004/art00004. Accessed: Jan. 28, 2026. doi:10.69554/LGTJ4498.

[6] Doc #US53615325, "IDC MarketScape: Worldwide Governance, Risk, and Compliance (GRC) Software Vendor Assessment, 2025," 2025. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=US53615325. Accessed: Jan. 28, 2026.

[7] "EDPB Guidelines 05/2020 on Consent," 2020. [Online]. Available: https://edpb.europa.eu. Accessed: Jan. 28, 2026.

[8] Butler & O'Brien, "Understanding RegTech for Digital Regulatory Compliance," 2019. [Online]. Available: https://doi.org/10.1007/978-3-030-02330-0_6. Accessed: Jan. 28, 2026. doi:10.1007/978-3-030-02330-0_6.

[9] Hevner et al., "Design Science in Information Systems Research," 2004. [Online]. Available: https://www.jstor.org/stable/25148625. Accessed: Jan. 28, 2026. doi:10.2307/25148625.

[10] Booch, Rumbaugh & Jacobson, "The Unified Modeling Language User Guide," 2005. [Online]. Available: https://dl.acm.org/doi/10.5555/1088874. Accessed: Jan. 28, 2026. doi:10.5555/1088874.

[11] DataNorth AI, "Local LLM: Privacy, Security, and Control," 2025. [Online]. Available: https://datanorth.ai/blog (search: "Local LLM: Privacy, Security, and Control"). Accessed: Jan. 28, 2026.

[12] Dahl et al., "Large Legal Fictions: Profiling Legal Hallucinations in LLMs," 2024. [Online]. Available: https://academic.oup.com/jla/article/16/1/64/7606432. Accessed: Jan. 28, 2026. doi:10.1093/jla/laae003.

[13] Voigt & von dem Bussche, "The EU General Data Protection Regulation," 2017. [Online]. Available: https://link.springer.com/book/10.1007/978-3-319-57959-7. Accessed: Jan. 28, 2026. doi:10.1007/978-3-319-57959-7.

[14] 2016, "CJEU Case C-582/14 — Breyer," 2016. [Online]. Available: https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN. Accessed: Jan. 28, 2026.

[15] WP248 rev.01, Article 29 Working Party, "Guidelines on DPIA," 2017. [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Accessed: Jan. 28, 2026.

[16] "ISO/IEC 27004:2016 — Information Security Management Measurement," 2016. [Online]. Available: https://www.iso.org/standard/64120.html. Accessed: Jan. 28, 2026.

[17] Cavoukian, "Privacy by Design: The 7 Foundational Principles," 2009. [Online]. Available: https://www.ipc.on.ca/en/media/1826/download?attachment=. Accessed: Jan. 28, 2026.

[18] ICO, "Guide to Accountability and Governance," 2023. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/. Accessed: Jan. 28, 2026.

[19] "Bee Group — e-Compliance GDPR, n.d.," [Online]. Available: https://www.bee.gr/e-compliance-gdpr/. Accessed: Jan. 28, 2026.

[20] "Priority Quality Consultants — eQualSuite GRC, n.d.," [Online]. Available: https://www.priority.com.gr/en/priority-equalsuite-the-first-greek-grc-software/. Accessed: Jan. 28, 2026.

[21] "Andersen Legal Greece — GDPR in a Box, n.d.," [Online]. Available: https://gdprinabox.eu/?lang=en. Accessed: Jan. 28, 2026.

[22] "GDPR Team — DPO & Compliance Services, n.d.," [Online]. Available: https://gdprteam.gr/. Accessed: Jan. 28, 2026.

[23] "Freen — WHISTLE (Whistleblowing App), n.d.," [Online]. Available: https://www.freen.gr/whistlefreen-app/. Accessed: Jan. 28, 2026.

[24] "Epsilon Informatics — GDPR Services, n.d.," [Online]. Available: https://www.epsilon-informatics.gr/en/lista-yphresies/business-compliance-gdpr. Accessed: Jan. 28, 2026.

[25] "Space Hellas — GRC Services, n.d.," [Online]. Available: https://www.space.gr/en/services/grc. Accessed: Jan. 28, 2026.

[26] Gadotti et al., "Anonymization: The Imperfect Science of Using Data While Preserving Privacy," 2024. [Online]. Available: https://www.science.org/doi/10.1126/sciadv.adn7053. Accessed: Jan. 28, 2026. doi:10.1126/sciadv.adn7053.

