

Ατομική Διπλωματική Εργασία

**“GRAPHICAL TOOL DEVELOPMENT FOR DEFINING
PRIVACY POLICIES”**

Ιωάννα Θεοφίλου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

**“GRAPHICAL TOOL DEVELOPMENT FOR DEFINING PRIVACY
POLICIES”**

Ιωάννα Θεοφίλου

Επιβλέπων Καθηγητής
Δρ. Γιώργος Παπαδόπουλος

Συνεπιβλέπουσα
Ευαγγελία Βανέζη

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2022

Ευχαριστίες

Με την βοήθεια του Θεού έχω φέρει εις πέρας αυτή την διπλωματική εργασία. Σε όλη την διάρκεια συγγραφής της εργασίας αυτής, έχω λάβει μεγάλη υποστήριξη και καθοδήγηση. Αρχικά θα ήθελα να ευχαριστήσω τον Επιβλέποντα Καθηγητή μου, Δρ. Γιώργο Παπαδόπουλο, ο οποίος με έχει εμπιστευτεί, και μου έδωσε την ευκαιρία να δουλέψω στο θέμα αυτό. Θα ήθελα να εκφράσω επίσης τις θερμές μου ευχαριστίες στην Ερευνήτρια και Συνεπιβλέπουσα μου κα. Ευαγγελία Βανέζη, για την βοήθεια και την εξαιρετική συνεργασία που είχαμε κατά την διάρκεια της εκπόνησης της διπλωματικής. Οι συμβουλές τους και η καθοδήγησή τους με βοήθησαν να τελειώσω με επιτυχία τον στόχο του.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου, αλλά και τους φίλους συμφοιτητές μου για την απέραντη ψυχολογική υποστήριξη και αγάπη τους.

Περίληψη

Στα πλαίσια της διπλωματικής εργασίας αυτής, έχει σχεδιαστεί και αναπτυχθεί ακολουθώντας την διαδικασία υλοποίησης λογισμικού, ένα “online” εργαλείο το οποίο προσφέρει την δυνατότητα ορισμού πολιτικών ιδιωτικότητας για ένα υπο-ανάπτυξη σύστημα, σε αυστηρά ορισμένη γλώσσα – τυπική γλώσσα (“formal language”) μέσω ενός εύχρηστου και απλού γραφικού περιβάλλοντος.

Έχουν μελετηθεί οι έννοιες της ιδιωτικότητας, των πολιτικών ιδιωτικότητας γενικά (χρησιμότητα και ανάγκη) αλλά και ειδικά, σε σχέση με το λογισμικό και τις τυπικές γλώσσες. Μετά από την έρευνα αυτή, έχει διεξαχθεί το συμπέρασμα ότι οι πολιτικές ιδιωτικότητας πρέπει να δηλώνονται με ένα τυπικό, δομημένο και αυστηρό τρόπο ο οποίος να είναι “machine-readable”, με απώτερο σκοπό τον έλεγχο συμβατότητας με το GDPR.

Λόγω του ότι η γραφική δήλωση αφορά υπό-ανάπτυξη συστήματα, το εργαλείο αυτό απευθύνεται σε άτομα που ασχολούνται με την υλοποίηση κάποιου συστήματος, όπως μηχανικούς λογισμικού, οι οποίοι δεν χρειάζεται να έχουν γνώσεις σχετικά με τις τυπικές γλώσσες. Η μετάφραση γίνεται αυτόματα από το εργαλείο.

Περιεχόμενα

Κεφάλαιο 1	Εισαγωγή.....	8
	1.1 Γενική Ιδέα	8
	1.2 Κίνητρα	8
	1.3 Γενικά για το εργαλείο	9
	1.4 Δομή Κειμένου Διπλωματικής Εργασίας	9
Κεφάλαιο 2	Έρευνα και Υπάρχοντα Εργαλεία.....	11
	2.1 Εισαγωγή	11
	2.2 Έρευνα	12
	2.2.1 “CompLicy : Evaluating the GDPR Alignment of Privacy Policies – a Study of Web Platforms”	12
	2.2.2 “DialogoP- A Language and a Graphical Tool for Formally Defining GDPR Purposes”	12
	2.2.3 “GDPR Compliance in the Design of INFORM e-Learning Platform: a Case Study”	13
	2.2.4 “Methods and tools for GDPR Compliance through Privacy and Data Protection Engineering”	14
	2.2.5 “Towards Defining Semantic Foundations for Purpose-Based Privacy Policies”	15
	2.3 Υπάρχοντα Εργαλεία	16
	2.4 Σύνοψη Μελέτης και Συμπεράσματα	17
Κεφάλαιο 3	Τεχνολογίες.....	18
	3.1 Εισαγωγή	18
	3.2 Front End Development	18
	3.2.1 JavaScript	18
	3.2.2 HTML5	19
	3.2.3 CSS3	19
	3.2.4 WordPress	19
	3.3 Back End Development	19
	3.3.1 PHP	19

Κεφάλαιο 4	Κύκλος Ζωής και ανάπτυξης Λογισμικού	21
4.1	Εισαγωγή / Μεθοδολογίες - περιγραφή	21
4.2	Έρευνα για Καταγραφή Απαιτήσεων και Προδιαγραφών	22
4.2.1	Μέθοδος έρευνας	22
4.2.2	Ερωτηματολόγιο	23
4.2.3	Αποτελέσματα	24
4.3	Προδιαγραφές	27
4.4	Μοντέλο της Πρωτοτυποποίησης	28
4.4.1	Εισαγωγή – “Throw-away prototyping”	28
4.4.2	Τεχνολογίες που Χρησιμοποιήθηκαν	28
4.4.3	Πρωτότυπο 1 – Πρώτη έκδοση	29
4.4.3.1	Σχεδίαση και Οθόνες	29
4.4.3.2	Έρευνα Αξιολόγησης Πρώτης έκδοσης	31
4.4.4	Πρωτότυπο 2 – Δεύτερη έκδοση	32
4.4.4.1	Σχεδίαση και Οθόνες	33
4.4.4.2	Έρευνα Αξιολόγησης Δεύτερης έκδοσης	33
4.4.5	Πρωτότυπο 3 – Τρίτη έκδοση	34
4.4.5.1	Σχεδίαση και Οθόνες	34
4.4.5.2	Έρευνα Αξιολόγησης Τρίτης έκδοσης	38
4.5	Σχεδιασμός Εργαλείου	39
4.5.1	Αρχιτεκτονική	39
4.5.2	Διαδικασία Σχεδίασης	39
4.5.2.1	“The design Process”	40
4.5.2.2	“Network Diagram”	41
4.6	Υλοποίηση Εργαλείου	42
4.6.1	Επεξήγηση Δομής Γραφικής Δήλωσης	42
4.6.2	Επεξήγηση Δομής Μετατροπής σε Τυπική Γλώσσα	44
4.6.2.1	Η τυπική γλώσσα που χρησιμοποιείται	44
4.6.2.2	Διαδικασία Μετατροπής	45
Κεφάλαιο 5	Επίδειξη Εργαλείου.....	47
5.1	Γενικές Λειτουργίες	47
5.1.1	Αρχική Σελίδα - “Login” – “Register” – “View Account”	47
5.1.2	“Main Menu” & Formal Methods Page	49
5.2	“Policy Menu” σελίδα	51
5.2.1	“Policy Tree”	51

5.2.1.1 “Policy Canvas”	52
5.2.1.2 “Palette”	52
5.2.1.3 “Instructions”	53
5.2.2 “Upload Policy”	54
Κεφάλαιο 6 Αξιολόγηση Εργαλείου.....	55
6.1 Εισαγωγή	55
6.2 Μεθοδολογία	55
6.3 Ερωτηματολόγιο	56
6.3.1 Περιγραφή και κίνητρα διεξαγωγής Έρευνας	56
6.3.2 Σενάριο Αξιολόγησης	57
6.3.3 Αποτελέσματα Σεναρίου	58
6.4 Αποτελέσματα Έρευνας / Ερωτηματολογίου	60
Κεφάλαιο 7 Συμπεράσματα.....	62
7.1 Συμπεράσματα	62
7.2 Μελλοντική Δουλειά	62
Βιβλιογραφία	64
Παράρτημα Α.....	66
Παράρτημα Β.....	80
Παράρτημα Γ.....	84

Κεφάλαιο 1

Εισαγωγή

1.1 Γενική Ιδέα	8
1.2 Κίνητρα	8
1.3 Γενικά για το εργαλείο	9
1.4 Δομή Κειμένου Διπλωματικής Εργασίας	9

1.1 Γενική Ιδέα

Η διπλωματική αυτή είχε σκοπό να μελετήσει την ιδιωτικότητα και τις πολιτικές ιδιωτικότητας, γενικά (χρησιμότητα, ανάγκη), αλλά και ειδικά σε σχέση με το λογισμικό και τις τυπικές γλώσσες. Έχουν μελετηθεί τα πιο κάτω: υφιστάμενα εργαλεία που υποστηρίζουν τον χρήστη (software engineer) να δηλώνει πολιτικές δεδομένων για ένα υπο-ανάπτυξη σύστημα, η ύπαρξη αυστηρών γλωσσών δήλωσης πολιτικών για συστήματα λογισμικού και η ενσωμάτωση αυτών στην διαδικασία ανάπτυξης λογισμικού, καθώς και η ανάγκη για την ύπαρξη ενός τέτοιου συστήματος. Στην μελέτη αυτή έχει διεξαχθεί μία βιβλιογραφική έρευνα και διερεύνηση της ανάγκης μέσω ερωτηματολογίου που απευθύνεται σε μηχανικούς λογισμικού.

Ακολουθώντας στην διπλωματική εργασία έχει σχεδιαστεί και αναπτυχθεί ακολουθώντας της διαδικασία υλοποίησης λογισμικού, ένα εργαλείο το οποίο προσφέρει την δυνατότητα ορισμού πολιτικών ιδιωτικότητας για ένα υπο-ανάπτυξη σύστημα, σε αυστηρά ορισμένη γλώσσα μέσω ενός εύχρηστου και απλού γραφικού περιβάλλοντος.

Έχει γίνει ο ορισμός των προδιαγραφών, ο σχεδιασμός καθώς και η ανάπτυξη του εργαλείου. Το τελευταίο κομμάτι της διπλωματικής εργασίας αφορά την αξιολόγηση του εργαλείου από μηχανικούς λογισμικού, που φανερώνει κατά πόσο το τελικό προϊόν είναι χρήσιμο και εύχρηστο.

1.2 Κίνητρα

Μετά από μελέτη διαφόρων άρθρων σχετικά με το θέμα, θεωρείται επιτακτική ανάγκη οι πολιτικές ιδιωτικότητας να δηλώνονται με ένα τυπικό και δομημένο τρόπο, για να γίνεται

πιο αυστηρά ο έλεγχος συμβατότητας ενός συστήματος με τις πολιτικές του. Το εργαλείο που έχει αναπτυχθεί, απευθύνεται κυρίως σε άτομα που ασχολούνται με την διαδικασία ανάπτυξης συστημάτων, όπως τεχνικούς λογισμικού ή και νομικές οντότητες ενός οργανισμού. Έτσι θα πρέπει να παρέχει ένα γραφικό περιβάλλον χρήσης, χωρίς να απαιτεί από τους χρήστες να γνωρίζουν την χρήση των τυπικών μεθόδων, και έπειτα να μπορεί να μεταφράζει αυτόματα την γραφική δήλωση πολιτικών ιδιωτικότητας σε τυπικές δηλώσεις.

Είναι κοινώς παραδεκτό ότι το πιο δύσκολο κομμάτι είναι ο έλεγχος κατά πόσο ένα σύστημα είναι συμβατό με το GDPR και τις πολιτικές ιδιωτικότητας του. Συχνά στην τεχνολογία λογισμικού χρησιμοποιούμε μεθόδους ελέγχου που δεν μπορούν να εγγυηθούν την επαλήθευση μιας ιδιότητας. Οι “Formal Methods” έχουν σκοπό να επιλύσουν το πιο πάνω θέμα χρησιμοποιώντας τυπικές γλώσσες και εργαλεία για την αυστηρή δήλωση, μοντελοποίηση και επιβεβαίωση των όσων χρειάζονται. Η μελέτη αυτή ήταν απαραίτητη για την κατανόηση της ανάγκης και του απώτερου σκοπού τον οποίο υποστηρίζει το εργαλείο που έχει αναπτυχθεί στα πλαίσια της διπλωματικής εργασίας, που είναι να γίνεται ο έλεγχος αυτός αυτοματοποιημένα.

1.3 Γενικά για το εργαλείο

Το εργαλείο στηρίζεται στην ιδέα ενός Web-based συστήματος και έχει ονομαστεί “privacyDef”, εξ ‘ου και η ονομασία της ιστοσελίδας. Γενικά ένα web-based σύστημα παρέχει οργάνωση, χρηστικότητα και εξοικονόμηση υπολογιστικού χώρου αφού τίποτα δεν θα φυλάγεται τοπικά. Στην ουσία δεν χρειάζεται να κατεβάσει κάποιο εργαλείο ο χρήστης. Είναι ένα online εργαλείο μέσω του οποίου ο κάθε χρήστης έχει ένα λογαριασμό για να του παρέχεται η υπηρεσία της γραφικής δήλωσης πολιτικών ιδιωτικότητας.

Το εργαλείο θεωρεί δεδομένο ότι ο χρήστης έχει μία αρχική ιδέα της πολιτικής του. Δεν βοηθά δηλαδή τον χρήστη να βρει τις πολιτικές του συστήματος του. Τον βοηθά να τις δηλώσει γραφικά και να μετατρέψει τις δηλώσεις αυτές σε μία τυπική γλώσσα. Παρέχει δηλαδή ένα “easy-to-use” περιβάλλον και δεν απαιτεί κάποια προηγούμενη γνώση από τον χρήστη σχετικά με τις τυπικές μεθόδους.

1.4 Δομή Κειμένου Διπλωματικής Εργασίας

Το κείμενο διπλωματικής εργασίας, διαχωρίζεται σε επτά μέρη. Αρχικά στο πρώτο μέρος παρουσιάστηκαν γενικές πληροφορίες σχετικά με το εργαλείο και τα διάφορα κίνητρα

της δημιουργίας του. Μετά, αναλύεται η έρευνα που έχει γίνει για κατανόηση του θέματος και για υποστήριξη των κινήτρων, ενώ στη συνέχεια αναφέρονται οι διάφορες τεχνολογίες που χρησιμοποιήθηκαν στην διαδικασία υλοποίησης του εργαλείου. Έπειτα παρουσιάζεται ο κύκλος ζωής και ανάπτυξης λογισμικού που έχει ακολουθηθεί, όπου αναλύονται όλα τα στάδιά του. Στο πέμπτο κεφάλαιο διαφαίνονται όλες οι λειτουργίες του εργαλείου και στο ακριβώς επόμενο κεφάλαιο, το εργαλείο αξιολογείται από δέκα μηχανικούς λογισμικού. Τέλος, παρουσιάζονται τα συμπεράσματα αυτής της διατριβής αλλά και ιδέες για μελλοντική δουλειά.

Κεφάλαιο 2

Έρευνα και Υπάρχοντα Εργαλεία

2.1	Εισαγωγή	11
2.2	Έρευνα	12
2.2.1	“CompLicy : Evaluating the GDPR Alignment of Privacy Policies – a Study of Web Platforms”	12
2.2.2	“DialogoP- A Language and a Graphical Tool for Formally Defining GDPR Purposes”	12
2.2.3	“GDPR Compliance in the Design of INFORM e-Learning Platform: a Case Study”	13
2.2.4	“Methods and tools for GDPR Compliance through Privacy and Data Protection Engineering”	14
2.2.5	“Towards Defining Semantic Foundations for Purpose-Based Privacy Policies”	15
2.3	Υπάρχοντα Εργαλεία	16
2.4	Σύνοψη Μελέτης και Συμπεράσματα	17

2.1 Εισαγωγή

Στην ενότητα αυτή παρουσιάζονται διάφορα επιστημονικά άρθρα μέσα στα πλαίσια της μελέτης της έννοιας της ιδιωτικότητας γενικά και ειδικά, αλλά και της σημαντικότητάς της. Έχει μελετηθεί ο τρόπος με τον οποίο το GDPR συνδέεται με τις πολιτικές ιδιωτικότητας, αφού είναι ένας τρόπος με τον οποίο έχουν τεθεί κάποια πλαίσια στην νομιμότητα επεξεργασίας, συλλογής και αποθήκευσης προσωπικών δεδομένων. Ταυτόχρονα, έχει μελετηθεί η έννοια του “Purpose”, ο τρόπος που συνδέεται με το GDPR, αλλά και τις πολιτικές ιδιωτικότητας. Συμπεραίνεται ότι, οι πολιτικές ιδιωτικότητας είναι μία νόμιμη «συμφωνία» μεταξύ χρηστών και συστήματος, η οποία δηλώνει ποια δεδομένα χρηστών θα χρησιμοποιηθούν, πώς θα χρησιμοποιηθούν και θα αποθηκευτούν, αλλά και ποια δικαιώματα επιβάλλεται οι χρήστες να γνωρίζουν[1]. Είναι δηλώσεις γραμμένες σε φυσική γλώσσα με σκοπό να τις διαβάζουν οι χρήστες.

Στην συνέχεια, έχει μελετηθεί η ανάγκη για “Τυπικές Μεθόδους”. Είναι κοινώς παραδεκτό ότι το πιο δύσκολο κομμάτι είναι ο έλεγχος κατά πόσο ένα σύστημα είναι συμβατό με το GDPR και τις πολιτικές ιδιωτικότητας του. Συχνά στην τεχνολογία

λογισμικού χρησιμοποιούμε μεθόδους ελέγχου που δεν υποστηρίζουν την επίσημη επαλήθευση της συμβατότητας του συστήματος. «Τυπικές μέθοδοι» είναι μαθηματικές προσεγγίσεις που περιλαμβάνουν γλώσσες και εργαλεία που χρησιμοποιούνται για την αυστηρή προδιαγραφή και μοντελοποίηση συστημάτων και την επαλήθευση συγκεκριμένων ιδιοτήτων. Οι «Τυπικές Μέθοδοι» μπορούν να επιλύσουν το πιο πάνω θέμα χρησιμοποιώντας τυπικές γλώσσες και εργαλεία, για την αυστηρή δήλωση, μοντελοποίηση και επιβεβαίωση των όσων χρειάζονται.

2.2 Έρευνα

2.2.1 “CompLicy : Evaluating the GDPR Alignment of Privacy Policies – a Study of Web Platforms”[1]

Στο άρθρο αυτό φαίνεται πώς οι πολιτικές ιδιωτικότητας σχετίζονται με το GDPR και κατ’ επέκταση κατά πόσο ο κώδικας ενός συστήματος ακολουθεί τους κανόνες του. Για την μελέτη των σημείων αυτών, οι συγγραφείς αποφάσισαν να εξετάσουν διάφορες πλατφόρμες διαδικτύου λόγω του ότι είναι εύκολα προσβάσιμες. Για να επιτευχθεί αυτό, έχουν δημιουργήσει το CompLicy εργαλείο του οποίου ο σκοπός είναι να σαρώνει μία σελίδα μίας διαδικτυακής πλατφόρμας και να εντοπίζει σε ποια πολιτική ιδιωτικότητας απευθύνεται.

Ο κύριος στόχος του CompLicy είναι να βοηθήσει τους χρήστες στην κατανόηση του GDPR και να επεκτείνει τις δυνατότητες των μηχανικών λογισμικού αφού θα μπορούν εύκολα πλέον να αναγνωρίσουν τους κανόνες του GDPR που υλοποιούνται στα διάφορα συστήματά τους.

Για την αναγνώριση κατά πόσο ένα σύστημα είναι συμβατό με το GDPR, οι συγγραφείς έχουν δημιουργήσει μία λίστα με τους βασικούς του κανόνες, οι οποίοι δηλώνουν τους όρους και τα δικαιώματα των χρηστών. Η τελική έκδοση της λίστας αυτής περιλαμβάνει 89 όρους κατηγοριοποιημένους σε ομάδες. Η σάρωση της σελίδας από το εργαλείο θεωρείται επιτυχής εάν τουλάχιστον ένας όρος από κάθε ομάδα υλοποιείται από τον κώδικα.

Έπειτα, το άρθρο παρουσιάζει αποτελέσματα ελέγχου συμβατότητας 148 διαφορετικών διαδικτυακών σελίδων, χρησιμοποιώντας το εργαλείο.

Καταληκτικά, οι συγγραφείς σημειώνουν την ανάγκη των πολιτικών ιδιωτικότητας, ειδικά σε πλατφόρμες διαδικτύου.

2.2.2 “DialogoP- A Language and a Graphical Tool for Formally Defining GDPR Purposes”[2]

Το άρθρο “DialogoP- A Language and a Graphical Tool for Formally Defining GDPR Purposes”, επικεντρώνεται στον όρο του ‘purpose’, το GDPR και πώς δημιουργείται ένα συμβατό στους κανόνες λογισμικό χρησιμοποιώντας τυπικές μεθόδους αλλά και μεθόδους “type-checking”.

Ο όρος ‘purpose’ είναι ένα πολύ σημαντικό κομμάτι στις πολιτικές ιδιωτικότητας ενός συστήματος. Δηλώνει τον τρόπο με τον οποίο συλλέγονται προσωπικά δεδομένα, πώς επεξεργάζονται και πώς χρησιμοποιούνται.

Για την απλοποίηση του όρου ‘purpose’ παρουσιάζεται το γραφικό εργαλείο DialogoP. Είναι ένα “UML – based meta-model” το οποίο παρέχει ενσωματωμένο ένα γραφικό τρόπο σχεδίασης, με τον οποίο οι χρήστες μπορούν να περιγράψουν την πολιτική ιδιωτικότητας που θέλουν να δηλώσουν (είτε με την χρήση ενός δεντρικού διαγράμματος, είτε με μία παλέτα) δημιουργώντας έτσι ένα ‘purpose diagram’.

Μετά την δημιουργία του ‘purpose diagram’, ακολουθεί η μετάφραση της πολιτικής ιδιωτικότητας. Μεταφράζεται σε “Formal Session Types” που χρησιμοποιούνται για την δήλωση του τρόπου επικοινωνίας μεταξύ των οντοτήτων του συστήματος.

Γενικότερα, απώτερος στόχος του άρθρου είναι να παρουσιάσει ένα τρόπο δήλωσης του «σκοπού» με γραφικό τρόπο.

2.2.3 “GDPR Compliance in the Design of INFORM e-Learning Platform: a Case Study”[3]

Το άρθρο αυτό παρουσιάζει διάφορες λειτουργίες υποστήριξης ιδιωτικότητας που ένα “web-based” σύστημα θα πρέπει να περιλαμβάνει από τα αρχικά στάδια της σχεδίασης, μέχρι και τα τελικά στάδια της υλοποίησης. Γενικά, το άρθρο επικεντρώνεται σε συγκεκριμένους κανόνες του GDPR και πώς αυτοί πρέπει να περιλαμβάνονται σε “web-based” περιβάλλοντα. Αυτοί οι κανόνες είναι οι εξής: “Data Minimization”, “Lawfulness of Processing”, “Right to Erasure”, “Right of Access”, “Right to Data Portability”, “Right to Rectification”, “Security of Processing”. Ο κύριος στόχος του άρθρου είναι να δείξει τους διάφορους τρόπους με τους οποίους αυτοί οι κανόνες πρέπει να συμπεριλαμβάνονται στα διάφορα συστήματα, για να επιτευχθεί πλήρης συμβατότητα με το GDPR.

Δημιουργήθηκε μία “e-Learning” πλατφόρμα η “INFORM” με την οποία οι κανόνες του GDPR που αναφέρθηκαν πιο πάνω τίθενται σε πράξη από τα αρχικά στάδια της σχεδίασης ενός λογισμικού. Οι συγγραφείς σημείωσαν ότι τις περισσότερες φορές σχεδιαστές

λογισμικού ή και μηχανικοί λογισμικού δεν λαμβάνουν υπόψη τους όρους που πρέπει να ακολουθούνται. Για τον λόγο αυτό, η ανάγκη για ένα πιο εύκολο και σαφές τρόπο παρουσίασης των κανόνων του GDPR είναι επιτακτική.

Συμπερασματικά, η συμβατότητα με το GDPR ενός συστήματος με τις πολιτικές του, πρέπει να γίνεται από τα αρχικά στάδια της σχεδίασης ενός λογισμικού. Η συλλογή, επεξεργασία και αποθήκευση προσωπικών δεδομένων χρηστών, πρέπει να γίνεται μετά την συγκατάθεσή τους και δεδομένα που δεν είναι χρήσιμα για την υλοποίηση του συστήματος δεν πρέπει να ζητούνται από τους χρήστες. Τέλος, οι χρήστες πρέπει να μπορούν να δουν, να επεξεργαστούν αλλά και να διαγράψουν τα δεδομένα τους από το σύστημα, όποτε αυτοί το θελήσουν.

2.2.4 “Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering”[4]

Οι συγγραφείς στο άρθρο αυτό, υποστηρίζουν ότι, παρόλο που η ιδιωτικότητα και η προστασία δεδομένων είναι αλληλένδετες, υπάρχει ακόμη ένα κενό που διαχωρίζει την εφαρμογή τους σε απλά συστήματα λογισμικού. Στο άρθρο υποστηρίζεται η ανάγκη για εργαλεία και μεθόδους που να συνδυάζουν αυτούς τους δύο όρους. Για τον λόγο αυτό, παρουσιάζεται ο όρος του “Privacy Engineering”.

Το “Privacy Engineering” θα τεθεί σε πράξη σε ένα μελλοντικό έργο που θα ονομάζεται “PDP4E”, όπου η ιδιωτικότητα θα συμπεριλαμβάνεται στα συστήματα λογισμικού από τα αρχικά στάδια της σχεδίασης τους. Τα στάδια στα οποία θα περιληφθεί η έννοια της ιδιωτικότητας είναι τα εξής: “risk management”, “requirements engineering”, “model-driven design” και “software/systems assurance”. Η γενική ιδέα που παρουσιάζουν οι συγγραφείς είναι ότι από την στιγμή που υπάρχουν είδη πρακτικές εφαρμογής άλλων απαιτήσεων σε συστήματα όπως η απαίτηση για «Ασφάλεια», κάτι παρόμοιο θα μπορούσε να υλοποιηθεί και για την απαίτηση της ιδιωτικότητας. Επομένως θα μπορούσαν όλοι οι μηχανικοί λογισμικού να υιοθετήσουν την έννοια του “Privacy Engineering”.

Όλα τα πιο πάνω θα τεθούν σε πράξη στο “PDP4E” το οποίο έχει σκοπό μακροπρόθεσμα να θέσει ένα «οικοσύστημα έρευνας και πρακτικής» για την ενδυνάμωση της έννοιας της προστασίας δεδομένων στα συστήματα λογισμικού.

2.2.5 “Towards Defining Semantic Foundations for Purpose-Based Privacy Policies”[5]

Στο άρθρο αυτό, οι συγγραφείς προτείνουν ένα μοντέλο, με το οποίο “purpose-based” πολιτικές ιδιωτικότητας θα μπορούν να εκφραστούν επίσης. Παρουσιάζουν ένα αλγόριθμο μοντελοελέγχου και την “Modal ” λογική του, μέσω των οποίων θα μπορεί να ελέγχεται “τυπικά” η συμβατότητα ενός συστήματος με την πολιτική του. Παρουσιάζουν επίσης διάφορα παραδείγματα πολιτικών ιδιωτικότητας – σκοπού, που μπορούν να δηλωθούν μέσω του μοντέλου που προτείνουν.

Με το άρθρο προτείνεται ένας αλγόριθμος μοντελοελέγχου που με τροπικό λογισμό θα μπορεί να εξασφαλίσει την επίσημη δήλωση πολιτικών ιδιωτικότητας.

Πολύ σημαντικοί συλλογισμοί στο άρθρο παρουσιάζονται με παραδείγματα όπου μπορεί ο «σκοπός» μίας ενέργειας να θεωρηθεί το αποτέλεσμά της. Οι συγγραφείς δηλαδή παρατήρησαν ότι μπορούμε να δούμε τί ενέργειες προέκυψαν για να έχουμε ως αποτέλεσμα την εκπλήρωση του «σκοπού».

Δηλαδή, εισάγουν την έννοια του «πλάνου» όπου πλάνο θεωρείται μία ακολουθία από ενέργειες που αποσκοπούν κάπου – «σκοπό». Οι ενέργειες αυτές είναι φυσικά αλληλένδετες αφού ακολουθούν η μία την άλλη και επομένως μπορούμε να δούμε την σχέση μεταξύ τους. Εισάγουν στην συνέχεια ένα “Action Graph” ως ένα αυθαίρετο μοντέλο για να μπορέσουν να καταγραφούν τα πλάνα μεταξύ των ενεργειών που συνδέονται μόνο με δύο σχέσεις τις οποίες εισάγουν μετά από μελέτη διαφόρων ειδών «σκοπού».

Οι συγγραφείς επομένως δημιούργησαν τυπικά εργαλεία για την δήλωση και τον έλεγχο συμβατότητας πολιτικών ιδιωτικότητας-σκοπού. Το χρησιμοποιούν αυτό για να επισημοποιήσουν τις σχέσεις μεταξύ ενεργειών και να τις αναπαραστήσουν μέσω ενός γράφου. Έπειτα δημιούργησαν μία τυπική γλώσσα για τον σκοπό αυτό και αναφέρουν ότι ο αλγόριθμος μοντελοελέγχου που προτείνουν, χρησιμοποιείται για τον έλεγχο συμβατότητας των ενεργειών του συστήματος με τις πολιτικές ιδιωτικότητας του.

2.3 Υπάρχοντα εργαλεία

Όνομα Εργαλείου	Τρόπος αξιολόγησης Εργαλείου / Περιγραφή	Χαρακτηριστικά που προσφέρει το εργαλείο “privacyDef” και σύγκριση με άλλα εργαλεία			
		Γραφική Δήλωση Πολιτικής	Μετατροπή πολιτικής σε Τυπική Γλώσσα	Αποθήκευση δήλωσης σε μορφή εικόνας και JSON αρχείου	Παρουσίαση υπάρχουσας δήλωσης μέσω ανέβασμα αρχείου
Terms Feed Policy Generator	Δημιουργήθηκε ένα παράδειγμα χρήσης αυτού του εργαλείου για ένα υποθετικό οργανισμό.	Δεν υπάρχει	Δεν υπάρχει	Δεν υπάρχει	Δεν υπάρχει
IUBENDA – Privacy & Cookie Policies Generator	Δημιουργήθηκε λογαριασμός. Είναι ένα γραπτό συμβόλαιο.	Δεν υπάρχει	Δεν υπάρχει	Δεν υπάρχει	Δεν υπάρχει
CONSENT MANAGER- Making Websites GDPR Compliant	Συμβατότητα ιστοσελίδων με GDPR ή CCPA.	Υπάρχει κάτι παρόμοιο αφού παρέχει την δυνατότητα “Design/Customi- zation”	Δεν υπάρχει	Δημιουργεί reports	Δεν υπάρχει
SHEQAPP – Compliance software monitoring the EU regulations	Περιέχει διάφορα έγγραφα με τα οποία μπορεί να γίνει το compliance checking.	Δεν υπάρχει	Δεν υπάρχει	Δεν υπάρχει	Δεν υπάρχει

GDPRWise –Online webpage scanner	Δυνατότητα σάρωσης ιστοσελίδας αλλά δεν περιέχει δήλωση πολιτικών	Δεν υπάρχει	Δεν υπάρχει	Δεν υπάρχει	Δεν υπάρχει
--	--	-------------	-------------	-------------	-------------

2.4 Σύνοψη Μελέτης και Συμπεράσματα

Σύμφωνα με την μελέτη που παρουσιάστηκε στην ενότητα 2.2, είναι πλέον κοινώς παραδεκτό ότι το πιο δύσκολο κομμάτι στην διαδικασία υλοποίησης λογισμικού, είναι το κομμάτι του ελέγχου. Ειδικότερα, ο έλεγχος συστημάτων που χρησιμοποιούν δεδομένα χρηστών, γιατί επιβάλλεται να είναι αυστηρότερος. Ο έλεγχος του κατά πόσο ένα σύστημα είναι συμβατό με το GDPR και τις πολιτικές ιδιωτικότητας του είναι ένα θέμα που χρειάζεται ειδική μεταχείριση. Οι τυπικές μέθοδοι, «καταργούν» την αβεβαιότητα και την ανάγκη για επαναληπτικούς ελέγχους, αφού χρησιμοποιούν τυπικές γλώσσες. Για τον λόγο αυτό, εργαλεία όπως το “privacyDef”, είναι αναγκαία αφού δεν γνωρίζει ο κάθε μηχανικός λογισμικού την ύπαρξη των τυπικών μεθόδων, ή εάν την γνωρίζει, υπάρχει μεγάλη πιθανότητα να μην ξέρει πώς να τις χρησιμοποιεί. Επομένως, η ανάγκη για ένα εργαλείο όπως το “privacyDef” επιβεβαιώνεται για ακόμη μία φορά, αφού το εργαλείο αυτό δεν απαιτεί καμία γνώση από τους χρήστες του για τυπικές γλώσσες και μεθόδους.

Παρατηρώντας τον πιο πάνω πίνακα της ενότητας 2.3, διεξάγεται το συμπέρασμα ότι δεν υπάρχει κάποιο εργαλείο παρόμοιο με το “privacyDef” και αυτό καθιστά την υλοποίησή του ακόμη πιο σημαντική και αναγκαία. Πιο συγκεκριμένα, στον πίνακα της ενότητας 2.3 παρουσιάζονται διάφορα εργαλεία που σχετίζονται με την δημιουργία πολιτικών ιδιωτικότητας, ελέγχους συμβατότητας κλπ. Παρατηρείται ότι κανένα από αυτά τα εργαλεία δεν εκφράζει την δήλωση πολιτικών με τρόπο πέραν της φυσικής γλώσσας, για την αποτελεσματικότητα του οποίου η διπλωματική εργασία αυτή διαφωνεί.

Κεφάλαιο 3

Τεχνολογίες

3.1 Εισαγωγή	18
3.2 Front End Development	18
3.2.1 JavaScript	18
3.2.2 HTML5	19
3.2.3 CSS3	19
3.2.4 WordPress	19
3.3 Back End Development	19
3.3.1 PHP	19

3.1 Εισαγωγή

Κατά την διάρκεια της υλοποίησης του εργαλείου privacyDef χρησιμοποιήθηκαν αρκετές τεχνολογίες. Επίσης χρησιμοποιήθηκαν εργαλεία, πλατφόρμες και ειδικοί “editors” κατά την διάρκεια της διεκπεραίωσης της Διπλωματικής εργασίας.

3.2 Front End Development

Το Front End development [6] επικεντρώνεται κυρίως με το τί θα έρθει σε επαφή ο πελάτης σε ότι έχει σχέση με την εφαρμογή (“client-side”).

Στην διαδικασία αυτή, οι developers ασχολούνται με την υλοποίηση κώδικα, τον σχεδιασμό και τον εντοπισμό σφαλμάτων εφαρμογών μαζί με την εξασφάλιση μίας απρόσκοπτης εμπειρίας για τον χρήστη. Διαχειρίζονται αυτά που μπορούν να δουν οι χρήστες.

3.2.1 JavaScript

Η JavaScript είναι μία προγραμματιστική γλώσσα για προγράμματα περιήγησης στο Web, και είναι απαραίτητη για τις σύγχρονες εφαρμογές ιστού. Οι προγραμματιστές την χρησιμοποιούν για την σύνταξη σύνθετων εφαρμογών [7]. Παρέχει στις ιστοσελίδες μία διαδραστικότητα. Η ενσωμάτωσή της, βελτιώνει την εμπειρία του χρήστη της ιστοσελίδας.

3.2.2 HTML5

Η HTML5 είναι η 5^η έκδοση της HTML η οποία είναι μία γλώσσα σήμανσης για ιστοσελίδες [8]. Χρησιμοποιείται, στην δημιουργία της δομής της ιστοσελίδας του εργαλείου privacyDef.

3.2.3 CSS3

Η CSS3 είναι το τρίτο επίπεδο της CSS (Cascading Style Sheets) και χρησιμοποιείται για την μορφοποίηση μίας ιστοσελίδας, ή και των διαφόρων στοιχείων της όπως η τοποθεσία τους, τα χρώματα κλπ [9]. Στην δημιουργία του privacyDef έχει χρησιμοποιηθεί για την μορφοποίηση συγκεκριμένων στοιχείων της ιστοσελίδας, όπως ο καμβάς και η παλέτα του εργαλείου, τα οποία παρουσιάζονται πιο αναλυτικά στις πιο κάτω ενότητες.

3.2.4 WordPress

Το WordPress είναι ένα CMS εργαλείο. Δηλαδή, ένα σύστημα διαχείρισης περιεχομένου, μέσω του οποίου μπορεί να γίνει τροποποίηση του περιεχομένου ενός ιστότοπου. [10]

3.3 Back End Development

Το back end development είναι το λεγόμενο “server-side development”. Εστιάζει στις βάσεις δεδομένων, και γενικότερα στην αρχιτεκτονική ενός συστήματος. [11]

3.3.1 PHP

Είναι μία ευρέως χρήσιμη γλώσσα που επικεντρώνεται στον προγραμματισμό στην πλευρά του server. [12]

Κεφάλαιο 4

Κύκλος Ζωής και Ανάπτυξης Λογισμικού

4.1 Εισαγωγή / Μεθοδολογίες - περιγραφή	21
4.2 Έρευνα για Καταγραφή Απαιτήσεων και Προδιαγραφών	22
4.2.1 Μέθοδος έρευνας	22
4.2.2 Ερωτηματολόγιο	23
4.2.3 Αποτελέσματα	24
4.3 Προδιαγραφές	27
4.4 Μοντέλο της Πρωτοτυποποίησης	28
4.4.1 Εισαγωγή – “Throw-away prototyping”	28
4.4.2 Τεχνολογίες που Χρησιμοποιήθηκαν	28
4.4.3 Πρωτότυπο 1 – Πρώτη έκδοση	29
4.4.3.1 Σχεδίαση και Οθόνες	29
4.4.3.2 Έρευνα Αξιολόγησης Πρώτης έκδοσης	31
4.4.4 Πρωτότυπο 2 – Δεύτερη έκδοση	32
4.4.4.1 Σχεδίαση και Οθόνες	33
4.4.4.2 Έρευνα Αξιολόγησης Δεύτερης έκδοσης	33
4.4.5 Πρωτότυπο 3 – Τρίτη έκδοση	34
4.4.5.1 Σχεδίαση και Οθόνες	34
4.4.5.2 Έρευνα Αξιολόγησης Τρίτης έκδοσης	38
4.5 Σχεδιασμός Εργαλείου	39
4.5.1 Αρχιτεκτονική	39
4.5.2 Διαδικασία Σχεδίασης	39
4.5.2.1 “The design Process”	40
4.5.2.2 “Network Diagram”	41
4.6 Υλοποίηση Εργαλείου	42
4.6.1 Επεξήγηση Δομής Γραφικής Δήλωσης	42
4.6.2 Επεξήγηση Δομής Μετατροπής σε Τυπική Γλώσσα	44
4.6.2.1 Η τυπική γλώσσα που χρησιμοποιείται	44
4.6.2.2 Διαδικασία Μετατροπής	45

4.1 Εισαγωγή/Μεθοδολογίες - Περιγραφή

Είναι γνωστό ότι τα έργα ανάπτυξης λογισμικού είναι πολύπλοκα. Επομένως μία προσέγγιση με φάσεις ανάπτυξης είναι απαραίτητη για τον έλεγχο των έργων. Η διαδικασία αυτή ονομάζεται «διαδικασία ανάπτυξης λογισμικού» και είναι κατά ορισμό, ένα δομημένο σύνολο δραστηριοτήτων για την ανάπτυξη ενός συστήματος λογισμικού[9].

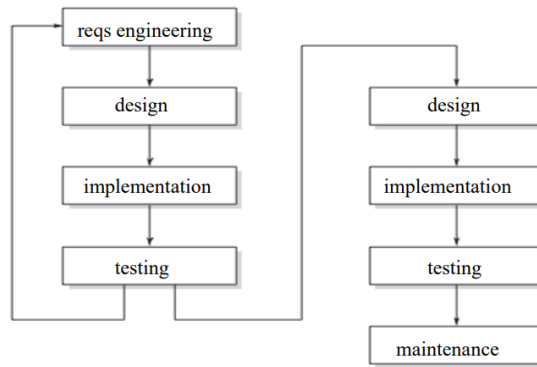
Η διαδικασία/μοντέλο που χρησιμοποιήθηκε για την ανάπτυξη του εργαλείου “privacyDef” στα πλαίσια της διπλωματική εργασίας αυτής, χρησιμοποιεί ένα συνδυασμό μοντέλων: των Agile Μεθοδολογιών και του Μοντέλου Πρωτοτυποποίησης (“Rapid Prototyping Model”).

Τα χαρακτηριστικά που οδήγησαν στην επιλογή της Agile Μεθοδολογίας είναι αρχικά το γεγονός ότι, δίνει προτεραιότητα στα άτομα έναντι των διεργασιών και των εργαλείων. Βασίζεται επίσης στην ορθότητα και στην λειτουργικότητα του λογισμικού. Λόγω του ότι οι Agile Μεθοδολογίες έχουν ήδη χαρακτηριστικά από πρωτοτυποποίηση, ήταν εύκολος ο συνδυασμός των δύο.



Εικόνα: 4.1 [13]

Το Μοντέλο Πρωτοτυποποίησης επικεντρώνεται στο ότι το πρωτότυπο δεν είναι το προϊόν και στο ότι η πρωτοτυποποίηση δεν πρέπει να έχει μεγάλο κόστος (χρησιμοποιούνται εργαλεία πρωτοτυποποίησης, δεν υλοποιείται όλη η λειτουργικότητα και δεν χρειάζεται ποιότητα προϊόντος). Υπάρχουν δύο επιλογές χρήσης του πρωτότυπου. Στα πλαίσια της διπλωματικής έχει επιλεγθεί το “Throwaway prototyping” το οποίο παρουσιάζεται στην ενότητα 4.4.1. Με το μοντέλο αυτό, το τελικό σύστημα είναι πιο εύκολο στη χρήση, έχει καλύτερη ενσωμάτωση των αναγκών των χρηστών, τα προβλήματα εντοπίζονται νωρίτερα και τέλος, η υλοποίηση μετέπειτα γίνεται λιγότερο απαιτητική [14].



Εικόνα: 4.2[14]

4.2 Έρευνα για Καταγραφή Απαιτήσεων και Προδιαγραφών

4.2.1 Μέθοδος Έρευνας:

Η μέθοδος της έρευνας που πραγματοποιήθηκε ήταν με την χρήση ενός ερωτηματολογίου όπου με σύντομες ερωτήσεις (κυρίως ερωτήσεις πολλαπλής επιλογής), ο χρήστης απαντούσε βάσει των γνώσεων του σχετικά την έννοια της ιδιωτικότητας, τις εμπειρίες που είχε μέχρι στιγμής με διάφορα εργαλεία μοντελοποίησης και άλλα τα οποία θα αναλυθούν στην συνέχεια.

Η έρευνα διαχωρίζεται σε τρία μέρη όμως αρχικά στην πρώτη σελίδα παρέχονται διάφορες πληροφορίες που εάν οι συμμετέχοντες δεν γνωρίζουν θα μπορούν να τις διαβάσουν. Οι πληροφορίες αυτές αφορούν τις έννοιες του “Privacy-Compliant software” και “Validation in Software Engineering”. Στην επεξήγηση των δυο αυτών εννοιών παρέχονται και παραδείγματα για να είναι πιο κατανοητές.

Το πρώτο μέρος των ερωτήσεων αφορά τα βιογραφικά στοιχεία των χρηστών, όπως ηλικία, φύλο επάγγελμα, χώρα κλπ. Το δεύτερο μέρος των ερωτήσεων αφορά τις γνώσεις τους σχετικά με την έννοια της ιδιωτικότητας και ποια η σχέση τους με αυτή αναφορικά με τα δικά τους συστήματα, αφού η έρευνα αφορά μόνο μηχανικούς λογισμικού. Το τρίτο και τελευταίο μέρος της έρευνας αφορά την σχέση και την γνώση των χρηστών με τις τυπικές μεθόδους. Κατά πόσο τις χρησιμοποιούν, με ποιο τρόπο κλπ. Στο τέλος αυτού του μέρους, υπάρχουν ερωτήσεις που προβληματίζουν τους συμμετέχοντες της έρευνας κατά πόσο, με όλα αυτά που μάλλον έχουν διαβάσει και καταλάβει από την πρώτη σελίδα, θα χρησιμοποιούσαν τυπικές μεθόδους για τον έλεγχο συμβατότητας των δικών τους

συστημάτων και κατ' επέκταση, κατά πόσο θα χρησιμοποιούσαν ένα εργαλείο που θα το υλοποιούσε αυτό παρέχοντάς τους έτσι μεγαλύτερη ευκολία.