[27] "OneTrust — IDC MarketScape 2025 Press Release," 2025. [Online]. Available: https://www.onetrust.com/news/onetrust-is-named-a-leader-in-the-idc-marketscape-2025-worldwide-grc-software-report/.https://www.onetrust.com/news/onetrust-is-named-a-leader-in-the-idc-marketscape-2025-worldwide-grc-software-report/ Accessed: Jan. 28, 2026.

[28] "OneTrust — Platform Overview, n.d.," [Online]. Available: https://www.onetrust.com/platformhttps://www.onetrust.com/platform/. Accessed: Jan. 28, 2026.

[29] "OneTrust — Pricing Analysis (SmartSuite), n.d.," [Online]. Available: https://www.smartsuite.com/blog/onetrust-pricing. Accessed: Jan. 28, 2026.

[30] "CMP Comparison Article (Enzuzo), n.d.," [Online]. Available: https://www.enzuzo.com/blog/best-consent-management-platforms. Accessed: Jan. 28, 2026.

[31] "TrustArc — G2 Best Software Award 2025 Press Release," 2025. [Online]. Available: https://trustarc.com/press/trustarc-earns-a-top-spot-on-g2s-2025-best-software-awards-for-data-privacy/. Accessed: Jan. 28, 2026.

[32] "Osano — "No Fines, No Penalties" Pledge, n.d.," [Online]. Available: https://www.osano.com/pledge. Accessed: Jan. 28, 2026.

[33] Captain Compliance, "GDPR," 2024. [Online]. Available: https://captaincompliance.com/solutions/gdpr. Accessed: Jan. 28, 2026.

[34] "Simple Analytics × Usercentrics Partnership, n.d.," [Online]. Available: https://www.simpleanalytics.com/blog/closing-the-data-gap-simple-analytics-x-usercentrics. Accessed: Jan. 28, 2026.

[35] SourceForge, "GDPR compliance software listings," 2025. [Online]. Available: https://sourceforge.net/software/gdpr-compliance/. Accessed: Jan. 28, 2026.

[36] "Securiti.ai — SaaSworthy Profile, n.d.," [Online]. Available: https://www.saasworthy.com/product/securiti-ai. Accessed: Jan. 28, 2026.

[37] G2, "Best Governance, Risk & Compliance (GRC) products for 2025," 2025. [Online]. Available: https://www.g2.com/best-software-companies/top-governance-risk-and-compliance. Accessed: Jan. 28, 2026.

[38] "BigID — Discovery Foundation, n.d.," [Online]. Available: https://bigid.com/discovery-foundation/. Accessed: Jan. 28, 2026.

[39] "BigID — Forrester Wave Privacy Management Q4 2023," 2023. [Online]. Available: https://bigid.com/blog/forrester-wave-privacy-management-software-q4-2023/. Accessed: Jan. 28, 2026.

[40] "Gartner — Market Guide for Consent and Preference Management," 2024. [Online]. Available: https://cdn.lawreportgroup.com/acuris/files/Cybersecurity-New/Consent Management Gartner CPM Guide.pdf Accessed: Jan. 28, 2026.

[41] 2025, "Collibra — Analyst Recognition Press Release," 2025. [Online]. Available: https://www.collibra.com/company/newsroom/press-releases/collibra-has-been-continually-recognized-in-data-and-ai-governance-by-industry-analysts-in-2024. Accessed: Jan. 28, 2026.

[42] BARC, "BARC Score Data Intelligence Platforms 2024," 2024. [Online]. Available: https://www.quest.com/analyst-report/barc-score-data-intelligence-platforms-2024/. Accessed: Jan. 28, 2026.

[43] "Collibra — Reviews (PeerSpot), n.d.," [Online]. Available: https://www.peerspot.com/products/collibra-data-intelligence-platform-reviews. Accessed: Jan. 28, 2026.

[44] Reuters 2024, "Vanta — Funding Round," 2024. [Online]. Available: https://www.reuters.com/technology/sequoia-capital-backed-vanta-raises-funding-245-bln-valuation-2024-07-24/. Accessed: Jan. 28, 2026.

[45] TechCrunch 2024, "Vanta — Series C Funding," 2024. [Online]. Available: https://techcrunch.com/2024/07/24/trust-management-platform-vanta-raises-150m-series-c-now-valued-at-2-45b/. Accessed: Jan. 28, 2026.

[46] Katz, Bommarito & Blackman, "A general approach for predicting the behavior of the Supreme Court of the United States," 2017. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0174698. Accessed: Jan. 28, 2026. doi:10.1371/journal.pone.0174698.

[47] Chalkidis et al., "LEGAL-BERT," 2020. [Online]. Available: https://arxiv.org/abs/2010.02559. Accessed: Jan. 28, 2026. doi:10.48550/arXiv.2010.02559.

[48] Harkous et al., "Polisis: Automated Analysis of Privacy Policies," 2018. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-harkous.pdf. Accessed: Jan. 28, 2026. doi:10.48550/arXiv.1802.02561.

[49] "AI-Driven Anonymization: Protecting Personal Data Privacy While Leveraging Machine Learning (Yang et al.), arXiv:2402.17191," 2024. [Online]. Available: https://arxiv.org/abs/2402.17191. Accessed: Jan. 28, 2026.

[50] Oligo Security, "LLM Security in 2025," 2025. [Online]. Available: https://www.oligo.security/academy/llm-security-in-2025-risks-examples-and-best-practices. Accessed: Jan. 28, 2026.

[51] upGrad, "Advantages of Using Python for Artificial Intelligence Development," 2025. [Online]. Available: https://www.upgrad.com/blog/advantages-of-using-python-for-artificial-intelligence-development/. Accessed: Jan. 28, 2026.

[52] Netguru, "Python Pros and Cons in 2025," 2025. [Online]. Available: https://www.netguru.com/blog/python-pros-and-cons. Accessed: Jan. 28, 2026.

[53] Abbacus Technologies, "Top 20 Python-Based CMS in 2025 Suggested by Experts," 2025. [Online]. Available: https://www.abbacustechnologies.com/top-20-python-based-cms-in-2023-suggested-by-experts/. Accessed: Jan. 28, 2026.

[54] DZone, "Run LLMs Locally Using Ollama," 2025. [Online]. Available: https://dzone.com/articles/run-llms-locally-using-ollama. Accessed: Jan. 28, 2026.

[55] Cohorte Projects, "Run LLMs Locally with Ollama: Privacy-First AI for Developers in 2025," 2025. [Online]. Available: https://www.cohorte.co/blog/run-llms-locally-with-ollama-privacy-first-ai-for-developers-in-2025. Accessed: Jan. 28, 2026.

[56] Galileo AI, "Exploring Llama 3 Models: A Deep Dive," 2025. [Online]. Available: https://galileo.ai/blog/exploring-llama-3-models-a-deep-dive. Accessed: Jan. 28, 2026.

[57] "Llama (language model) — Wikipedia, n.d.,)," [Online]. Available: https://en.wikipedia.org/wiki/Llama_(language_model). Accessed: Jan. 28, 2026.

[58] arXiv, "DABstep: Data Agent Benchmark for Multi-step Reasoning," 2025. [Online]. Available: https://arxiv.org/abs/2506.23719. Accessed: Jan. 28, 2026.

[59] Stanford HAI, "AI on Trial: Legal Models Hallucinate in 1 out of 6 Benchmarking Queries," 2024. [Online]. Available: https://hai.stanford.edu/news/ai-trial-legal-models-hallucinate-1-out-6-or-more-benchmarking-queries. Accessed: Jan. 28, 2026.

[60] Cranium, "Why AI Still Needs a Human in the Loop," 2025. [Online]. Available: https://www.cranium.eu/why-ai-still-needs-a-human-in-the-loop-and-what-eu-law-says-about-it/. Accessed: Jan. 28, 2026.

[61] Medium, "Human-in-the-Loop AI: Balancing Autonomy with Oversight," 2025. [Online]. Available: https://medium.com/@amitkharche14/human-in-the-loop-ai-balancing-autonomy-with-oversight-07010b5657c9. Accessed: Jan. 28, 2026.

[62] "Reach New Heights: Paving the Way for Your Journey to the Cloud (EDRM), " 2025. [Online]. Available: https://edrm.net/2025/06/reach-new-heights-paving-the-way-for-your-journey-to-the-cloud/. Accessed: Jan. 28, 2026.

[63] NLSIU, "A Primer on Data Regulation and AI Development in India," 2025. [Online]. Available: https://forum.nls.ac.in/ijlt-blog-post/a-primer-on-data-regulation-and-ai-development-in-india/. Accessed: Jan. 28, 2026.

[64] "Understanding NetApp Instaclustr architectures, part 2: Running workloads in customer accounts (Instaclustr by NetApp), " 2025. [Online]. Available: https://www.instaclustr.com/blog/understanding-netapp-instaclustr-architectures-part-2-running-workloads-in-customer-accounts/. Accessed: Jan. 28, 2026.