Ολόκληρη η έρευνα καθώς και τα αποτελέσματά της, είναι διαθέσιμα και στο Παράρτημα Α.

4.2.2 Ερωτηματολόγιο

Αρχικά παρουσιάζεται και επεξηγείται ο λόγος που γίνεται αυτή η έρευνα στους συμμετέχοντες. Επεξηγείται επίσης το θέμα και οι έννοιες του “Privacy-Compliant software” και “Validation in Software Engineering”. Αυτές οι έννοιες μπορούν να χαρακτηριστούν και ως η υφιστάμενη γνώση που πρέπει να έχει κάποιος για να μπορέσει να απαντήσει ορθά και αντικειμενικά στο ερωτηματολόγιο. Στην συνέχεια εμφανίζεται η φόρμα συγκατάθεσης όπου τονίζεται ότι τα δεδομένα και οι απαντήσεις των συμμετεχόντων θα χρησιμοποιηθούν μόνο για τον σκοπό της διπλωματικής εργασίας. Μπορούν οποιαδήποτε στιγμή να σταματήσουν να απαντούν στην έρευνα χωρίς να πατήσουν ‘Υποβολή’. Τέλος απαντώντας ‘Yes’ στην φόρμα συγκατάθεσης θα μεταβούν στις πρώτες ερωτήσεις.

Οι πρώτες ερωτήσεις όπως έχει αναφερθεί και πιο πάνω, αφορούν τα βιογραφικά στοιχεία των συμμετεχόντων, την ηλικία τους, το φύλο, την πόλη και εάν είναι μηχανικοί λογισμικού. Εάν είναι, πρέπει να απαντήσουν στην ερώτηση που αναφέρεται στα χρόνια εμπειρίας τους ως μηχανικοί λογισμικού (εδώ υπάρχει και επιλογή για φοιτητές πληροφορικής). Στο τέλος της ενότητας αυτής οι συμμετέχοντες δηλώνουν πόσο ικανοποιητική ήταν η εμπειρία τους με εργαλεία μοντελοποίησης και γενικά με UML.

Στην επόμενη ενότητα υπάρχουν ερωτήσεις που αφορούν γενικά για την έννοια της ιδιωτικότητας. Οι συμμετέχοντες πρέπει να απαντήσουν κατά πόσο γνωρίζουν όλα τα στάδια σχεδίασης ενός λογισμικού, εάν θεωρούν την ιδιωτικότητα σημαντική και κατά πόσο γνωρίζουν για αυτή γενικά. Πιο ειδικά έπειτα, καλούνται να απαντήσουν σχετικά με τις γνώσεις τους για τις πολιτικές ιδιωτικότητας και εάν είναι εξοικειωμένοι με το GDPR. Στην συνέχεια ακολουθούν δύο ερωτήσεις που αφορούν το χρόνο που αφιερώνουν για την εφαρμογή της έννοιας της ιδιωτικότητας στα συστήματά τους και για τον χρόνο που αφιερώνουν στην δήλωση πολιτικών ιδιωτικότητας των συστημάτων τους. Σε επόμενη ερώτηση πρέπει να δηλώσουν πόσο συχνά τους έτυχαν τα πιο κάτω:

- «υλοποίηση συστήματος χωρίς να ληφθεί υπόψη η έννοια της ιδιωτικότητας»

- «χρειάστηκαν να γίνουν μικρές αλλαγές στην σχεδίαση του συστήματος μετά που λήφθηκε υπόψη η έννοια της ιδιωτικότητας»
- «χρειάστηκαν να γίνουν μεγάλες αλλαγές στην σχεδίαση του συστήματος μετά που λήφθηκε υπόψη η έννοια της ιδιωτικότητας»
- «χρειάστηκαν να γίνουν μικρές αλλαγές στην υλοποίηση του συστήματος μετά που λήφθηκε υπόψη η έννοια της ιδιωτικότητας»
- «χρειάστηκαν να γίνουν μεγάλες αλλαγές στην υλοποίηση του συστήματος μετά που λήφθηκε υπόψη η έννοια της ιδιωτικότητας»

Τέλος, στην ενότητα αυτή υπάρχουν ερωτήσεις σχετικά με την σημαντικότητα της δήλωσης πολιτικών ιδιωτικότητας στα αρχικά στάδια της σχεδίασης ενός συστήματος και εάν γνωρίζουν οι συμμετέχοντες αρκετά για τα δικαιώματα των χρηστών σχετικά με την ιδιωτικότητα στα συστήματα λογισμικού.

Στην τρίτη και τελευταία ενότητα, υπάρχουν ερωτήσεις που αφορούν τις γνώσεις των χρηστών για τις τυπικές μεθόδους. Αρχικά πρέπει να απαντήσουν κατά πόσο είναι εξοικειωμένοι με τις τυπικές μεθόδους και πόσο συχνά τις χρησιμοποιούν στην μοντελοποίηση των συστημάτων τους. Έπειτα πρέπει να απαντήσουν κατά πόσο και εάν τις χρησιμοποιούν για τον έλεγχο των συστημάτων τους, και εάν όχι κατά πόσο θα τις χρησιμοποιούσαν, λαμβάνοντας υπόψη ότι με αυτές μπορεί να εγγυηθεί η ιδιωτικότητα. Τέλος, οι συμμετέχοντες καλούνται να απαντήσουν κατά πόσο θα χρησιμοποιούσαν ένα γραφικό εργαλείο στην φάση της σχεδίασης του συστήματός τους, με το οποίο θα μπορούσαν να δηλώσουν τις πολιτικές ιδιωτικότητας που θέλουν, το οποίο αυτόματα θα μετέτρεπε την δήλωση αυτή σε μία τυπική μέθοδο.

Το ερωτηματολόγιο βρίσκεται στον ακόλουθο σύνδεσμο:

<https://forms.gle/HqAhYXQzuewhicjF7>

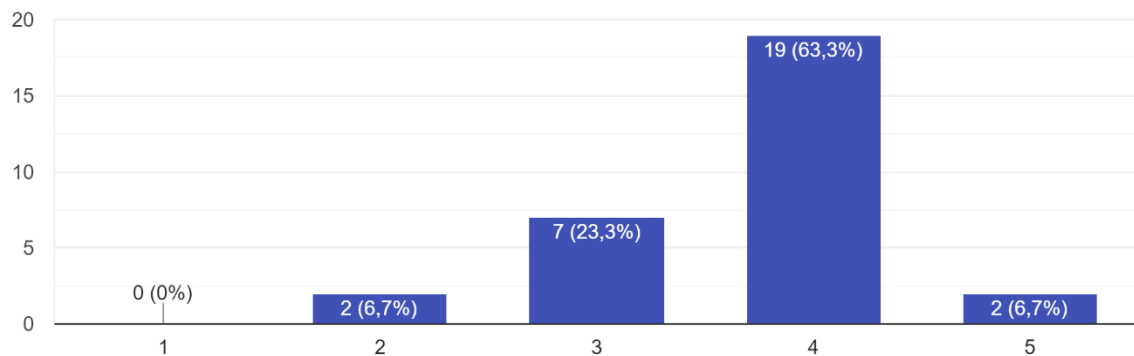
4.2.3 Αποτελέσματα

Στο ερωτηματολόγιο για το ‘Graphical Tool Development for Defining Privacy Policies’ συμμετείχαν συνολικά 30 άτομα. Πιο συγκεκριμένα απάντησαν 12 φοιτητές, 9 άτομα με 0 έως και 2 χρόνια εμπειρίας ως μηχανικοί λογισμικού, 4 άτομα με 2 έως και 5 χρόνια εμπειρίας και ένα άτομο με 5 έως και 10 χρόνια εμπειρίας. Τα 17 από τα 30 άτομα έχουν μέτρια εμπειρία με εργαλεία μοντελοποίησης και 18 από τα 30 έχουν μέτρια εμπειρία με

UML γενικότερα. 26 από τα 30 άτομα γνωρίζουν όλα τα στάδια σχεδίασης ενός λογισμικού.

10. Are you familiar with Privacy in general

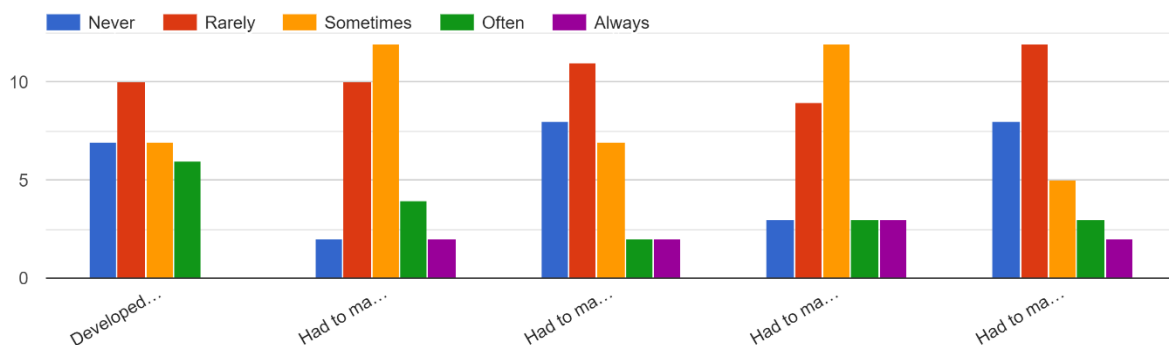
30 απαντήσεις



Εικόνα 4.1

Παρατηρείται ότι οι περισσότεροι είναι σε κάποιο βαθμό εξοικειωμένοι με την έννοια της ιδιωτικότητας ενώ λιγότεροι είναι εξοικειωμένοι με την έννοια των «πολιτικών ιδιωτικότητας» όπως φαίνεται στο Παράρτημα Α' στην ερώτηση 11 του ερωτηματολογίου. Περισσότερη θετική ανταπόκριση υπάρχει σχετικά με την γνώση των συμμετεχόντων για το GDPR γεγονός πολύ θετικό.

15. How often do the following happen to you? (Software Development - wise)



Εικόνα 4.2

Όπως έχει περιγράψει στην ενότητα 4.4.2, η ερώτηση αυτή είχε πέντε υπο-ερωτήματα. Ιδανικές απαντήσεις και για τα 5 αυτά υπο-ερωτήματα, είναι το 'Never' αφού και τα πέντε περιγράφουν δυσάρεστες συνθήκες που μάλλον βρέθηκαν αντιμέτωποι οι μηχανικοί λογισμικού, ως αποτέλεσμα της μη απαιτούμενης σημασίας στην έννοια της ιδιωτικότητας.

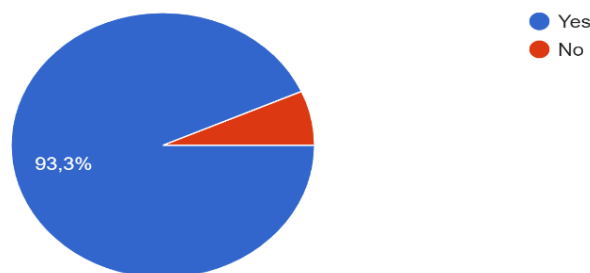
Επομένως, φαίνεται ότι το εργαλείο που προτείνεται μέσω της διπλωματικής αυτής θα επιλύσει τα πιο πάνω προβλήματα ή μάλλον θα μειώσει τα φαινόμενα αυτά. Πιο αναλυτικά τα υπο-ερωτήματα της ερώτησης 15 διαφαίνονται στο Παράρτημα Α'.

Μελετώντας τα αποτελέσματα από την ερώτηση 16, παρατηρείται ότι η πλειοψηφία πιστεύει ότι είναι σημαντική η δήλωση πολιτικών ιδιωτικότητας από τα αρχικά στάδια της σχεδίασης ενός λογισμικού, γεγονός θετικό αφού τονίζει την αναγκαιότητα του εργαλείου. Αρνητικό όμως, θεωρείται το γεγονός ότι το 50 % των συμμετεχόντων δήλωσε ότι γνωρίζει αρκετά αλλά όχι πολλά σχετικά με τα δικαιώματα των χρηστών.

Σχετικά με τις τυπικές μεθόδους τα αποτελέσματα πιο κάτω πηγάζουν από τις ερωτήσεις 18-21 που παρουσιάζονται στο Παράρτημα Α'. Αρχικά, το 26,7 % δήλωσε ότι δεν είναι εξοικειωμένοι με τις τυπικές μεθόδους ενώ το 33% δήλωσε ότι δεν τις έχει χρησιμοποιήσει ποτέ στην φάση της μοντελοποίησης των συστημάτων τους. Επίσης το 33% δεν τις έχει χρησιμοποιήσει ποτέ ούτε στις διαδικασίες ελέγχου του συστήματός του.

21. Having in mind that Formal Methods can help you guarantee privacy in your software system, would you use them, if there was an easy way for that?

30 απαντήσεις

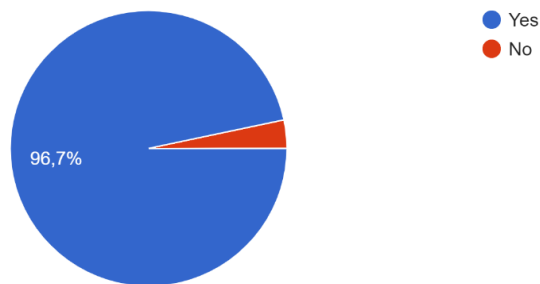


Εικόνα 4.3

Θετικό όμως είναι το γεγονός ότι η συντριπτική πλειοψηφία, γνωρίζοντας μετά την διεξαγωγή αυτής της έρευνας, τις δυνατότητες των τυπικών μεθόδων, απάντησαν ότι θα τις χρησιμοποιούσαν σε μελλοντικά συστήματά τους όπως φαίνεται και στην Εικόνα 4.3.

22. If there was a graphical tool where you could define a privacy policy in an easy-to-use diagram-based way (e.g. UML-like), that would th...ould you use it during the system design stage?

30 απαντήσεις



Εικόνα 4.4

Τέλος, επίσης πολύ θετικά αποτελέσματα εισπράττονται και από αυτή την ερώτηση αφού όλοι σχεδόν απάντησαν ότι θα χρησιμοποιούσαν το εργαλείο που υλοποιείται στα πλαίσια της διπλωματικής αυτής.

4.3 Προδιαγραφές

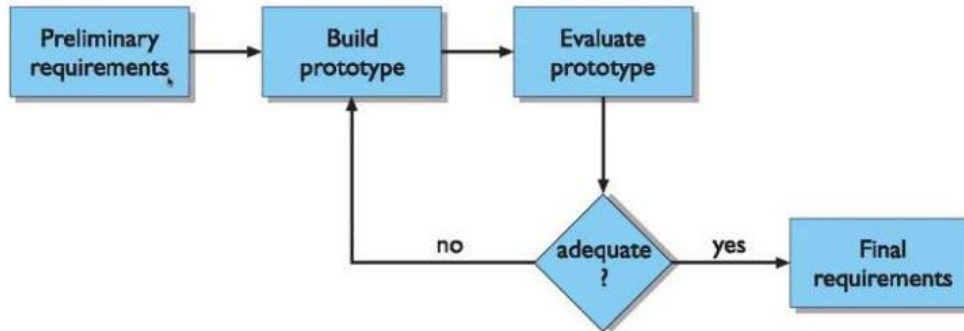
Εδώ παρουσιάζεται μία λίστα με τις διάφορες προδιαγραφές/απαιτήσεις του συστήματος:

<i>Login Page & Register Page</i>	Η αρχική σελίδα όπου ο χρήστης θα μπορεί μέσω του λογαριασμού του να εισέλθει στο σύστημα.
<i>Main Menu</i>	Το κυρίως μενού, η σελίδα δηλαδή στην οποία να φαίνονται όλες οι επιλογές που έχει ο χρήστης.
<i>Create Privacy Policy</i>	Η επιλογή για δημιουργία μίας δήλωσης πολιτικής ιδιωτικότητας.
<i>View policy</i>	Η επιλογή για προβολή της γραφικής δήλωσης, μέσω ενός JSON αρχείου.
<i>View Account</i>	Η επιλογή για προβολή του λογαριασμού του χρήστη
<i>Logout</i>	Επιλογή για έξοδο από το εργαλείο.

4.4 Μοντέλο της Πρωτοτυποποίησης

4.4.1 Εισαγωγή – “Throw-away Prototyping”

Αυτή η επιλογή χρήσης του πρωτοτύπου αποτελεί συνδυασμό της πρωτοτυποποίησης με το μοντέλο του καταρράκτη. Έχει εφαρμοστεί η τακτική που παρουσιάζεται γραφικά με το πιο κάτω σχήμα



Εικόνα:4.5 [15]

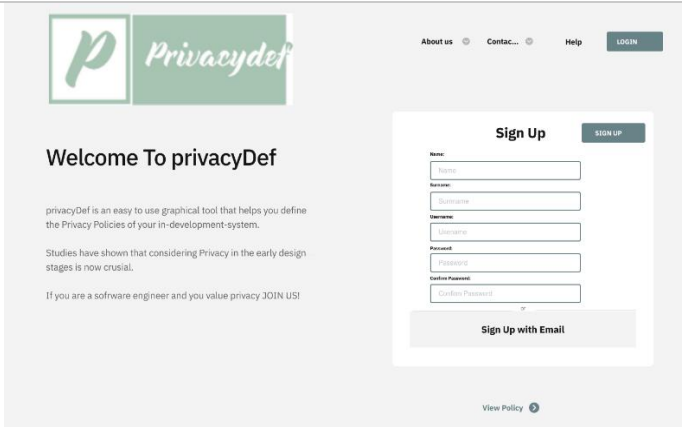
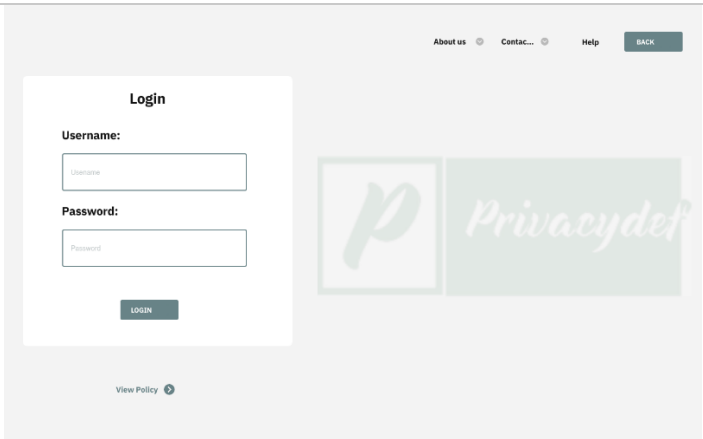
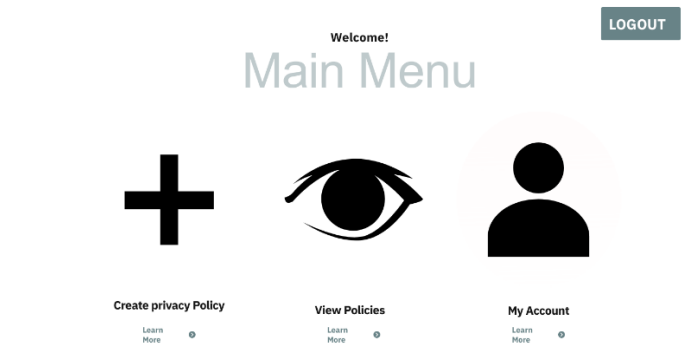
Έχουν δημιουργηθεί συνολικά τρία πρωτότυπα τα οποία έχουν αξιολογηθεί από μία ομάδα 8 ατόμων (ίδια ομάδα ατόμων αξιολογούσε και τις τρεις εκδόσεις). Μετά την τρίτη έκδοση, το πρωτότυπο θεωρήθηκε επαρκές και βοήθησε στην πλήρη κατανόηση των απαιτήσεων από τους χρήστες αλλά και στην απλούστευση της υλοποίησης στην μετέπειτα πορεία.

4.4.2 Τεχνολογίες που χρησιμοποιήθηκαν

Η τεχνολογία που έχει χρησιμοποιηθεί για την δημιουργία των πρωτοτύπων είναι το proto.io.

4.4.3 Πρωτότυπο 1 – Πρώτη Έκδοση

4.4.3.1 Σχεδίαση και Οθόνες:

Οθόνες	Επεξήγηση
	<u>Οθόνη 1 :</u> Εδώ ο χρήστης μπορεί να εγγραφεί δίνοντας τα στοιχεία του, ή μέσω email. Εάν έχει ήδη λογαριασμό μπορεί απλά με το κουμπί “login” να συνδεθεί. Στην οθόνη αυτή υπάρχουν και άλλες ενέργειες που μπορεί να κάνει ο χρήστης όπως να επικοινωνήσει με εμάς και ή να μάθει περισσότερα για το privacyDef.
	<u>Οθόνη 2:</u> Εδώ με την χρήση ενός username ο χρήστης που ήδη έχει λογαριασμό ή ο χρήστης που μόλις έχει δημιουργήσει λογαριασμό, μπορεί να συνδεθεί στο σύστημα.
	<u>Οθόνη 3:</u> Εδώ ο κάθε χρήστης μπορεί να δει το κυρίως μενού όπου μπορεί να επιλέξει την δημιουργία μίας πολιτικής, να δει τις πολιτικές που έχει ήδη δημιουργήσει και τον λογαριασμό του.

+ Create New Privacy Policy

Create a new repository and add later new policies, or create directly a new Privacy policy.

Create New
Privacy Policy

Create New
Repository

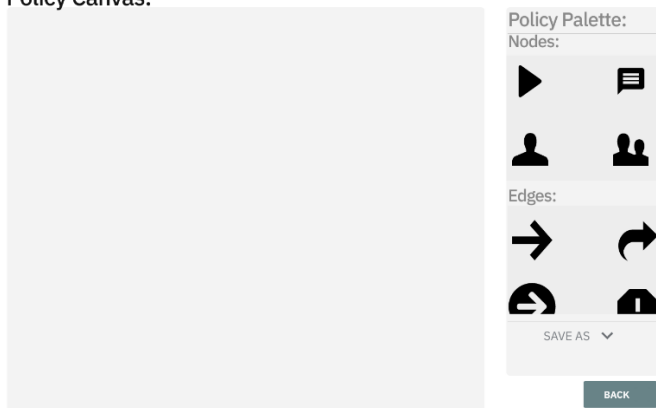
Back to Main
Menu

Οθόνη 4:

Η οθόνη αυτή παρουσιάζει το μενού που θα βρεθεί ο χρήστης εάν πατήσει το “Create privacy policy” στην οθόνη 3.

Εδώ μπορεί είτε να δημιουργήσει μία εντελώς καινούρια αυτόνομη πολιτική, είτε να δημιουργήσει ένα καινούριο φάκελο για να δημιουργήσει μετέπειτα πολιτικές για ένα συγκεκριμένο σύστημα.

Policy Canvas:

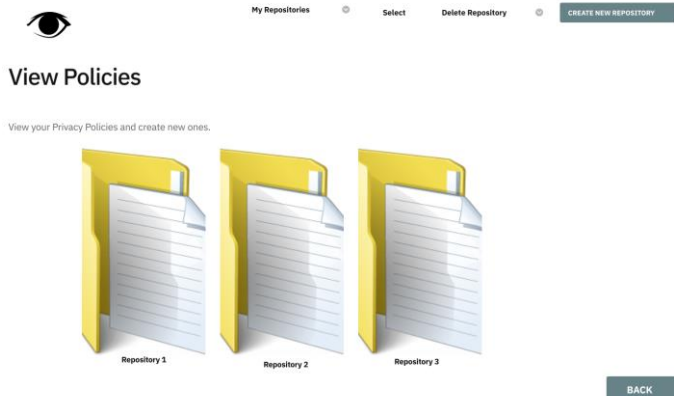


Οθόνη 5:

Η οθόνη αυτή παρουσιάζει την επιλογή “ Create new privacy policy” στην οθόνη 4.

Εδώ φαίνεται ο καμβάς και η παλέτα η οποία περιέχει δύο ενότητες. Τους κόμβους και τις ακμές, που είναι τα στοιχεία που βοηθούν στην γραφική δήλωση των πολιτικών ιδιωτικότητας.

Ο καμβάς μπορεί να αποθηκευτεί ως XML, PNG και άλλα.



Οθόνη 6:

Η οθόνη αυτή παρουσιάζει την επιλογή “ Create new repository” στην οθόνη 4.

Εδώ απλά ο χρήστης μπορεί να δημιουργήσει ένα καινούριο φάκελο. Μετέπειτα θα μπορεί να έχει πρόσβαση στον φάκελο αυτό όπου υπάρχουν φυλαγμένες πολιτικές ιδιωτικότητας.

My Account

My Information Review Contact Us

Due to GDPR, you can review the information we hold in our platform and you can change them anytime.
You can also delete your account anytime.
GIVE US A REVIEW BY TAPPING THE REVIEW BUTTON!

press to enable editing

Name Ioanna
Surname Theophilou
Username ltheop02
Password *****
Email ltheop02@ucy.ac.cy

Delete my Account

LOGOUT

BACK



Οθόνη 7:

Η οθόνη αυτή παρουσιάζει την επιλογή “My account” στην οθόνη 3.

Εδώ ο χρήστης μπορεί να δει τα στοιχεία που έχει δηλώσει στο σύστημα, να τα αλλάξει, να τα διαγράψει ή και να διαγράψει ολόκληρό του τον λογαριασμό.

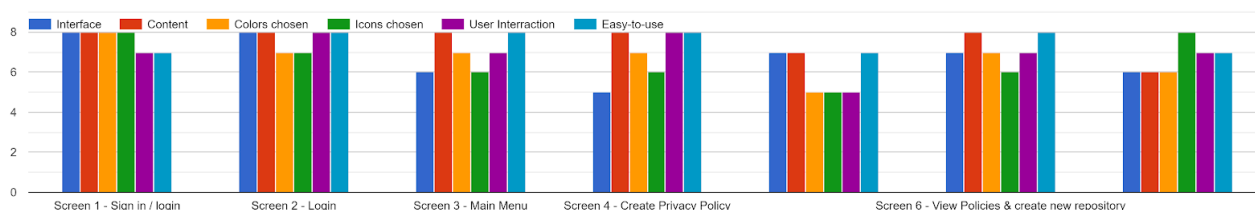
4.4.3.2 Έρευνα Αξιολόγησης πρώτης έκδοσης:

Η αξιολόγηση της πρώτης έκδοσης του πρωτότυπου, αλλά και των επόμενων εκδόσεών του, έγιναν με την μέθοδο του ερωτηματολογίου. Όπως έχει προαναφερθεί, η αξιολόγηση έγινε από 8 άτομα.

Στα 8 αυτά άτομα, έχει δοθεί ένα βίντεο που δείχνει το πρωτότυπο, και την αλληλεπίδραση του χρήστη με τις διάφορες οθόνες. Μετά την προβολή του βίντεο έπρεπε να απαντήσουν κατά πόσο οι πιο κάτω μετρικές θεωρούνται επαρκής σε κάθε οθόνη.

Μετρικές:	Διεπαφή	Περιεχόμενο	Χρώματα	Εικονίδια	Αλληλεπίδραση με χρήστη	Εύκολο στη χρήση	Σύνολο:
Οθόνη 1:	100 %	100 %	100 %	100 %	87.5 %	87.5 %	95,8 %
Οθόνη 2:	100 %	100 %	87.5 %	87.5 %	100 %	100 %	95,8 %
Οθόνη 3:	75 %	100 %	87.5 %	75 %	87.5 %	100 %	87.5 %
Οθόνη 4:	62.5 %	100 %	87.5 %	75 %	100 %	100 %	87.5 %
Οθόνη 5:	87.5 %	87.5 %	62.5 %	62.5 %	62.5 %	87.5 %	75 %
Οθόνη 6:	87.5 %	100 %	87.5 %	75 %	87.5 %	100 %	89.6 %
Οθόνη 7:	75 %	75 %	87.5 %	100 %	87.5 %	87.5 %	85.4 %

Please select for each screen the options you think are correctly presented / fulfilling:



Σύμφωνα με τα αποτελέσματα της έρευνας αξιολόγησης καμιοία οθόνη δεν έχει εξασφαλίσει το 100 % επομένως όλες χρειάζονται βελτίωση. Μετά την αξιολόγηση της κάθε οθόνης οι συμμετέχοντες στην έρευνα μπορούσαν να γράψουν σχόλια διόρθωσης για οποιαδήποτε οθόνη. Τα σχόλια αυτά θα αναφερθούν στην επόμενη έκδοση όπου διορθώνονται μερικά λάθη.

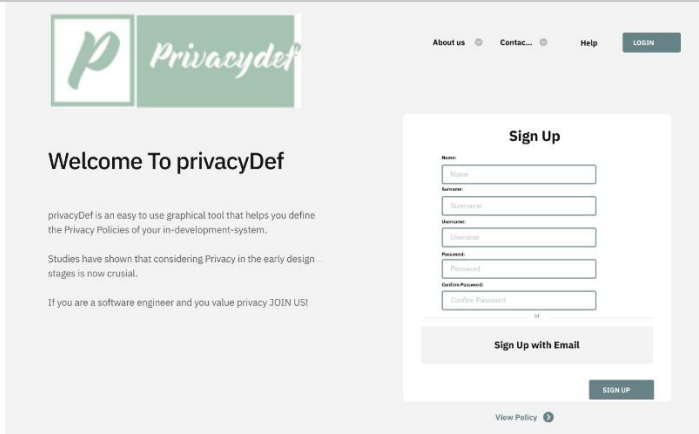
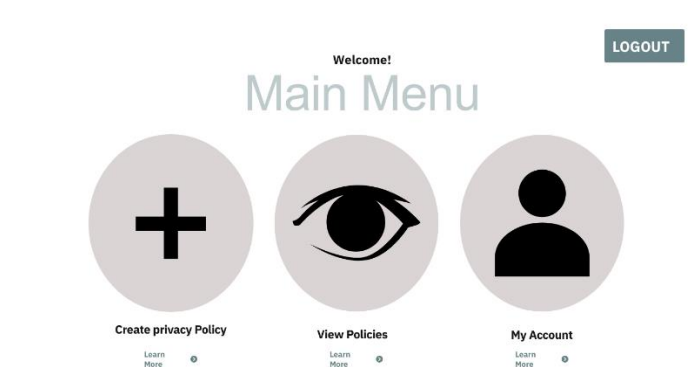
Το ερωτηματολόγιο βρίσκεται στον ακόλουθο σύνδεσμο:

<https://forms.gle/YUsJ9QzAPaWPL7uH9>

4.4.4 Πρωτότυπο 2 – Δεύτερη έκδοση:

4.4.4.1 Σχεδίαση και Οθόνες:

Ο σκοπός της δεύτερης έκδοσης ήταν να υλοποιηθούν οι αλλαγές που χρειάζονται από την πρώτη σύμφωνα με την έρευνα αξιολόγησης και τα σχόλια των συμμετεχόντων. Στον πιο κάτω πίνακα θα παρουσιαστούν μόνο οι οθόνες που διαφέρουν από το πρώτο πρωτότυπο στο δεύτερο.

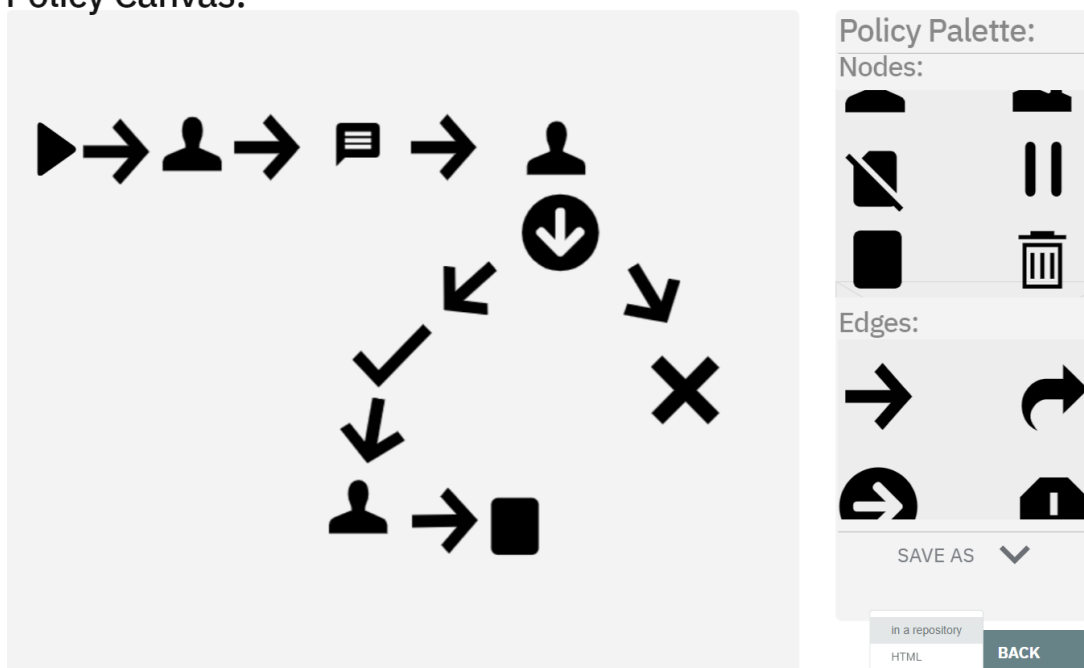
Οθόνες	Αλλαγές
	<u>Οθόνη 1 :</u> Ένα από τα σχόλια ήταν ότι το κουμπί με το οποίο μπορεί ο χρήστης να συνδεθεί στο σύστημα δεν ήταν εμφανείς. Έχει τοποθετηθεί στο κάτω μέρος για να είναι πιο εμφανής.
	<u>Οθόνη 3:</u> Ένα από τα σχόλια ήταν ότι δεν είναι εμφανές ποιο αποτελεί κουμπί στο κυρίως μενού επομένως έχει προστεθεί ένα γκριζο πλαίσιο και έχουν μικρύνει τα εικονίδια.

4.4.4.2 Έρευνα Αξιολόγησης Δεύτερης έκδοσης:

Η αξιολόγηση της δεύτερης έκδοσης του πρωτοτύπου έφερε στην επιφάνεια κάποια προβλήματα που θα μπορούσε κάποιος χρήστης να έχει σχετικά με την κατανόηση των κουμπιών και της τοποθεσίας τους. Κυριότερο πρόβλημα ήταν η δημιουργία του καμβά όπου τα εικονίδια δεν ήταν και τόσο επεξηγηματικά. Για τους λόγους αυτούς αλλά και για αισθητικούς λόγους, έχει αποφασιστεί να γίνεται η γραφική δήλωση πολιτικών ιδιωτικότητας με ένα ιεραρχικό τρόπο. Για την δημιουργία της ιεραρχίας χρησιμοποιείται η δομή «δένδρο». Αναγκαία επομένως ήταν η δημιουργία της τρίτης και τελευταίας έκδοσης του πρωτοτύπου.

Στην πιο κάτω εικόνα φαίνεται ο τρόπος με τον οποίο, τόσο στο 2^ο όσο και στο 1^ο πρωτότυπο, γινόταν η δήλωση πολιτικών ιδιωτικότητας.

Policy Canvas:



Εικόνα:4.6

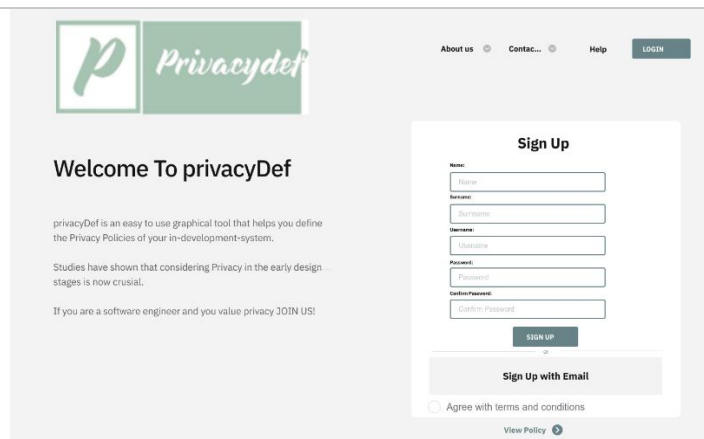
Σχετικά με την οθόνη 6 όπου αρχειοθετούνται οι πολιτικές, αποφασίστηκε ότι μάλλον αυτή η λειτουργία θα ήταν περιττή. Επομένως στο τελευταίο πρωτότυπο θα δημιουργηθεί κάτι σαν «γκαλερί», όπου όλες οι πολιτικές θα εμφανίζονται εκεί.

4.4.5 Πρωτότυπο 3 – Τρίτη έκδοση:

4.4.5.1 Σχεδίαση και Οθόνες:

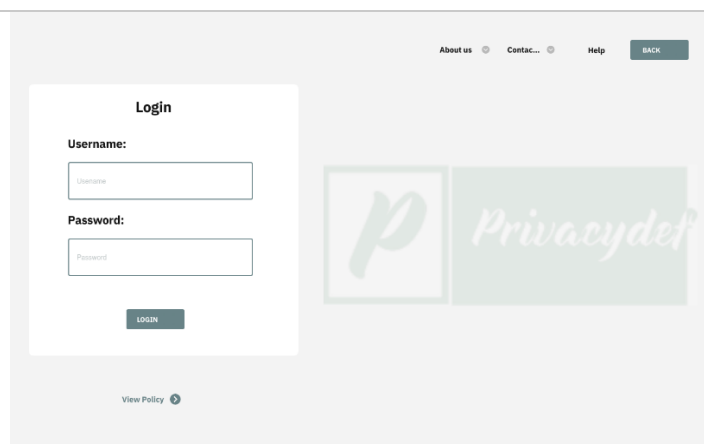
Οθόνες

Επεξήγηση και αλλαγές



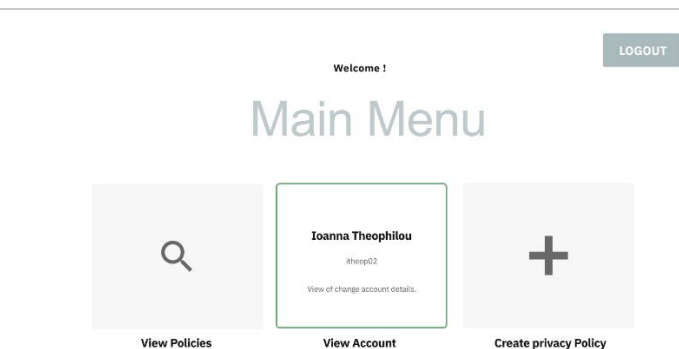
Οθόνη 1 :

Είναι η αρχική σελίδα. Οι αλλαγές που έγιναν από τις προηγούμενες εκδόσεις είναι ότι διαχωρίζονται πιο ορθά οι επιλογές για “sign up” και ο χρήστης πρέπει να πατήσει ότι δέχεται τους όρους και τις προϋποθέσεις αφού διαβάσει την πολιτική ιδιωτικότητας που ακολουθεί το privacyDef.



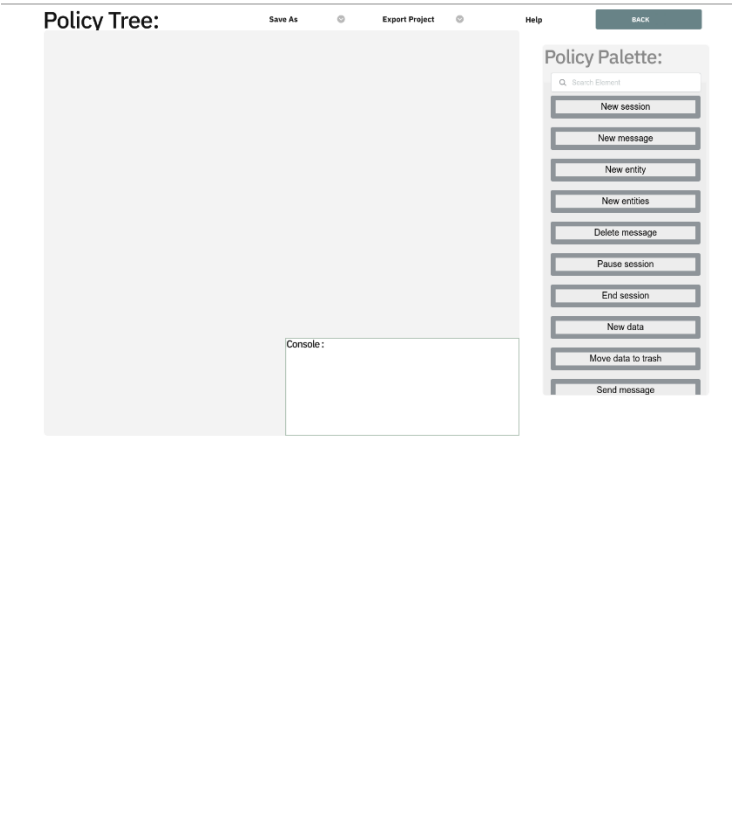
Οθόνη 2:

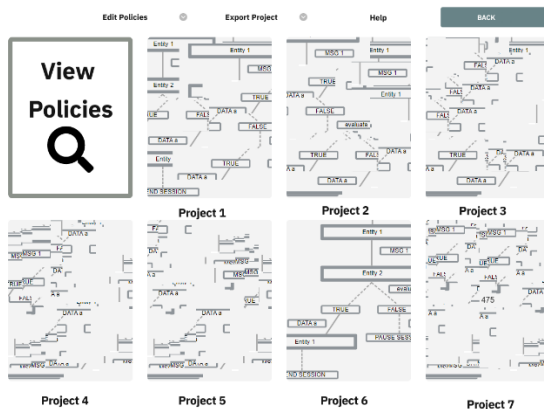
Εδώ δεν έχουν γίνει αλλαγές, αφού είχε υψηλό ποσοστό επιτυχίας σύμφωνα με τις αξιολογήσεις που έχουν γίνει.



Οθόνη 3:

Το κυρίως μενού έχει διαφοροποιηθεί, αφού σύμφωνα με τις αξιολογήσεις είναι καλύτερη επιλογή (για αισθητικούς λόγους) να δημιουργηθεί κάτι πιο συμμετρικό.

	<u>Οθόνη 4:</u> Οι μόνες αλλαγές που έγιναν σε αυτή την οθόνη είναι ότι προστέθηκε η επιλογή “Learn more” κάτω από κάθε κουμπί, για ευκολία του χρήστη και περισσότερη επεξήγηση. Ταυτόχρονα, αφού σύμφωνα με την δεύτερη έρευνα το “New Repository” δεν θεωρείται αναγκαίο, με την επιλογή “Edit Privacy Policies” θα μπορεί ο χρήστης να μεταβαίνει στην οθόνη 6 που εμφανίζεται μία γκαλερί με όλους τους καμβάδες.
	<u>Οθόνη 5:</u> Η οθόνη αυτή χρειάστηκε τις περισσότερες αλλαγές, όπως έχει παρουσιαστεί και στην ενότητα 4.4.4.2. Αντί καμβάς έχει δημιουργηθεί η δομή του δέντρου, και η παλέτα πλέον αποτελείται από επεξηγηματικά κουμπιά. Με το πάτημα του κουμπιού θα εμφανίζεται κόμβος ή ακμή στο δέντρο. Υπάρχει κάτω αριστερά και η κονσόλα που ενημερώνει τον χρήστη για τυχόν λάθη στην σειρά επιλογής κόμβων ή ακμών.



Οθόνη 6:

Η οθόνη αυτή έχει μετατραπεί σε μία «γκαλερί» από καμβάδες πολιτικών ιδιωτικότητας.

Υπάρχει και η επιλογή “Export” της πολιτικής σε διάφορες μορφές. Επίσης εάν ο χρήστης επιλέξει μία πολιτική, θα τον μεταφέρει στην οθόνη 5 όπου θα μπορεί να την επεξεργαστεί και να την ξανά-αποθηκεύσει.