[65] "The security paradox of local LLMs (Migdał, Quesma), " 2025. [Online]. Available: https://quesma.com/blog/local-llms-security-paradox/. Accessed: Jan. 28, 2026.

[66] Bitcot, "Flask vs Django," 2025. [Online]. Available: https://www.bitcot.com/flask-vs-django/. Accessed: Jan. 28, 2026.

[67] Bertelsmann Stiftung, "Simplifying with Responsibility: How Europe Can Make the AI Act More Practical," 2025. [Online]. Available: https://www.bertelsmann-stiftung.de/en/our-projects/reframetech-algorithmen-fuers-gemeinwohl/project-news/simplifying-with-responsibility-how-europe-can-make-the-ai-act-more-practical. Accessed: Jan. 28, 2026.

[68] PrajnaAI, "Inside the Agent's Mind: How AI Agents Decide What to Do Next," 2025. [Online]. Available: https://prajnaaiwisdom.medium.com/inside-the-agents-mind-how-ai-agents-decide-what-to-do-next-392e2d8672c5. Accessed: Jan. 28, 2026.

Παράρτημα Ι Οδηγός Εγκατάστασης για το GDPR-Assesor (Mac/Linux/W10/W11)

Το GDPR Assessor είναι ένα εργαλείο αξιολόγησης συμμόρφωσης που έχει υλοποιηθεί σε Python με Flask και λειτουργεί ως τοπική web εφαρμογή. Δεν διανέμεται ως κλασικό πρόγραμμα εγκατάστασης· εκτελείται στον υπολογιστή του χρήστη μετά τη λήψη του πηγαίου κώδικα από το GitHub. Ο παρών οδηγός περιγράφει συνοπτικά και με πρακτικό τρόπο τα βήματα εγκατάστασης και εκτέλεσης σε Windows 10/11 (64-bit).

Για να λειτουργήσει ομαλά η εφαρμογή, απαιτείται σύστημα με Windows 10 ή 11 64-bit, διαθέσιμη μνήμη τουλάχιστον 4 GB RAM (συνίσταται 8 GB για καλύτερη εμπειρία), καθώς και τουλάχιστον 1 GB ελεύθερου χώρου στον δίσκο για την εφαρμογή, μαζί με πρόσθετο χώρο για τις αναφορές και τα αρχεία εξαγωγής. Αρχικά χρειάζεται σύνδεση στο διαδίκτυο ώστε να ληφθεί ο κώδικας και οι βιβλιοθήκες, αν και είναι εφικτή και offline εγκατάσταση όταν υπάρχουν προετοιμασμένα πακέτα. Σε επίπεδο λογισμικού, είναι απαραίτητη η εγκατάσταση Python 3.11 ή νεότερης, επειδή η εφαρμογή αξιοποιεί τη σταθερά datetime.UTC που εισάγεται στην έκδοση 3.11. Προαιρετικά αλλά ιδιαίτερα χρήσιμο είναι το Git, καθώς επιτρέπει εύκολη κλωνοποίηση του αποθετηρίου και απλούστερες ενημερώσεις. Για τη χρήση της εφαρμογής απαιτείται επίσης ένας σύγχρονος browser (Chrome, Edge ή Firefox). Προαιρετικά εργαλεία που βελτιώνουν ή επεκτείνουν λειτουργίες είναι το Ollama για τοπική εκτέλεση LLM (η εφαρμογή συνδέεται σε τοπική υπηρεσία στη διεύθυνση http://localhost:11434) και το Pandoc για εναλλακτική ή εμπλουτισμένη δημιουργία PDF—αν και η εφαρμογή μπορεί να παράγει PDF και χωρίς αυτό.

Η εγκατάσταση ξεκινά με την εγκατάσταση της Python. Ο χρήστης κατεβάζει από το python.org τον 64-bit εγκαταστάτη (π.χ. 3.11.x ή 3.12.x), τον εκτελεί και φροντίζει να είναι ενεργοποιημένη η επιλογή “Add Python to PATH”, ώστε οι εντολές να αναγνωρίζονται από το τερματικό. Μετά την εγκατάσταση, είναι καλό να γίνει ένας σύντομος έλεγχος μέσω Windows Terminal ή PowerShell εκτελώντας python --version και pip --version. Αν η εντολή python δεν αναγνωρίζεται, συνήθως λειτουργεί η εναλλακτική py --version ή py -3.11 --version.