My Account

My Information Review Contact Us

Due to GDPR, you can review the information we hold in our platform and you can change them anytime. You can also delete your account anytime. GIVE US A REVIEW BY TAPPING THE REVIEW BUTTON!

press to enable editing

Name Ioanna
Surname Theophiliou
Username ltheop02
Password *****
Email ltheop02@ucy.ac.cy

Delete my Account

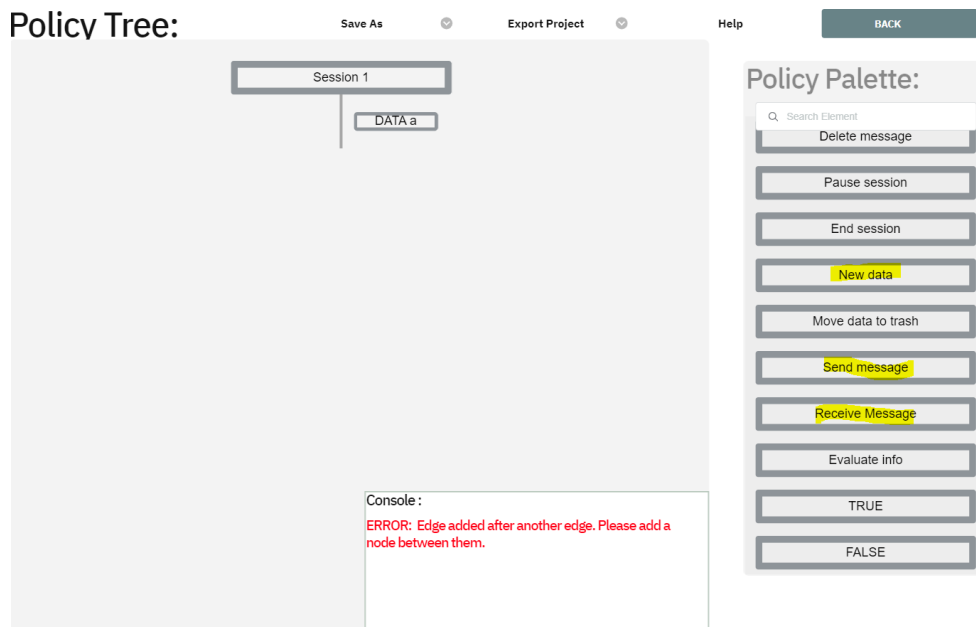
LOGOUT

BACK

Οθόνη 7:

Η οθόνη αυτή δεν έχει καθόλου αλλαγές σχετικά με τις 2 πρώτες εκδόσεις.

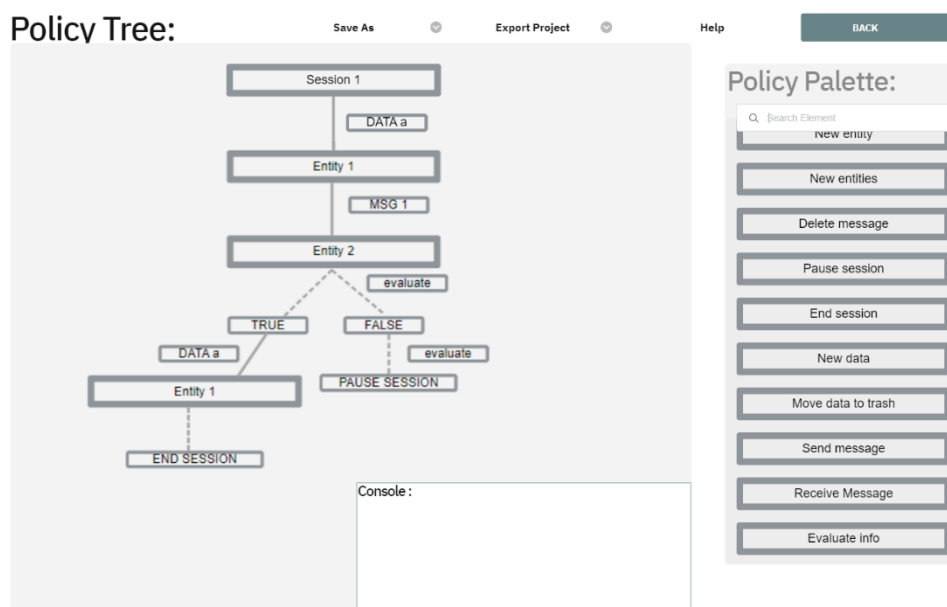
Όπως έχει αναφερθεί και πιο πάνω (ενότητα 4.4.4.2) υπήρξε η ανάγκη για μία ιεραρχική δομή στην γραφική δήλωση πολιτικών. Η πιο κάτω εικόνα παρουσιάζει το παράδειγμα δήλωσης της ενότητας 4.4.4.2 σε μία δεντρική δομή, η οποία είναι πιο κατανοητή και ορθή, αφού με την χρήση της κονσόλας, ο χρήστης μπορεί να είναι βέβαιος για τις κινήσεις του στην παλέτα.



Εικόνα :4.7

Όπως φαίνεται, εάν ο χρήστης κινηθεί στην παλέτα με αυτή την σειρά: “New entity”, “Send message”, “New data”, “Receive Message”, θα υπάρχει σφάλμα αφού μετά το “Send message” αναμένεται να υπάρχει μία οντότητα.

Πιο κάτω παρουσιάζεται το παράδειγμα της ενότητας 4.4.4.2 στην τελική του δεντρική μορφή μέσω της 3^{ης} έκδοσης του πρωτοτύπου:



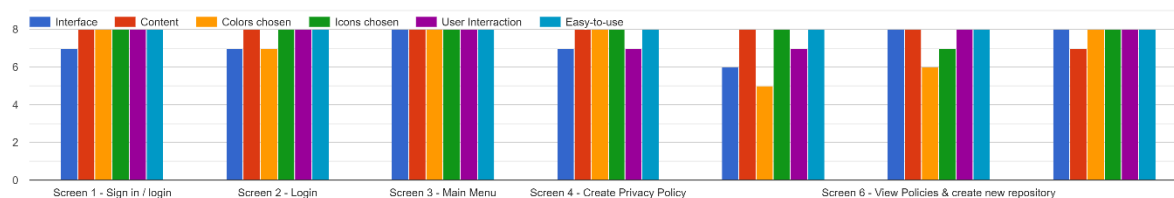
Εικόνα:4.7

4.4.5.2 Έρευνα Αξιολόγησης Τρίτης έκδοσης:

Οι συμμετέχοντες της τελευταίας έρευνας αξιολόγησης έλαβαν ένα νέο βίντεο που δείχνει το πρωτότυπο, και την αλληλεπίδραση του χρήστη με τις διάφορες οθόνες. Μετά την προβολή του βίντεο έπρεπε να απαντήσουν και πάλι κατά πόσο οι πιο κάτω μετρικές θεωρούνται επαρκής σε κάθε οθόνη.

Μετρικές:	Διεπαφή	Περιεχόμενο	Χρώματα	Εικονίδια	Αλληλεπίδραση με χρήστη	Εύκολο στη χρήση	Σύνολο:
Οθόνη 1:	100 %	100 %	100 %	100 %	100 %	100 %	100 %
Οθόνη 2:	87.5 %	100 %	87.5 %	100 %	100 %	100 %	95.8 %
Οθόνη 3:	100 %	100 %	100 %	100 %	100 %	100 %	100 %
Οθόνη 4:	87.5 %	100 %	100 %	100 %	87.5 %	100 %	95.8 %
Οθόνη 5:	75 %	100 %	62.5 %	100 %	87.5 %	100 %	87.5 %
Οθόνη 6:	100 %	100 %	75 %	87.5 %	100 %	100 %	93.75 %
Οθόνη 7:	100 %	87.5 %	100 %	100 %	100 %	100 %	98 %

Please select for each screen the options you think are correctly presented / fulfilling:



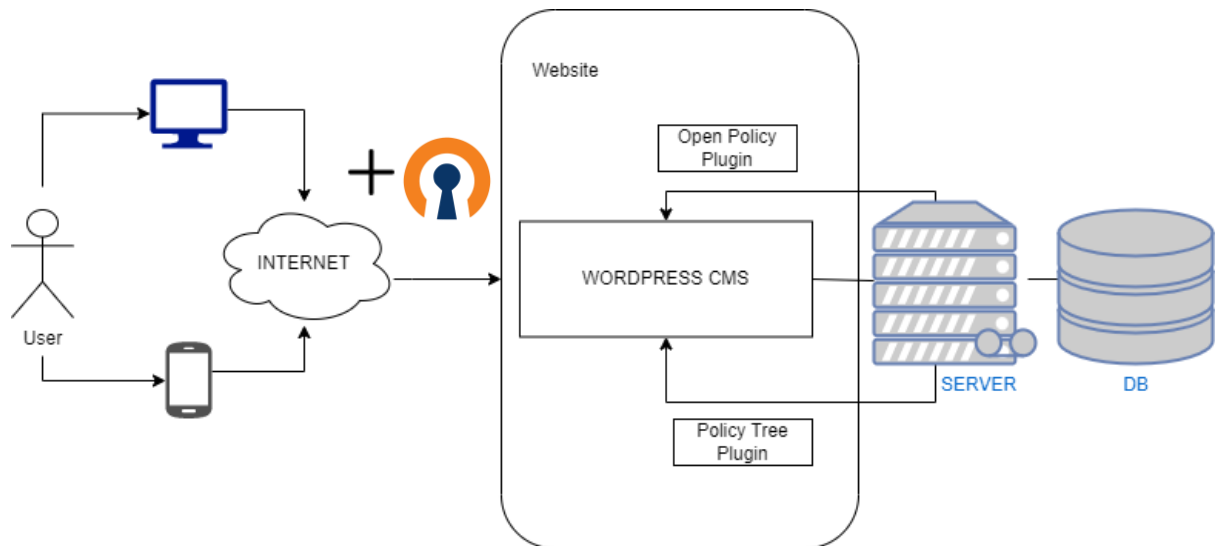
Τα αποτελέσματα είναι αρκετά θετικά, επομένως η υλοποίηση στηρίζεται σε αυτά τα στατιστικά και τα δεδομένα.

Το ερωτηματολόγιο βρίσκεται στον ακόλουθο σύνδεσμο:

<https://forms.gle/nD9oN9hHd1Z59cwH8>

4.5 Σχεδιασμός Εργαλείου

4.5.1 Αρχιτεκτονική:



Εικόνα :4.8

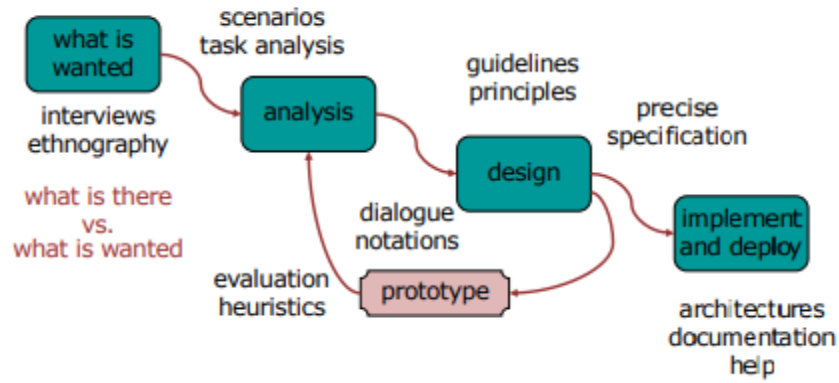
Στην πιο πάνω εικόνα, παρουσιάζεται η αρχιτεκτονική που ακολουθείται στο σύστημα. Αρχικά, ο κάθε χρήστης μπορεί να έχει πρόσβαση στην ιστοσελίδα, μέσω τηλεφώνου , μέσω υπολογιστή αλλά και οποιασδήποτε άλλης συσκευής που έχει πρόσβαση στο διαδίκτυο.

Όπως περιγράφεται και στην ενότητα 3, χρησιμοποιείται το εργαλείο WordPress το οποίο παρέχει διάφορες βοηθητικές και βασικές λειτουργίες στην διαδικασία του Web Development. Το εργαλείο επεκτάθηκε με δύο plug-ins τα οποία είναι υπεύθυνα για τις 2 κυριότερες λειτουργίες του εργαλείου privacyDef. Το πρώτο plugin είναι υπεύθυνο για την λειτουργία δημιουργίας της γραφικής δήλωσης των πολιτικών ιδιωτικότητας και το δεύτερο plugin είναι υπεύθυνο για την λειτουργία “upload” αρχείων JSON που περιγράφουν μία πολιτική, με σκοπό την προβολή της.

4.5.2 Διαδικασία Σχεδίασης:

Στην υπο-ενότητα αυτή περιγράφεται ο τρόπος και η διαδικασία σχεδίασης. Σχεδίαση είναι η επίτευξη στόχων εντός κάποιων περιορισμών. Στόχος είναι ο προσδιορισμός του λόγου δημιουργίας του συστήματος, και ποιες ακριβώς είναι οι απαιτήσεις [15]. Οι περιορισμοί μπορεί να είναι σχετικά με την πλατφόρμα ή και περιορισμοί υλικού. Πολλές φορές χρειάζεται να γίνει χαλάρωση κάποιων από τους περιορισμούς για να μπορέσουν να επιτευχθούν οι στόχοι, ή κάποιοι από αυτούς.

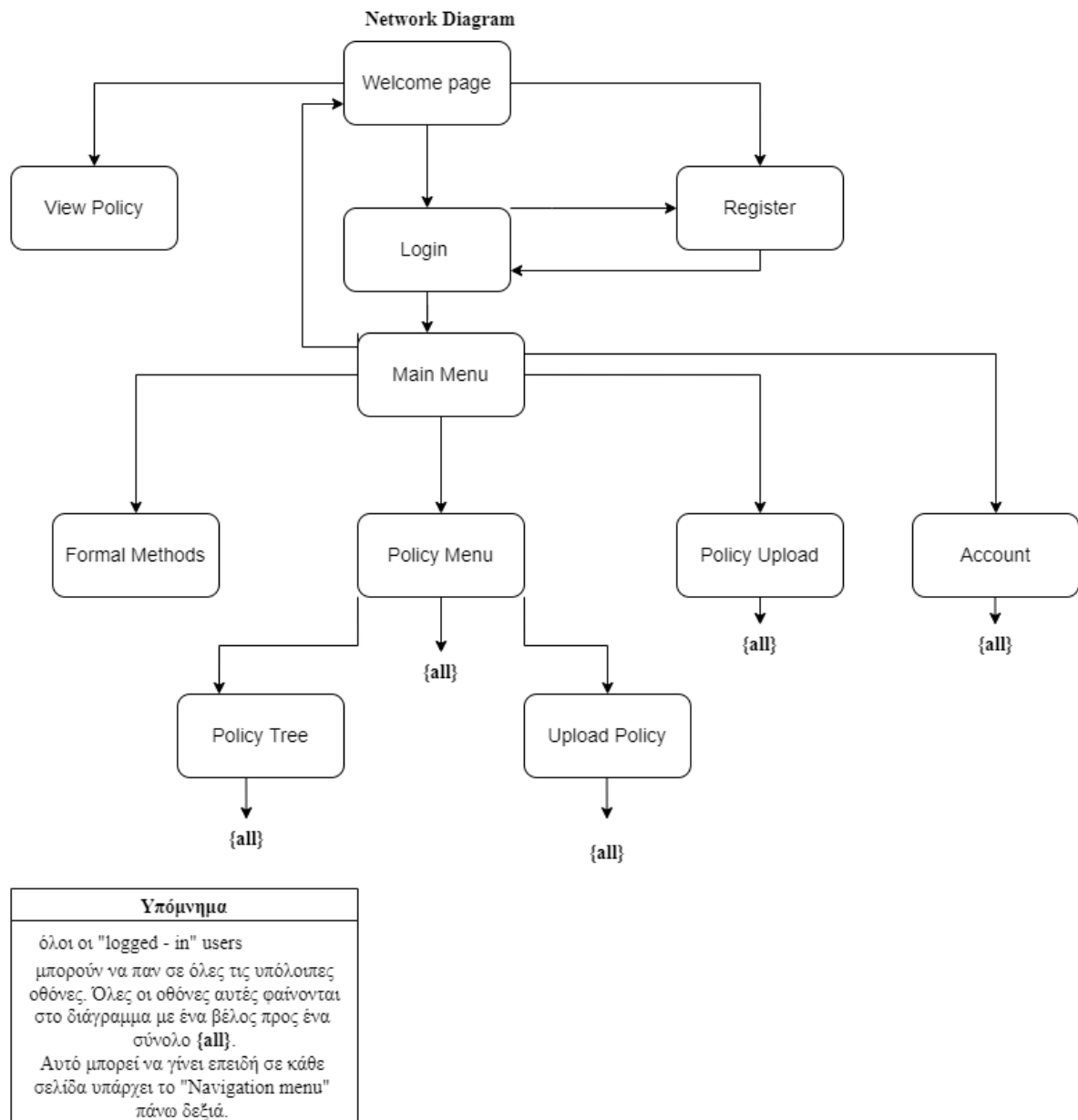
4.5.2.1 “The design Process”:



Εικόνα:4.9 [15]

Η πιο πάνω εικόνα περιγράφει τον τρόπο που έγινε η διαδικασία σχεδίασης του εργαλείου. Αρχικά έχουν εντοπιστεί οι απαιτήσεις, έγινε ανάλυση των απαιτήσεων, έπειτα η σχεδίαση και έχουν βρεθεί οι τελικές απαιτήσεις και ανάγκες μέσω των πρωτοτύπων που έχουν αναλυθεί στην ενότητα 4.

4.5.2.2 “Network Diagram”:



Εικόνα:4.10

Σε αυτό το ιεραρχικό διάγραμμα παρουσιάζεται ο τρόπος που μπορεί να γίνει η πλοήγηση μέσα στην ιστοσελίδα. Για ευκολία πλοήγησης, υπάρχει ένα Navigation menu πάνω δεξιά της σελίδας, έτσι ένας χρήστης ο οποίος έχει λογαριασμό, μπορεί να κινείται ελεύθερα. Όπως φαίνεται και στην πιο πάνω εικόνα, ο χρήστης που έχει λογαριασμό στο σύστημα, μπορεί όπου και εάν βρίσκεται να γνωρίζει τα ακόλουθα: πού βρίσκεται, πού μπορεί να πάει, πού ήταν πριν και τί μπορεί να κάνει.

Σημειώνεται ότι μέσα στο σύνολο {all} το οποίο περιλαμβάνει όλες τις σελίδες, περιέχεται και η αρχική σελίδα “Welcome page” όπου ο κάθε χρήστης μπορεί με την λειτουργία “logout” να βρεθεί εκεί ανά πάσα στιγμή.

Πιθανό παράδειγμα πλοήγησης : “Welcome page” , “Register” , “Login” , “Main Menu” , “Policy Menu”, “Policy Tree”, “Upload Project”, “Login”.

4.6 Υλοποίηση Εργαλείου

Όλα τα εργαλεία και οι τεχνολογίες που έχουν χρησιμοποιηθεί για την υλοποίηση του εργαλείου, αναφέρονται στην Ενότητα 3 και η επίδειξη του εργαλείου και των λειτουργιών του γίνεται στην Ενότητα 5, ενώ η αξιολόγησή του, παρουσιάζεται στην ενότητα 6.

4.6.1 Επεξήγηση Δομής Γραφικής Δήλωσης:

Η τρόπος που γίνεται η γραφική δήλωση μίας πολιτικής ιδιωτικότητας ακολουθεί την έννοια της δεντρικής δομής όπου ένας πρωταρχικός κόμβος επεκτείνεται σε άλλους. Όπως και στην δεντρική δομή, έτσι και εδώ, δεν επιτρέπονται οι κύκλοι. Δηλαδή ένας κόμβος μπορεί να έχει μία εξερχόμενη και μία εισερχόμενη σύνδεση, εκτός από τον κόμβο ο οποίος υλοποιεί το “branching / decision node” ο οποίος επιβάλλεται να έχει 2 εξερχόμενες συνδέσεις για την ένδειξη των “True” και “False”.

Υπάρχουν έξι ειδών συνδέσεις και επτά ειδών κόμβοι, δύο εκ των οποίων λειτουργούν ως ετικέτες . Παρουσιάζονται πιο αναλυτικά στους πιο κάτω πίνακες.

Συνδέσεις	Επεξήγηση	Περιορισμοί
“ Send Message ”	Αποστολή δεδομένου	-
“ Receive Message ”	Παραλαβή δεδομένου	
“ Evaluate ”	Κόμβος που συνδέει οτιδήποτε άλλο, με έναν «Κόμβο Απόφασης»	Πρέπει πάντα ο ένας κόμβος από τους 2 να είναι κόμβος απόφασης.
“ Continue Flow ”	Χρησιμοποιείται για την ένδειξη ότι συνεχίζει η ροή. Για παράδειγμα, μετά από τον κόμβο έναρξης, ή πριν από τον κόμβο λήξης	-
“ TRUE ”	Χρησιμοποιείται για την ένδειξη ότι κάτι ισχύει.	Πρέπει πάντοτε ο ένας κόμβος από τους 2 να είναι

	Χρησιμοποιείται πάντα μετά από έναν κόμβο απόφασης.	κόμβος απόφασης.
“FALSE ”	Χρησιμοποιείται για την ένδειξη ότι κάτι δεν ισχύει. Χρησιμοποιείται πάντα μετά από έναν κόμβο απόφασης.	Πρέπει πάντοτε ο ένας κόμβος από τους 2 να είναι κόμβος απόφασης.