Στη συνέχεια, ο πηγαίος κώδικας μπορεί να ληφθεί με δύο τρόπους. Η πιο πρακτική επιλογή είναι η κλωνοποίηση με Git, όπου ο χρήστης αντιγράφει το URL του αποθετηρίου από το GitHub και εκτελεί σε τερματικό εντολές τύπου git clone <URL>, μέσα σε έναν φάκελο εργασίας (π.χ. Documents\Projects). Εναλλακτικά, μπορεί να γίνει λήψη ως ZIP από το GitHub και αποσυμπίεση σε έναν φάκελο (π.χ. Documents\GDPR Assessor), με αντίστοιχη μετάβαση σε αυτόν τον φάκελο μέσω τερματικού.

Αφού βρεθεί μέσα στον φάκελο του έργου, ο χρήστης δημιουργεί ένα εικονικό περιβάλλον ώστε να απομονωθούν οι εξαρτήσεις της εφαρμογής από το υπόλοιπο σύστημα. Αυτό γίνεται με python -m venv .venv (ή py -3.11 -m venv .venv αν χρειάζεται ρητή επιλογή έκδοσης). Έπειτα ενεργοποιείται το περιβάλλον, ανάλογα με το τερματικό: σε PowerShell με .\.venv\Scripts\Activate.ps1, σε Command Prompt με .\.venv\Scripts\activate.bat, ή σε Git Bash με source .venv/Scripts/activate. Αν στο PowerShell εμφανιστεί περιορισμός εκτέλεσης scripts, συνήθως επιλύεται με μία φορά την εντολή Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser, επανεκκίνηση του PowerShell και νέα ενεργοποίηση του venv. Όταν το

περιβάλλον ενεργοποιηθεί σωστά, εμφανίζεται συνήθως στην αρχή της γραμμής εντολών ένα πρόθεμα όπως (venv) ή (.venv).

Με ενεργό το εικονικό περιβάλλον, το επόμενο βήμα είναι η εγκατάσταση των εξαρτήσεων. Αρχικά συνιστάται αναβάθμιση του pip με python -m pip install --upgrade pip και στη συνέχεια εγκατάσταση των απαιτούμενων πακέτων από το requirements.txt με pip install -r requirements.txt. Τα πακέτα που εγκαθίστανται περιλαμβάνουν ενδεικτικά τις βιβλιοθήκες Flask, requests, jsonschema και reportlab. Ένας γρήγορος έλεγχος επιτυχούς εγκατάστασης μπορεί να γίνει με μια εντολή εισαγωγής βιβλιοθηκών, π.χ. python -c "import flask, requests, jsonschema, reportlab; print('OK')".

Για την εκτέλεση της εφαρμογής, αρκεί η εντολή python app.py. Στο τερματικό θα εμφανιστεί ότι ο server εκτελείται στη διεύθυνση http://127.0.0.1:5000/. Ο χρήστης ανοίγει αυτή τη διεύθυνση στον browser για να χρησιμοποιήσει την εφαρμογή, ενώ για έναν βασικό έλεγχο λειτουργίας μπορεί να επισκεφθεί το endpoint http://127.0.0.1:5000/healthz.

Τέλος, σε ό,τι αφορά την πρώτη πρόσβαση και τις βασικές ρυθμίσεις ασφαλείας, η εφαρμογή μπορεί να παρέχει προεπιλεγμένα διαπιστευτήρια για τοπικές δοκιμές. Αυτά πρέπει να χρησιμοποιούνται μόνο για δοκιμή και να αντικαθίστανται σε κανονική χρήση. Η αλλαγή τους γίνεται μέσω μεταβλητών περιβάλλοντος, συγκεκριμένα PLATFORM_USERNAME και PLATFORM_PASSWORD. Για παράδειγμα, σε PowerShell μπορούν να τεθούν προσωρινά με $env:PLATFORM_USERNAME="AdminUser" και $env:PLATFORM_PASSWORD="Ισχυρός_Κωδικός_123!" πριν την εκτέλεση του python app.py. Σε Command Prompt χρησιμοποιείται set αντί για $env:. Αν απαιτείται μόνιμη ρύθμιση στο προφίλ του χρήστη, μπορούν να χρησιμοποιηθούν setx PLATFORM_USERNAME "AdminUser" και setx PLATFORM_PASSWORD "Ισχυρός_Κωδικός_123!", με την προϋπόθεση ότι θα γίνει επανεκκίνηση του τερματικού. Για ανάγκες ανάπτυξης υπάρχει δυνατότητα παράκαμψης του login μέσω LOGIN_DISABLED=1, ωστόσο αυτό προορίζεται αυστηρά για development και δεν συνιστάται σε πραγματική χρήση.