Κόμβοι	Επεξήγηση	Περιορισμοί
“Initial Node”	Δηλώνει την αρχή της δήλωσης	Πάντα το επόμενο βήμα πρέπει να συνδέεται με σύνδεση τύπου “Continue Flow”
“Final Node”	Δηλώνει το τέλος της δήλωσης.	Πάντα το προηγούμενο βήμα πρέπει να συνδέεται με σύνδεση τύπου “Continue Flow”
“Decision Node”	Δηλώνει την απόφαση όπου οι συγκρίσεις που δίνετε να γίνουν είναι οι εξής : $\{ = , \leq , \geq \}$.	1. Πάντα πριν τον κόμβο αυτό πρέπει να προηγείται ακμή τύπου “Evaluate”. 2. Πάντα πριν μετά τον κόμβο αυτό πρέπει να έπονται συνδέσεις τύπου “TRUE” και “FALSE”.
“Entity”	Παριστάνει μία οντότητα του συστήματος	-
“ Data Store”	Παριστάνει μία οντότητα η οποία αναγνωρίζεται με τον τύπο – “Data type” και το όνομα – “Data name”.	Αναγνωριστικό θεωρείται το όνομα.
“True”	Είναι μία ετικέτα η οποία υπάρχει για βοηθητικούς λόγους, ένδειξης πού βρίσκεται το “TRUE” στο δέντρο.	-
“False”	Είναι μία ετικέτα η οποία	-

υπάρχει για βοηθητικούς λόγους, ένδειξης πού βρίσκεται το “FALSE” στο δέντρο.	
---	--

4.6.2 Επεξήγηση Δομής Μετατροπής σε Τυπική Γλώσσα:

4.6.2.1 Η τυπική Γλώσσα που χρησιμοποιείται

Ground Types	$g ::= \text{int} \mid \text{bool} \mid \dots$											
Exchange Types	$U ::= g \mid \text{pd}[U]^\alpha \mid \alpha$											
Global Types	$G ::=$ <table> <tr> <td>end</td> <td>Termination</td> </tr> <tr> <td>$\mid p \rightarrow q : U.G$</td> <td>Value Exchange</td> </tr> <tr> <td>$\mid \alpha \rightarrow p : U.G$</td> <td>Personal Data Read</td> </tr> <tr> <td>$\mid p \rightarrow \alpha : U.G$</td> <td>Personal Data Storage</td> </tr> <tr> <td>$\mid p \rightarrow q : (U \text{ op } U')\{\text{tt} : G_1, \text{ff} : G_2\}$</td> <td>Conditional Branching</td> </tr> </table>	end	Termination	$\mid p \rightarrow q : U.G$	Value Exchange	$\mid \alpha \rightarrow p : U.G$	Personal Data Read	$\mid p \rightarrow \alpha : U.G$	Personal Data Storage	$\mid p \rightarrow q : (U \text{ op } U')\{\text{tt} : G_1, \text{ff} : G_2\}$	Conditional Branching	
end	Termination											
$\mid p \rightarrow q : U.G$	Value Exchange											
$\mid \alpha \rightarrow p : U.G$	Personal Data Read											
$\mid p \rightarrow \alpha : U.G$	Personal Data Storage											
$\mid p \rightarrow q : (U \text{ op } U')\{\text{tt} : G_1, \text{ff} : G_2\}$	Conditional Branching											
Operators	$op ::= = \mid \geq \mid \leq$											

Εικόνα:4.11[2]

Στην πιο πάνω εικόνα παρουσιάζεται η σύνταξη/σημασιολογία της γλώσσας που χρησιμοποιείται. Οι βασικοί τύποι είναι όλοι οι βασικοί τύποι, όπως ακέραιοι κλπ. Σχετικά με τα “Exchange Types” μπορούν να είναι είτε βασικοί τύποι, είτε οποιαδήποτε πλειάδα από προσωπικά δεδομένα τα οποία έχουν το αναγνωριστικό «α», είτε το «α» αυτούσιο. Τα “Global Types” παρουσιάζουν τις διάφορες συνδέσεις που μπορούν να γίνουν, όπως αναφέρονται και στην πιο πάνω υπο-ενότητα. Τέλος οι “Operators” είναι οι τελεστές σύγκρισης σε περίπτωση ενός “conditional branching”.

4.6.2.2 Διαδικασία Μετατροπής

Αρχικά έχουν διαχωριστεί τα είδη των συνδέσεων και των κόμβων σε δύο σταθερούς πίνακες όπως φαίνεται και στον πιο κάτω κώδικα.

```
1 function formalMethod() {  
2  
3     . . . . . //More pieces of code in appendix  
4  
5 //Target Types  
6 const TargetTypes = ["start", "end", "entity", "decision", "data"  
7 ];  
8 //Connection Types  
9 const ConnectionTypes = ["continue", "send", "receive", "evaluate"  
10 , "true", "false"];  
11  
12 . . . . . //More pieces of code in appendix  
13  
14 var filename = "FormalTranslation.txt";  
15  
16 var str;  
17  
18 output.forEach((out)=>{  
19     str+=out + "\n" ;  
20 });  
21 alert("Formal Translation will be downloaded");  
22 //downloads the formal translation locally  
23 downloadFile(filename,str);  
24 }
```

Με το πάτημα του αντίστοιχου κουμπιού που μετατρέπει την δήλωση στην τυπική γλώσσα, η μετάφραση σώζεται τοπικά σε ένα αρχείο με όνομα “FormalTranslation.txt”. Ολόκληρος ο κώδικας της μετατροπής παρουσιάζεται στο Παράρτημα Β’.

Για την διαδικασία της μετατροπής, έχουν δημιουργηθεί τρεις δομές πινάκων. Η πρώτη δομή αφορά τους κόμβους, και ορίζεται ως εξής:

$$\forall t \in Targets \exists \{ id , text , type \},$$
$$type := [start , end , entity , decision , data]$$

Δηλώνει ότι το κάθε στοιχείο που βρίσκεται στην δομή Targets είναι μία τριάδα του id του, ενός “text” το οποίο αποθηκεύει την είσοδο του χρήστη, και το είδος του κόμβου αυτού.

Η δεύτερη δομή που έχει δημιουργηθεί, είναι η δομή που αφορά τις διάφορες συνδέσεις. Ορίζεται ως εξής:

$$\forall c \in Connectors \exists \{ id , from , to , type \},$$
$$type := [continue , send , receive , evaluate , true , false] ,$$
$$from \in Targets , to \in Targets ,$$

Δηλώνει ότι το κάθε στοιχείο που βρίσκεται στην δομή Connectors είναι μία τετράδα του id του, ενός “Target” from που δηλώνει τον κόμβο έναρξης της ακμής , ενός “Target” το που δηλώνει τον κόμβο λήξης της ακμής και το είδος της.

Τέλος, η τρίτη δομή που έχει δημιουργηθεί, είναι η δομή Output για την οποία ισχύουν τα πιο κάτω:

$$\forall out \in Output \exists \{ c.from.id, symb, c.to.id \}, \\ c \in Connectors,$$

| if $c.type = "continue"$ then $symb := ';' \text{ else if } c.type = "send"$ then $symb := '-->' \text{ else}$
 if $c.type = 'receive'$ then $symb := ':' \text{ else if } c.type = 'evaluate'$ then $symb := '.' \text{ else}$
 if $c.type = 'true'$ then $symb := 'true >>' \text{ else if } c.type = 'false'$ then $symb := 'false >>'$

Δηλώνει ότι το κάθε στοιχείο που βρίσκεται στην δομή Output είναι μία τριάδα η οποία δηλώνει τον αρχικό κόμβο, τον τελικό κόμβο και την σχέση τους, ανάλογα με το είδος της σύνδεσής τους.

Βάσει των πιο πάνω δομών δεδομένων, έγινε η όλη διαδικασία της μετατροπής μίας γραφικής δήλωσης πολιτικής ιδιωτικότητας, στην Τυπική γλώσσα.

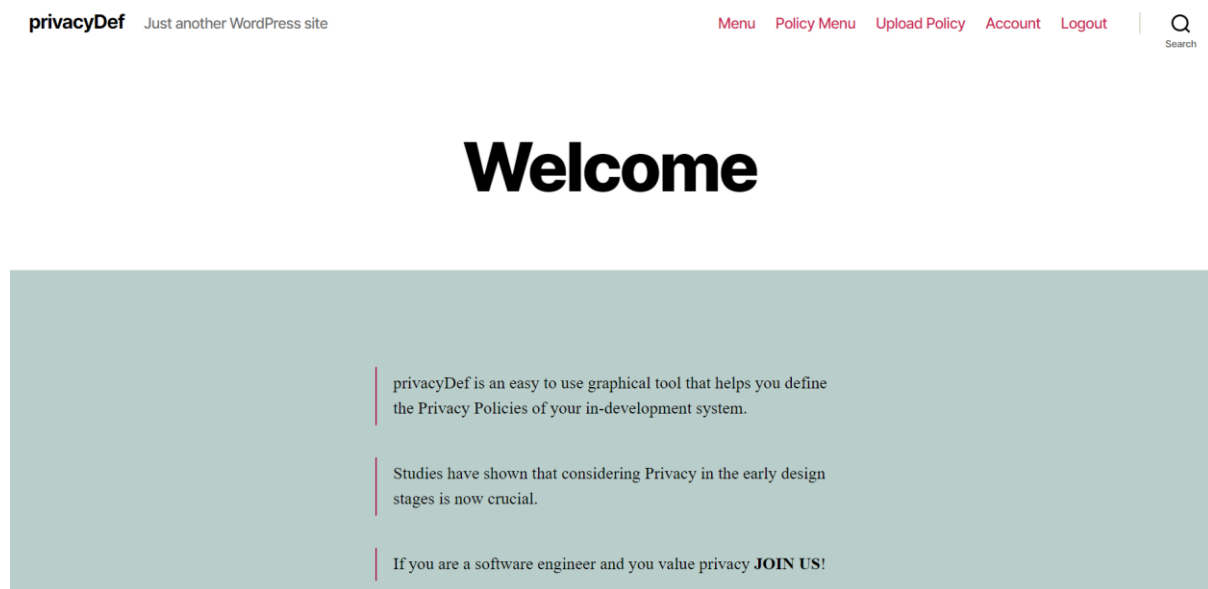
Κεφάλαιο 5

Επίδειξη Εργαλείου

5.1 Γενικές Λειτουργίες	47
5.1.1 Αρχική Σελίδα - “Login” – “Register” – “View Account”	47
5.1.2 “Main Menu” & Formal Methods Page	49
5.2 “Policy Menu” σελίδα	51
5.2.1 “Policy Tree”	51
5.2.1.1 “Policy Canvas”	52
5.2.1.2 “Palette”	52
5.2.1.3 “Instructions”	53
5.2.2 “Upload Policy”	54

5.1 Γενικές Λειτουργίες

5.1.1 Αρχική Σελίδα - “Login” – “Register” – “View Account”



Εικόνα: 5.1

Η πιο πάνω εικόνα είναι η αρχική σελίδα της ιστοσελίδας. Πάνω δεξιά φαίνεται το “navigation menu” ενός ήδη υπάρχον χρήστη. Ένας χρήστης που δεν είναι συνδεδεμένος, θα έχει διαφορετικό navigation menu μέσω του οποίου θα μπορεί να συνδεθεί στον λογαριασμό του εάν έχει, ή να δημιουργήσει λογαριασμό στην αντίθετη περίπτωση.

privacyDef

Just another WordPress site

[Login](#)[Register](#)

Q

Search

Login

Username or E-mail

itheop02

Password

☐ Keep me signed in

Login

Register

[Forgot your password?](#)

Εικόνα:5.2

Στην πιο πάνω εικόνα φαίνεται η διαδικασία εισδοχής στο σύστημα. Ένας χρήστης ο οποίος έχει ήδη λογαριασμό μπορεί με την είσοδο των στοιχείων του, να έχει τις υπηρεσίες που προσφέρει το privacyDef.

Register

Username

First Name

Last Name

E-mail Address

Password

Confirm Password

Confirm Password

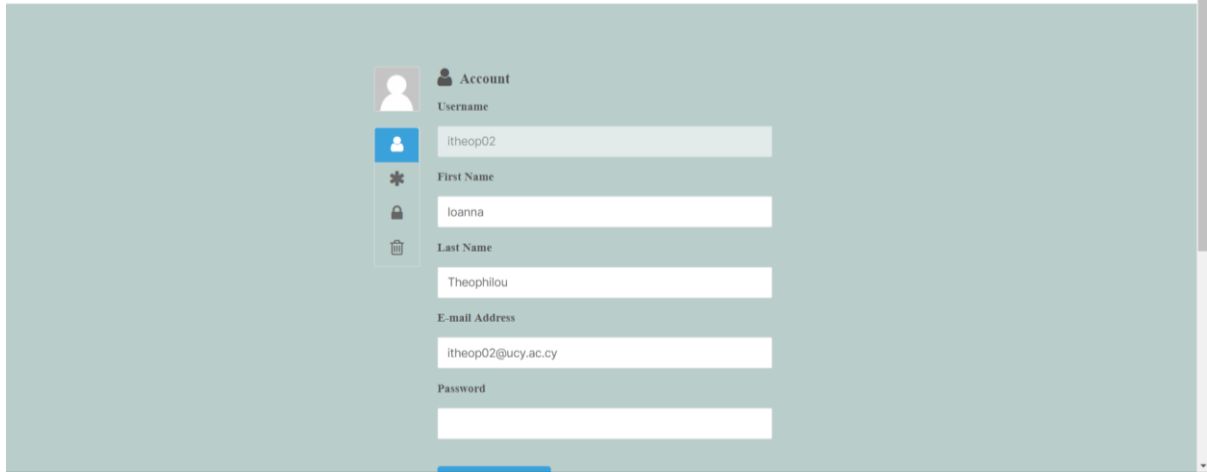
Register

Login

Εικόνα:5.3

Πιο πάνω παρουσιάζονται τα δεδομένα που συλλέγονται στην διαδικασία εγγραφής ενός χρήστη στο σύστημα.

Account

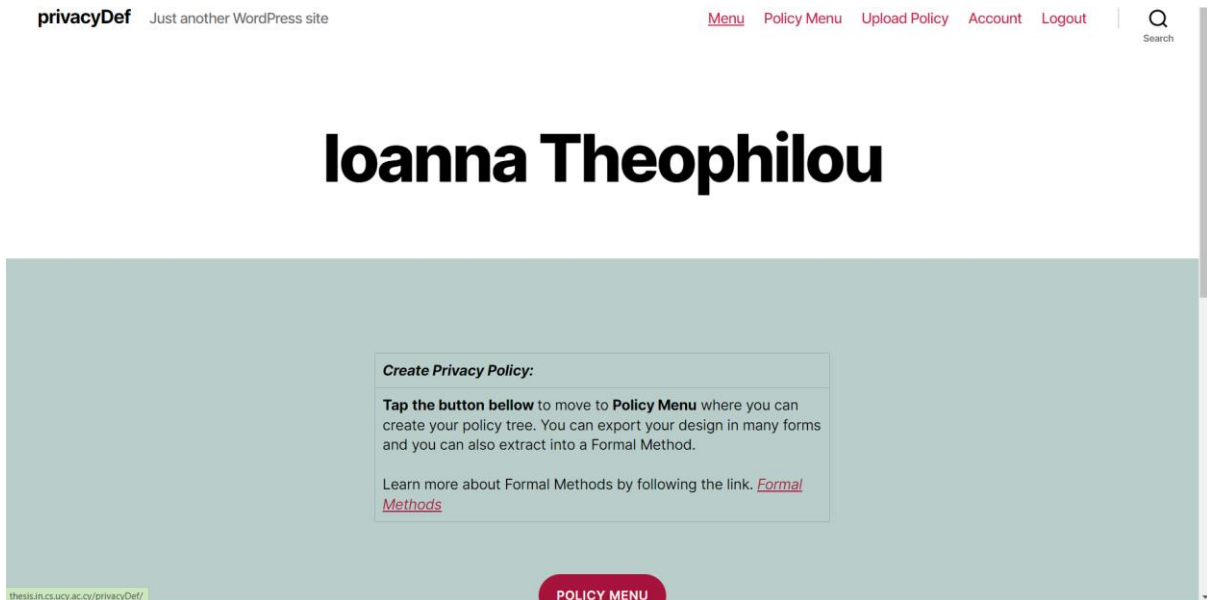


The screenshot shows a user account management interface. On the left, there is a vertical sidebar with icons for profile, settings, security, and trash. The main area contains a form with the following fields: Username (filled with 'itheop02'), First Name (filled with 'Ioanna'), Last Name (filled with 'Theophilou'), E-mail Address (filled with 'itheop02@ucy.ac.cy'), and Password (empty). The form is set against a light teal background.

Εικόνα : 5.4

Ένας χρήστης ο οποίος έχει λογαριασμό στο σύστημα, μπορεί να δει τα στοιχεία του λογαριασμού του και να τα αλλάξει εάν το θελήσει, ή και να διαγράψει τον λογαριασμό του πλήρως.

5.1.2 Main Menu & Formal Methods Page



The screenshot displays a website header with the text 'privacyDef Just another WordPress site' and a navigation menu with links: Menu, Policy Menu, Upload Policy, Account, and Logout. A search icon is also present. The main content area features the name 'Ioanna Theophilou' in large bold text. Below this, there is a box titled 'Create Privacy Policy:' containing instructions to tap a button to move to the 'Policy Menu' and create a policy tree. It also mentions that the design can be exported into various forms and extracted into a Formal Method. A link 'Formal Methods' is provided for more information. At the bottom of the page, there is a red button labeled 'POLICY MENU'.

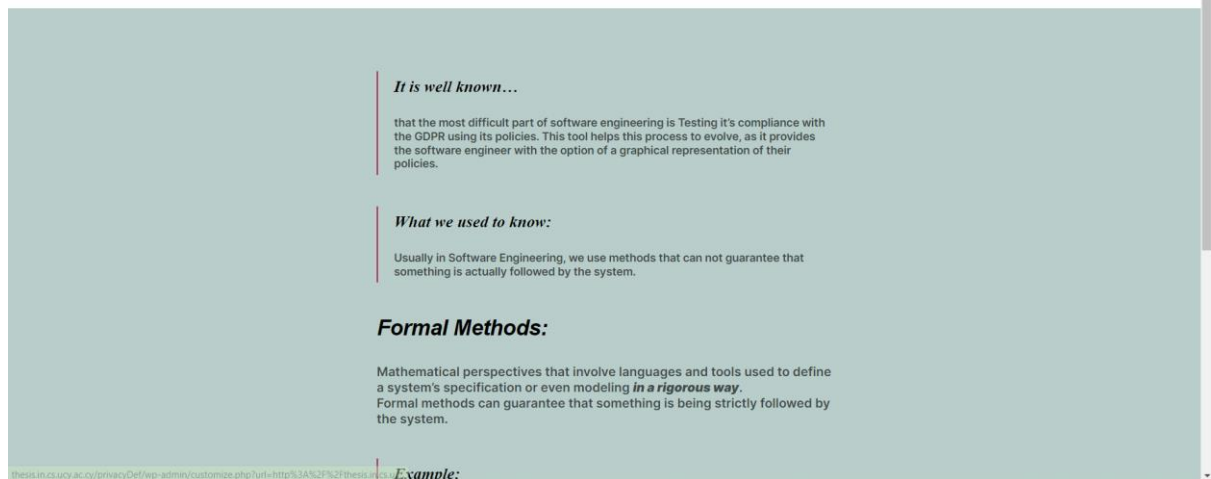
Εικόνα : 5.5

Πιο πάνω παρουσιάζεται το κυρίως μενού ενός εγγεγραμμένου χρήστη. Από αυτή την σελίδα μπορεί να μεταβεί στο “Policy Menu” και στο “Upload Policy”. Εάν το επιθυμεί,

μπορεί να μεταβεί στο “Formal Methods” όπου μπορεί να μάθει περισσότερα πράγματα για τις τυπικές γλώσσες.

Η κάθε λειτουργία επεξηγείται και στο “navigation menu” διαφαίνεται ότι ο χρήστης ξέρει ανά πάσα στιγμή το πού βρίσκεται, τί μπορεί να κάνει εκεί που βρίσκεται και πού μπορεί να μεταβεί.

Formal Methods

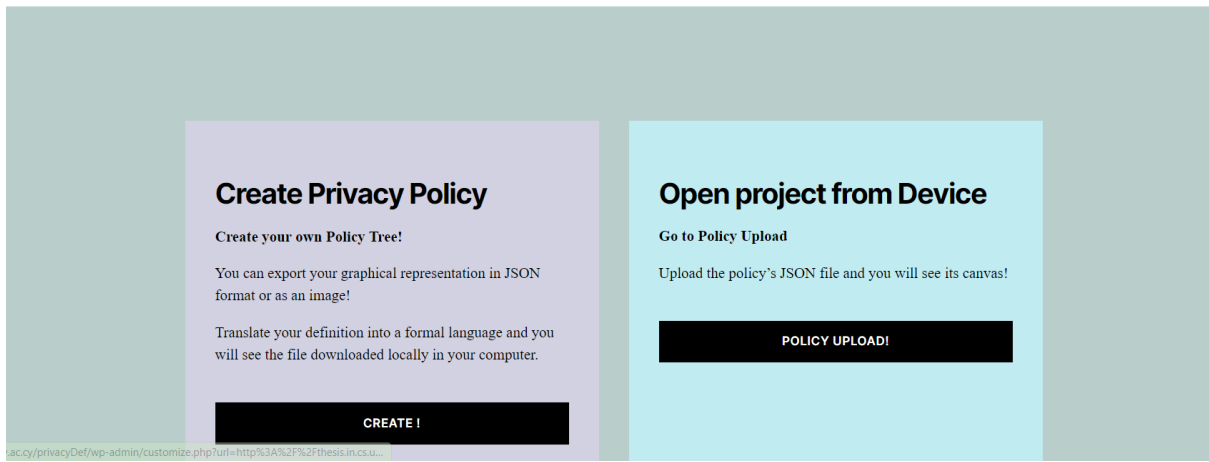


Εικόνα: 5.6

Εδώ ο χρήστης έχει πρόσβαση μέσω της κύριας σελίδας του συστήματος ή αλλιώς το “Main Menu”. Ο χρήστης του εργαλείου μπορεί να μάθει ένα μικρό ιστορικό για τις τυπικές γλώσσες, γιατί είναι χρήσιμες, τί είναι και να δει ένα παράδειγμα στο κάτω μέρος της σελίδας.

5.2 “Policy Menu” σελίδα

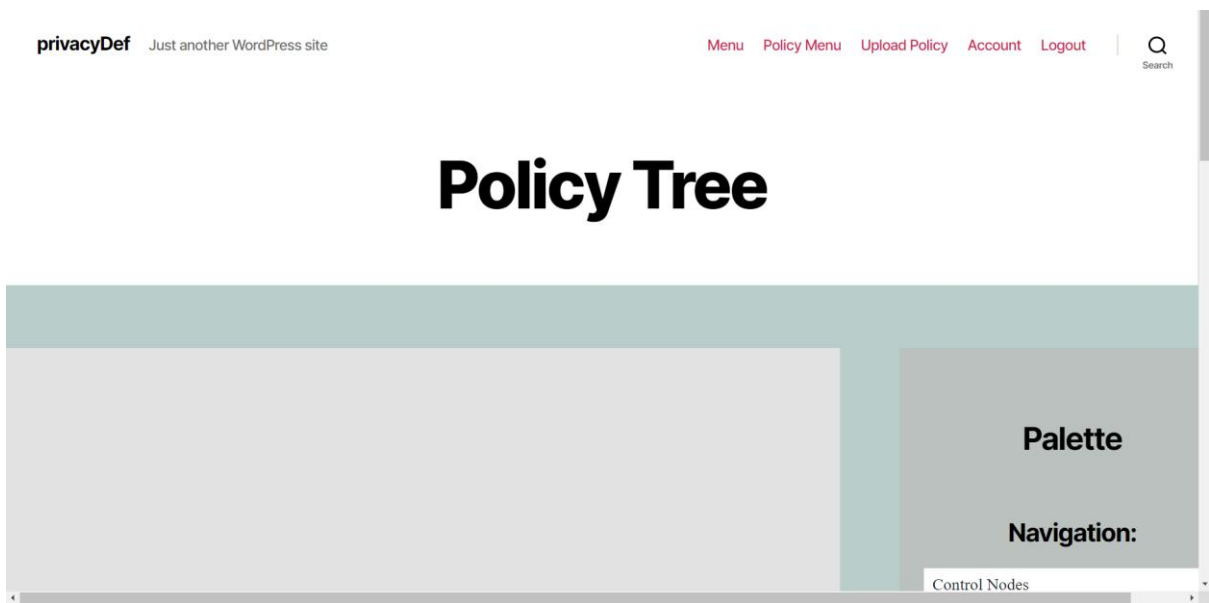
Policy Menu



Εικόνα : 5.7

Πιο πάνω, παρουσιάζεται το “Policy Menu” το οποίο παρουσιάζει και εξηγεί τις δύο επιλογές που έχει ως χρήστης (δημιουργία ή ανέβασμα πολιτικής).

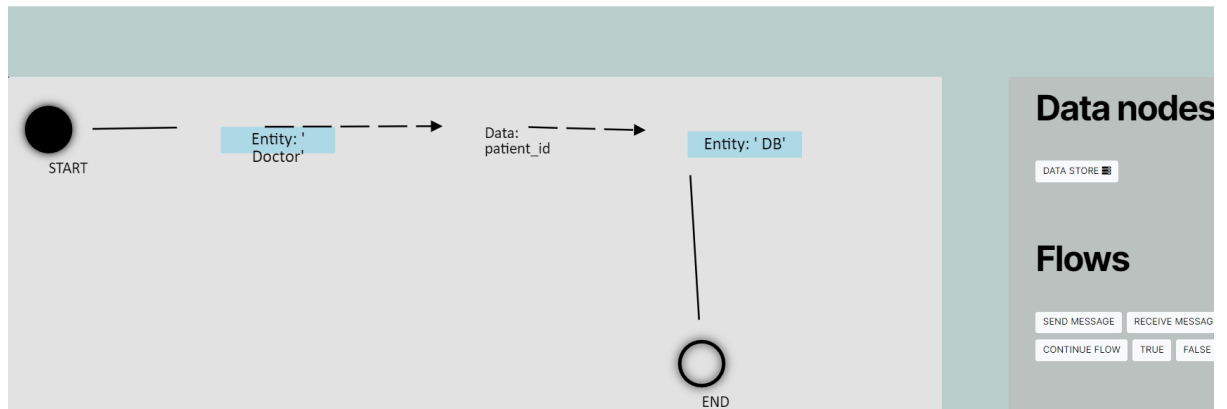
5.2.1 “Policy Tree”



Εικόνα:5.8

Στην πιο πάνω εικόνα, παρουσιάζεται το “Policy Tree”. Δεξιά της οθόνης φαίνεται η παλέτα η οποία περιέχει τους κόμβους και τις συνδέσεις και άλλα πολλά τα οποία θα αναλυθούν στην ενότητα 5.2.1.2.

5.2.1.1 “Policy Canvas”

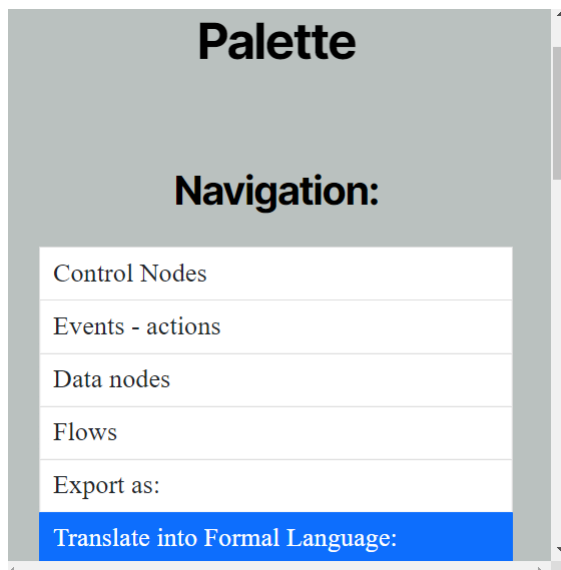


Εικόνα : 5.9

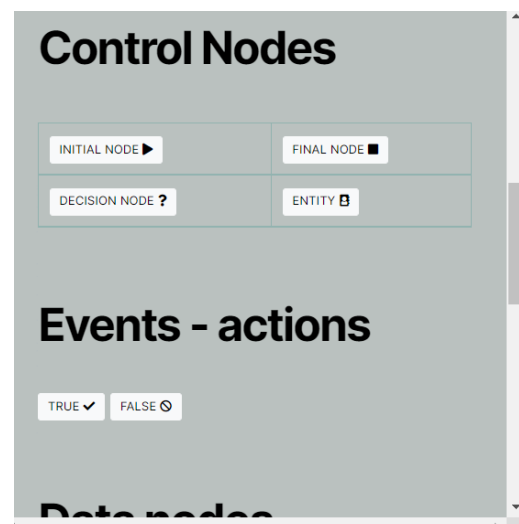
Στην εικόνα 5.9 παρουσιάζεται ο καμβάς στον οποίο εμφανίζονται οι συνδέσεις και οι διάφοροι κόμβοι που χρειάζονται για την δήλωση μίας πολιτικής.

Όλοι οι κόμβοι που απαρτίζουν μία πολιτική, μπορούν να κινηθούν στον καμβά και οι συνδέσεις τους δεν θα χαθούν. Οι συνδέσεις δηλαδή, ακολουθούν τον κόμβο που αλλάζει θέση και προσαρμόζονται αναλόγως της τοποθεσίας του κόμβου.

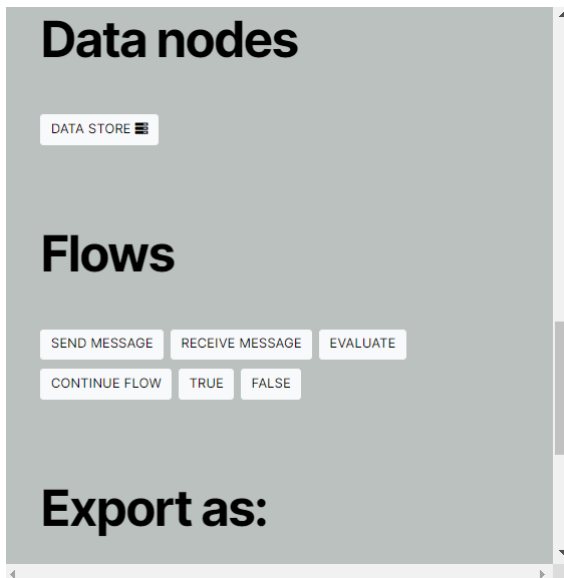
5.2.1.2 “Palette”



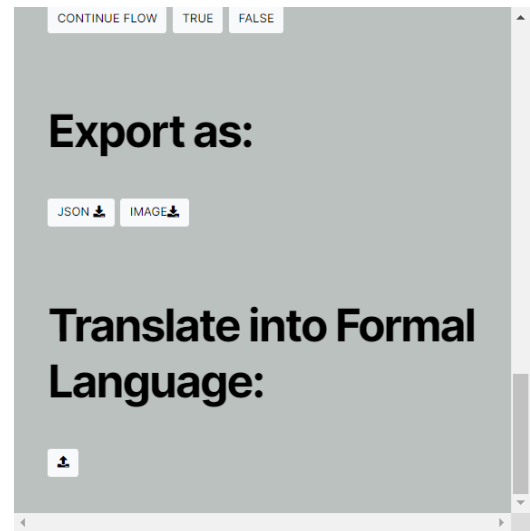
Εικόνα: 5.10



Εικόνα: 5.11



Εικόνα: 5.13



Εικόνα: 5.14

Πιο πάνω στις εικόνες 5.10 – 5.14 παρουσιάζεται η δομή τη παλέτας από την αρχή μέχρι και το τέλος της. Στην αρχική εικόνα παρουσιάζεται ένα “navigation bar” το οποίο μεταφέρει τον χρήστη στο επιλεγμένο σημείο της παλέτας. Οι λειτουργίες Export as JSON, Image και Translate into Formal Language, κατεβάζουν τοπικά αρχεία τα οποία ο χρήστης μπορεί να χρησιμοποιήσει μεταγενέστερα.

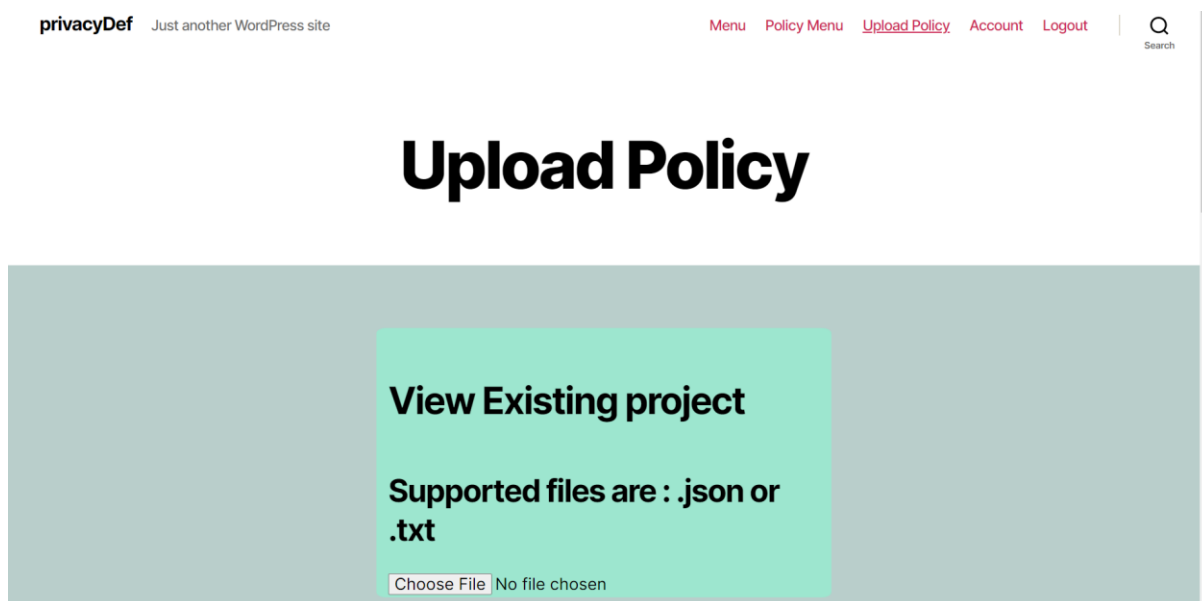
5.2.1.3 “Instructions”

Instructions :						
Actions	Dependent	Valid Action 1	Valid Action 2	Valid Action 3	Valid Action 4	Description
Initial Node	-	Continue flow	-	-	-	Press it to start the session
Final Node	Continue Flow before it	-	-	-	-	Press it to end the session
Decision Node	Evaluate node before it	True Flow	False Flow	True Label in Actions	False Label in Actions	Press it to show a decision
Entity Node	-	Send message Flow	Receive message Flow	Continue Flow Flow in Actions (if the next will be an ending node)	-	Press it to define an entity
Data Store	-	Send message Flow	Receive message Flow	Continue Flow Flow in Actions (if the next will be an ending node)	-	Press it to define a data store. Hovering above it, reveal the type.
General Instructions	-	Double tap on an element to delete it	Pressing a flow requires 2 elements to be presented	-	-	-

Εικόνα : 5.15

Στην πιο πάνω εικόνα παρουσιάζονται οι διάφορες οδηγίες που παρέχονται στο κάτω μέρος της σελίδας “Policy Tree” κάτω από τον καμβά. Δίνονται διάφορες επεξηγηματικές οδηγίες, τόσο για τις συνδέσεις, όσο και για τους κόμβους αλλά και γενικές πληροφορίες, όπως ο τρόπος που μπορεί να διαγραφεί ένα στοιχείο από τον καμβά.

5.2.2 “Upload Policy”



Εικόνα : 5.16

Τέλος, στην εικόνα αυτή, παρουσιάζεται η λειτουργία, όπου ένας χρήστης έχει την δυνατότητα να ανεβάσει το JSON ή το .txt αρχείο μίας πολιτικής και να δει την γραφική της δήλωση.

Κεφάλαιο 6

Αξιολόγηση Εργαλείου

6.1 Εισαγωγή	55
6.2 Μεθοδολογία	55
6.3 Ερωτηματολόγιο	56
6.3.1 Περιγραφή και κίνητρα διεξαγωγής Έρευνας	56
6.3.2 Σενάριο Αξιολόγησης	57
6.3.3 Αποτελέσματα Σεναρίου	58
6.4 Αποτελέσματα Έρευνας / Ερωτηματολογίου	60

6.1 Εισαγωγή

Στο κεφάλαιο αυτό, περιγράφεται η διαδικασία που έχει ακολουθηθεί για την διεξαγωγή της έρευνας αξιολόγησης του εργαλείου “privacyDef”. Αρχικά περιγράφεται η μεθοδολογία η οποία ακολουθήθηκε και στην συνέχεια, παρουσιάζονται οι λεπτομέρειες σχετικά με το ερωτηματολόγιο.

6.2 Μεθοδολογία

Έχει ακολουθηθεί η μεθοδολογία διεξαγωγής έρευνας με χρήση ερωτηματολογίου. Αρχικά στην έρευνα αυτή, γίνεται μία περιγραφή των κινήτρων διεξαγωγής της και έπειτα ζητείται η συγκατάθεση των συμμετεχόντων για να προχωρήσουν με τη διεξαγωγή της. Συνάμα, έχει δημιουργηθεί ένα βίντεο το οποίο περιγράφει ένα σενάριο χρήστης του εργαλείου privacyDef, τόσο στην δήλωση πολιτικών ιδιωτικότητας όσο και σε άλλες βασικές λειτουργίες. Επεξηγείται και παρουσιάζεται δηλαδή σε αυτό το βίντεο, η κάθε πιθανή κίνηση ενός “Demo” χρήστη. Οι οδηγίες που έχουν δοθεί στους συμμετέχοντες της έρευνας, ήταν να παρακολουθήσουν το βίντεο και στην συνέχεια να χρησιμοποιήσουν το εργαλείο. Περισσότερες πληροφορίες σχετικά με αυτό το στάδιο συμπλήρωσης του ερωτηματολογίου, αναφέρονται στην ενότητα 6.3.2.

6.3 Ερωτηματολόγιο

Το ερωτηματολόγιο βρίσκεται στον πιο κάτω σύνδεσμο:

<https://forms.gle/GPNPLSXALemLDzV46>

6.3.1 Περιγραφή και κίνητρα διεξαγωγής Έρευνας

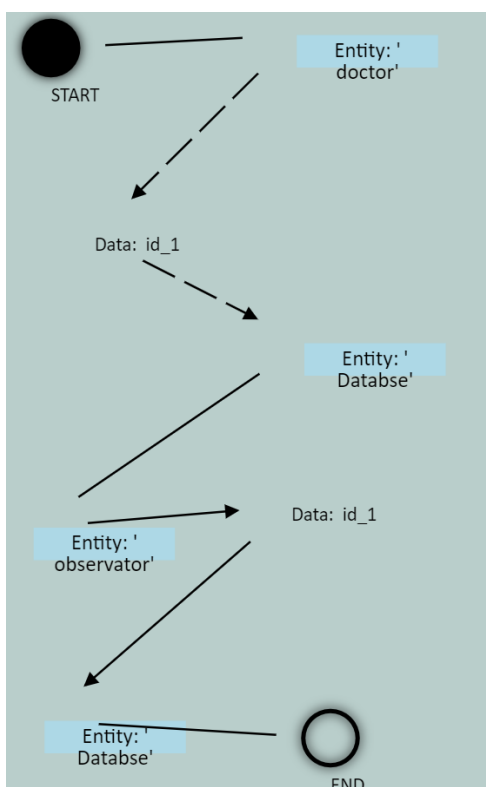
Η έρευνα αυτή είχε σκοπό την αντικειμενική αξιολόγηση του εργαλείου privacyDef με σκοπό την βελτίωσή του σε μεταγενέστερο στάδιο αλλά και την κατανόηση των οποιονδήποτε δυσκολιών που μπορεί να ήρθαν αντιμέτωποι οι χρήστες.

Στην έρευνα έλαβαν μέρος 10 άτομα, τεταρτοετής φοιτητές του τμήματος πληροφορικής.

Αρχικά, όπως έχει αναφερθεί και πιο πάνω, έχει δημιουργηθεί ένα βίντεο το οποίο δείχνει τις διάφορες λειτουργίες που υποστηρίζει το σύστημα. Μέσα σε αυτές και η δημιουργία πολιτικής. Στο βίντεο παρουσιάζεται το πιο κάτω σενάριο:

«Είστε μηχανικός λογισμικού για ένα σύστημα που παρέχει υπηρεσίες σε ιατρούς και επόπτες ενός νοσοκομείου. Ο ιατρός μπορεί να στείλει διάφορα αιτήματα στον επόπτη. Εάν ένας ιατρός στείλει αίτημα προς την βάση, τότε ο επόπτης έχει το δικαίωμα να το διαβάσει και να το εγκρίνει ή να το απορρίψει στέλνοντας και εκείνος με την σειρά του, την πληροφορία αυτή προς την βάση σημειώνοντας σε ποιο αίτημα αναφέρεται. Επομένως έχει το δικαίωμα να το διαβάσει από την βάση και να στείλει πίσω απάντηση.»

Η πολιτική ιδιωτικότητας που παρουσιάζεται στο βίντεο είναι η ακόλουθη:



«Ο ιατρός στέλνει το Data: id_1 στην βάση. Έπειτα ο επόπτης μπορεί να πάρει το Data: id_1 από την βάση.»

Εικόνα:6.1

6.3.2 Σενάριο Αξιολόγησης

Μόλις οι συμμετέχοντες έβλεπαν το βοηθητικό βίντεο, διάβαζαν ένα σχετικό σενάριο και καλούνταν να το υλοποιήσουν χρησιμοποιώντας το εργαλείο.

Το σενάριο περιέγραφε το εξής:

«Είστε μηχανικός λογισμικού για ένα σύστημα που παρέχει υπηρεσίες σε ιατρούς και εργαζομένους φαρμακευτικής ασφάλειας ενός νοσοκομείου. Οι εργαζόμενοι φαρμακευτικής ασφάλειας, έχουν κυρίως εποπτικό ρόλο.

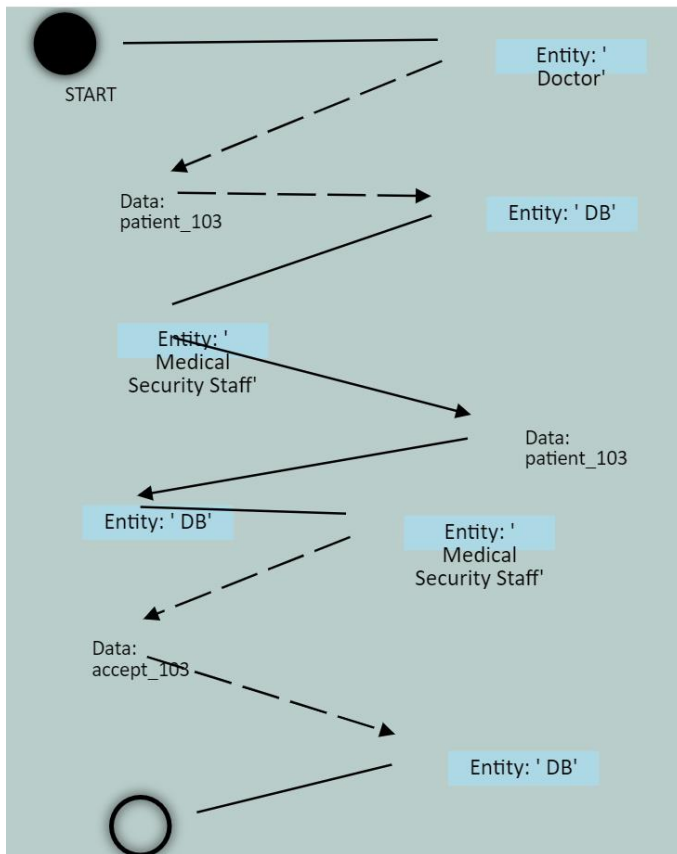
Θέλετε να δηλώσετε την πολιτική του συστήματός σας με ένα τυπικό, αυστηρό και μαθηματικό τρόπο, όμως δεν είστε εξοικειωμένοι με τις τυπικές γλώσσες και θα ήταν πολύ πιο δύσκολο, έχοντας επίσης την σκέψη ότι μπορεί να κάνετε και διάφορα λάθη.

Έχετε πληροφορηθεί ότι το `privacyDef` είναι ένα εργαλείο, που επιτρέπει την γραφική δήλωση πολιτικών και αυτομάτων με ένα κουμπί, μεταφράζει την δήλωση αυτή σε μία τυπική γλώσσα. Αποφασίζεται να το δοκιμάσετε.

Δηλώστε την πιο κάτω πολιτική, με χρήση του εργαλείου:

Ο ιατρός αλλά και ο εργαζόμενος φαρμακευτικής ασφάλειας του νοσοκομείου, μπορούν να έχουν πρόσβαση στις προσωπικές πληροφορίες των ασθενών, όπως την ταυτότητά τους. Ένας ιατρός, είναι υπεύθυνος για πολλούς ασθενής. Εάν ένας ασθενής του έχει αποβιώσει, τότε πρέπει να στείλει ένα αίτημα στην βάση δεδομένων, με την πληροφορία ότι ο ασθενής με αυτή την ταυτότητα έχει αποβιώσει. Έπειτα εάν το αίτημα αυτό υπάρχει στην βάση, τότε ο εργαζόμενος φαρμακευτικής ασφάλειας, μπορεί να το λάβει (με όλα τα στοιχεία τα οποία περιέχει το αίτημα αυτό) και μπορεί να το αποδεχτεί. Για να το αποδεχτεί, πρέπει να χρησιμοποιήσει και πάλι την ταυτότητα του ασθενή, για να στείλει στην βάση εάν έχει αποδεχτεί το αίτημα το οποίο αφορά τον ασθενή αυτό.»

Μία ενδεικτική πολιτική που να περιγράφει το πιο πάνω σενάριο είναι η εξής:



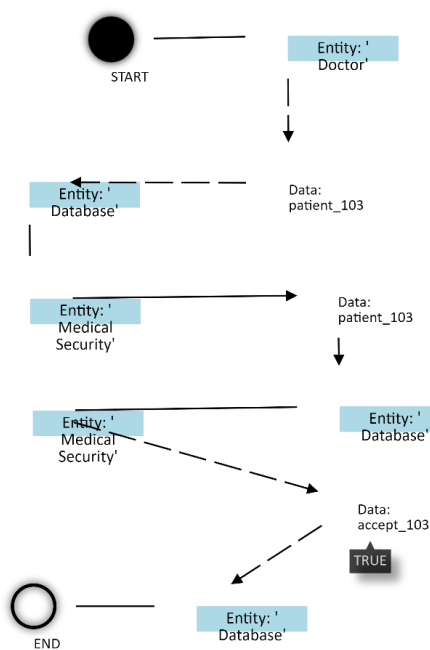
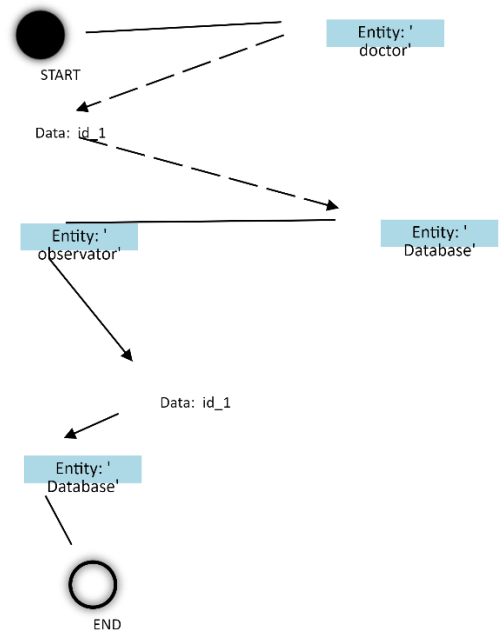
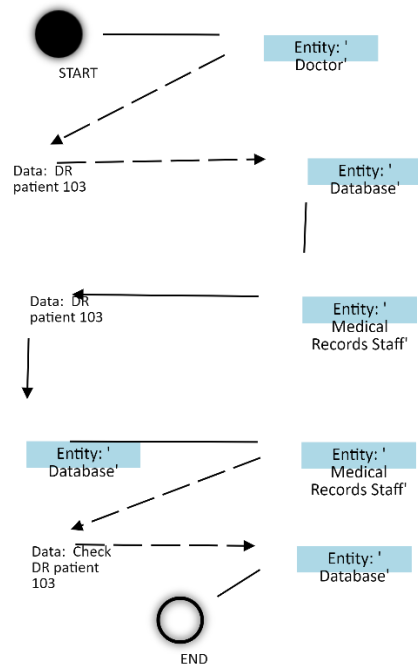
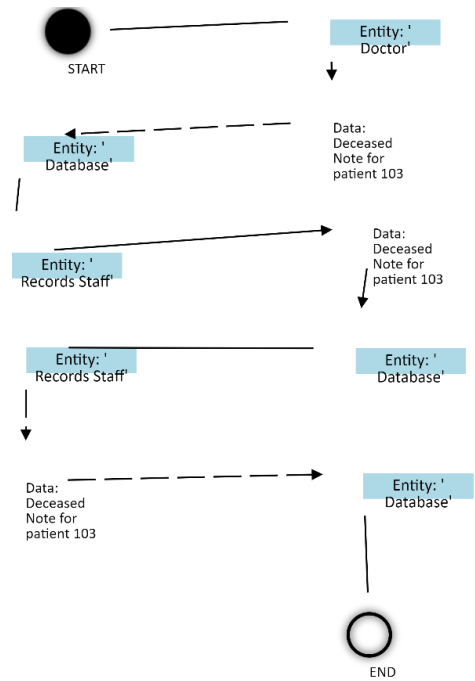
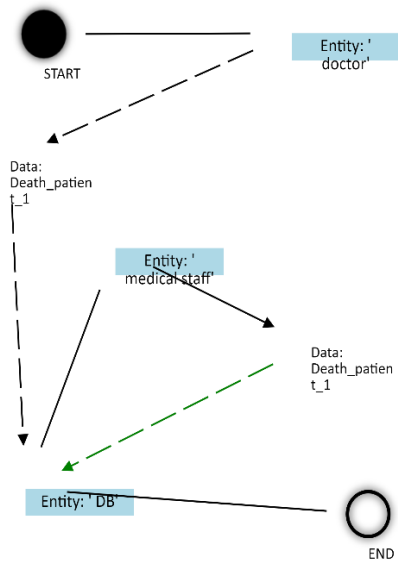
Εικόνα:6.2

6.3.3 Αποτελέσματα Σεναρίου

Μετά την δήλωση της πολιτικής ιδιωτικότητας, οι συμμετέχοντες της έρευνας, καλούνταν να χρησιμοποιήσουν την επιλογή “Export as image” που παρέχει το εργαλείο, και να στείλουν την πολιτική τους μέσω email.

Αυτό έχει γίνει με την συγκατάθεσή τους. Είχαν δηλαδή την επιλογή να μην στείλουν την πολιτική που δήλωσαν.

Πιο κάτω παρουσιάζεται ένας πίνακας από δηλώσεις της πολιτικής του ίδιου σεναρίου, από διαφορετικούς συμμετέχοντες.

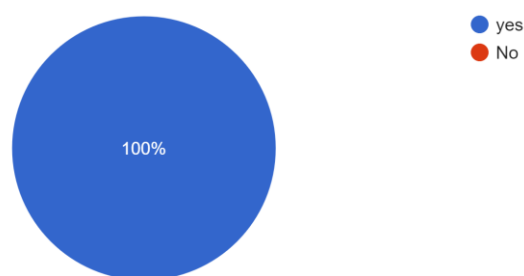


Παρατηρείται πιο πάνω ότι όλες οι πολιτικές είναι σχεδόν όμοιες, εκτός από την πρώτη, όπου ο χρήστης έχει σημειώσει στην αξιολόγησή του ότι δεν ήταν ξεκάθαρο το γεγονός ότι ένα έγκυρο διάγραμμα έχει δεντρική μορφή και όχι μορφή γράφου. Ορθά όμως, έλαβε το μήνυμα λάθους.

6.4 Αποτελέσματα Έρευνας / Ερωτηματολογίου

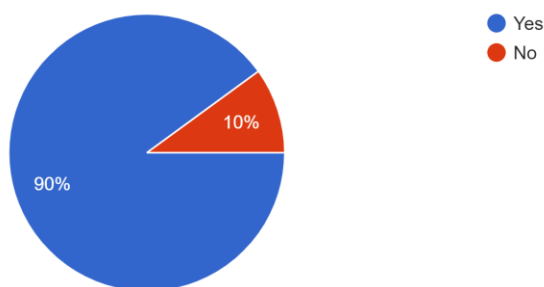
Πιο κάτω παρουσιάζονται τα αποτελέσματα, της έρευνας αξιολόγησης του εργαλείου.

1. State the following: Have you seen the instruction's video?
10 απαντήσεις



Στο πιο πάνω διάγραμμα φαίνεται ότι όλοι οι συμμετέχοντες έχουν παρακολουθήσει το βοηθητικό βίντεο που τους έχει σταλεί σχετικά με πληροφορίες και οδηγίες χρήσεις του εργαλείου.

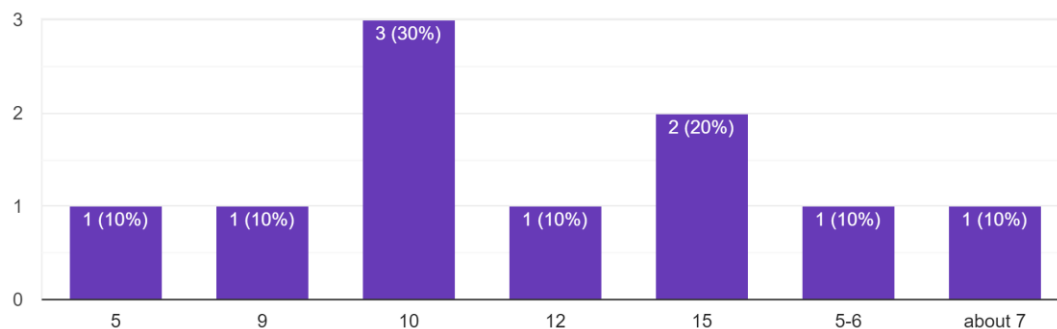
2. Have you successfully completed the task?
10 απαντήσεις



Ένα άτομο από τα δέκα δεν έχει ολοκληρώσει επιτυχώς την γραφική δήλωση του σεναρίου, που σημαίνει ότι έχει πάρει μήνυμα λάθους σχετικά με την ορθότητα του διαγράμματος κατά την δημιουργία της μετάφρασης σε τυπική γλώσσα.

3. How long did it take to complete the task ? (in minutes)

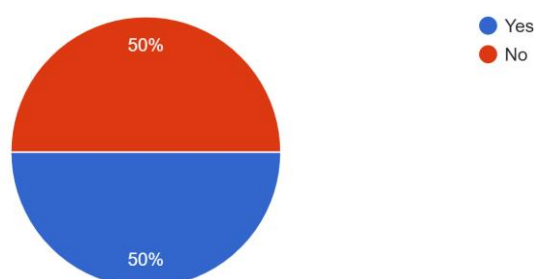
10 απαντήσεις



Σύμφωνα με το πιο πάνω διάγραμμα ο μέσος όρος χρόνου διάρκειας της ολοκλήρωσης του έργου που έχει ανατεθεί στους συμμετέχοντες είναι : $(5 + 9 + (10 * 3) + 12 + (15 * 2) + 6 + 7) / 10 = 9.9 = 10$ λεπτά. Το αποτέλεσμα αυτό είναι ικανοποιητικό και αναμενόμενο, αφού όλοι οι συμμετέχοντες δεν είχαν χρησιμοποιήσει ξανά το εργαλείο. Σε μεταγενέστερες δηλώσεις πολιτικών όπου θα υπάρχει εξοικείωση, ο χρόνος διάρκειας θα είναι μικρότερος.

5. Did you make any errors during the task?

10 απαντήσεις



Τέλος, η πιο πάνω παράσταση υποδεικνύει ότι η λειτουργία διαγραφής ενός στοιχείου, με το διπλό πάτημα πάνω του, είναι αναγκαία. Οι χρήστες δηλαδή μπορούν να διαγράψουν οποιοδήποτε στοιχείο πάνω στον καμβά τους εάν γίνει κάποιο λάθος (πχ: στην είσοδο ονόματος της οντότητας). Η λειτουργία αυτή μπορεί να χαρακτηριστεί αναγκαία, αφού το 50% των συμμετεχόντων την χρησιμοποίησε.

Συμπερασματικά, τα αποτελέσματα από την έρευνα θεωρούνται θετικά και αναμενόμενα, αφού είναι λογικό ένα 10% απόκλισης στην επιτυχία ολοκλήρωσης του έργου. Το γεγονός αυτό, δίνει περιθώρια βελτίωσης σχετικά με τις οδηγίες που δίνονται στους χρήστες του εργαλείου για την δημιουργία της πολιτικής τους. Θα μπορούσε ένα πιο επεξηγηματικό βίντεο να παρουσιάζεται στους χρήστες σε μία καινούρια σελίδα αποκλειστικά για παροχή βοήθειας.

Κεφάλαιο 7

Συμπεράσματα

7.1 Συμπεράσματα	62
7.2 Μελλοντική Δουλειά	62

7.1 Συμπεράσματα

Η διπλωματική αυτή είχε ως σκοπό την δημιουργία ενός εργαλείου το οποίο βοηθά τους μηχανικούς λογισμικού να δηλώσουν με ένα γραφικό τρόπο τις πολιτικές ιδιωτικότητας του υπο-ανάπτυξη συστήματός τους. Παρέχει επίσης την δυνατότητα μετάφρασης της δήλωσης αυτής σε τυπική γλώσσα, η οποία μπορεί με μαθηματικό τρόπο να εγγυηθεί την επαλήθευση μίας ιδιότητας.

Μετά την εκπόνηση αυτής της έρευνας, υπογραμμίζεται η σημαντικότητα της ανάγκης δήλωσης πολιτικών ιδιωτικότητας στις αρχικές φάσεις σχεδίασης ενός συστήματος. Σε συνδυασμό με το εργαλείο `privacyDef` μπορούν να αποφευχθούν λάθη τα οποία υπό άλλες συνθήκες θα ήταν αναπόφευκτα. Τέτοια λάθη μπορεί να είναι : επαναληπτικές αλλαγές στις διαδικασίες υλοποίησης ενός συστήματος λόγω έλλειψης βασικών εννοιών ιδιωτικότητας, ασάφειες στις δηλώσεις πολιτικών με φυσική γλώσσα και άλλα.

Λόγω του ότι το εργαλείο ακολουθεί αρχές απλού σχεδιασμού και απλής αρχιτεκτονικής, δεν είναι δύσκολο στην κατανόηση και αυτό το καθιστά εύχρηστο. Ταυτόχρονα παρέχει και οδηγίες χρήσης βοηθητικές για κάθε περίπτωση.

7.2 Μελλοντική Δουλειά

Το εργαλείο που έχει δημιουργηθεί για την διπλωματική αυτή είναι πλήρως λειτουργικό και ελεγχμένο. Πάντοτε όμως υπάρχει περιθώριο βελτίωσης, με την προσθήκη περισσότερων λειτουργιών. Μέσω της έρευνας αξιολόγησης του εργαλείου, διαφαίνεται ότι θα ήταν πιο βοηθητικό εάν υπήρχε μία πιο ξεκάθαρη δομή που να επιβάλλει την δημιουργία δεντρικών δηλώσεων και να αποκλείει την δημιουργία γράφων. Επιπλέον, μία ιδέα για βελτίωση της εμπειρίας του χρήστη είναι η καθοδήγησή του, κατά την διάρκεια της δημιουργίας μίας γραφικής δήλωσης. Να υλοποιηθούν δηλαδή, επιπρόσθετοι

περιορισμοί, που να καθοδηγούν την κάθε επόμενη κίνηση του χρήστη για αποτροπή λαθών. Τέλος, στο μέλλον θα μπορούσε να υλοποιηθεί η έννοια της επεξεργασίας ενός κόμβου.

Βιβλιογραφία

- [1] E. Vanezi, G. Zampa, C. Mettouris, A. Yeratziotis, and G. A. Papadopoulos, “Complicity: Evaluating the GDPR alignment of privacy policies - A study on web platforms,” SpringerLink, 01-Jan-1970. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-75018-3_10.
- [2] “DiálogoP - a language and a graphical tool for formally defining GDPR purposes,” springerprofessional.de. [Online]. Available: <https://www.springerprofessional.de/en/dialogop-a-language-and-a-graphical-tool-for-formally-defining-g/18116658>.
- [3] E. Vanezi, D. Kouzapas, G. M. Kapitsaki, T. Costi, A. Yeratziotis, C. Mettouris, A. Philippou, and G. A. Papadopoulos, “GDPR compliance in the design of the inform e-learning platform: A case study,” Home, 01-Jan-1970. [Online]. Available: <https://gnosis.library.ucy.ac.cy/handle/7/62371>.
- [4] “Methods and tools for GDPR compliance through privacy and Data Protection Engineering,” IEEE Xplore. [Online]. Available: <https://ieeexplore.ieee.org/document/8406568>.
- [5] M. J. U. of Calgary, M. Jafari, U. of Calgary, Philip W.L. Fong University of Calgary, P. W. L. Fong, R. S.-N. U. of Calgary, R. Safavi-Naini, K. B. U. of Calgary, K. Barker, Nicholas Paul Sheppard Queensland University of Technology, N. P. Sheppard, Q. U. of Technology, University of Texas at San Antonio, P. University, and O. M. V. A. Metrics, “Towards defining semantic foundations for purpose-based privacy policies: Proceedings of the first ACM conference on data and Application Security and privacy,” ACM Conferences, 01-Feb-2011. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1943513.1943541?casa_token=JZHbIvVdGXEEAA%3AKk5JjReQwxYH0WJg0rgSpk3A5YfqZKQziahmtam7IGcxtavSz78mEPTSQ9Z7SNboPynN9RxbKMe-9Q.
- [6] “What is front-end development?,” *The Guardian*, 28-Sep-2009. [Online]. Available: <https://www.theguardian.com/help/insideguardian/2009/sep/28/blogpost>.

- [7] R. Cousot and M. Martel, Static Analysis: 17th International Symposium, SAS 2010, Perpignan, France, September 14-16, 2010: Proceedings. Berlin: Springer, 2010.
- [8] *HTML 5*. [Online]. Available: <https://www.w3.org/TR/2008/WD-html5-20080122/>.
- [9] <https://www.techopedia.com/definition/28243/cascading-style-sheets-level-3-css3>
- [10] “Τι είναι το WordPress & πώς γίνεται η διαχείριση eshop: Keme seminars,” *KEME*, 07-Apr-2022. [Online]. Available: <https://www.keme.com.gr/wordpress-diaxeirisi-eshop/>.
- [11] V. Thapliyal, *Difference between frontend and backend MVC - Joomla!tuts*. [Online]. Available: <https://web.archive.org/web/20161230230237/http://joomlatuts.net/joomla-2-5/87-how-backend-model-view-controller-mvc-works-in-joomla/98-difference-between-frontend-and-backend-mvc>.
- [12] “What is php?,” *php*. [Online]. Available: <https://www.php.net/manual/en/intro-what-is.php>.
- [13] number8, “Kanban versus Scrum in agile methodology: Blog,” number8, 03-May-2022. [Online]. Available: <https://number8.com/kanban-versus-scrum/>.
- [14] I. Sommerville, *Software engineering*. Singapore: Pearson Education South Asia Pte Ltd, 2016.
- [15] A. Dix, J. Finlay, G. D. Abowd, and .. [et al.], *Human-Computer Interaction*. Harlow: Pearson Education, 2004.

Παράρτημα Α

Σε αυτό το παράρτημα παρουσιάζονται όλες οι λεπτομέρειες σχετικά με την έρευνα που εξάχθηκε για την διερεύνηση και καταγραφή απαιτήσεων και αναγκών του χρήστη.

What this survey is about

Dear participant,

privacy in software is now mandatory due to the new General Data Protection Regulation (GDPR). The GDPR enforces rights and provisions for protecting users' personal data. A very important point is that systems should function according to their privacy policies, meaning that the data collection and processing should be done exactly as described in the respective privacy policy.

Example:

-
- Privacy Policy: "We will only use your phone number in order to inform you when the product you want is back in stock."
 - In order for the system to be compliant with its privacy policy, the phone number should only be used to inform the user when the product they want is back in stock.

In the context of my bachelor's thesis, I will be designing and developing an easy-to-use graphical tool to be used by software developers. The tool will allow the user to define privacy policies in a graphical, diagram-based, intuitive way, and will then automatically translate the policy to the respective formal language definition, that can be used for formal verification of compliance. The translation will not require any interaction with the user.

The main target group of this survey, are software developers.

* Απαιτείται

Privacy Policy-compliant software systems

Regulation defines that privacy should be considered from the early stages of the software engineering process, i.e., since designing the system.

It is evident, that software developers' should from now on build Privacy Policy-compliant software systems.

This includes two main steps:

1. Defining the system's privacy policy;
2. Check the software to verify if it functions according to the policy.

Validation in Software Engineering - "Formal Methods"

In software engineering, validation is being done by using auditing, exhaustive testing, automated script execution and other methods that are not strict enough to verify systems' property satisfaction, i.e., they cannot guarantee a specific condition, including privacy policy compliance.

In computer science "Formal methods" are mathematical approaches including languages and tools, used for the rigorous specification and modelling of systems, and verification of specific properties. For instance, they could ensure that a system is compliant with its privacy policy, handling personal data as it should.

Example:

- According to the GDPR every user has the "Right to Erasure", i.e., the user is able to ask to delete their personal data from the system whenever they want, and the data will be deleted without any undue delay.
- Formal Methods can confirm that this rule is being strictly considered and therefore put into practice by the system.

In order to achieve formal verification of privacy policies, one needs to define their privacy policy in a formal rigorous way.

However, software engineers are not familiar with formal methods.

Consent Form

Thank you for considering participating in this survey for collecting the requirements of the project explained on the previous section.

Informed Consent Form:
This survey does not have any commercial purposes; the involved researchers do not have any monetary benefits by conducting it, and the results will be published in the form of reports and research papers based on the survey. We ask you to provide only anonymous data in this survey. All information will be safeguarded subject to any legal requirements.

This research will involve you completing a number of questions. The whole procedure is estimated to take about 10 minutes.

By responding to this questionnaire, you confirm the following:

- You have read and understood the purpose of the survey.
- You understand that taking part is voluntary. You can withdraw from the study at any time during the survey, and do not have to give any reasons for why you no longer want to take part.
- You agree that the answers you would give will be stored in digital form. Only the involved researchers will have access to this information, and this information will not be distributed to any other person or entity.

By completing this survey, you are consenting to participate in this study voluntarily. You are indicating that you have read the research description and that you agree to the terms as described

If you have any comments or questions, please contact the persons responsible:

- Ioanna Theophilou, University of Cyprus, Cyprus (itheop02@ucy.ac.cy)
- Evangelia Vanezi, University of Cyprus, Cyprus (vanezievangelia@gmail.com)

CONSENT *

Να επισημαίνεται μόνο μία έλλειψη.

- ☐ Yes Παράβλεψη και μετάβαση στην ερώτηση 2
- ☐ No

Biographical Data

1. Age Range *

Να επισημαίνεται μόνο μία έλλειψη.

- ☐ 18-25
☐ 26-40
☐ 41-50
☐ 60+

2. Gender *

Να επισημαίνεται μόνο μία έλλειψη.

- ☐ Male
☐ Female
☐ Other

3. Country: *

4. Are you a software developer? *

Να επισημαίνεται μόνο μία έλλειψη.

- ☐ Yes
☐ No
☐ Άλλο: _____

5. If yes, how many years of experience do you have as a software developer?

Να επισημαίνεται μόνο μία έλλειψη.

- ☐ 0-2
☐ 2-5
☐ 5-10
☐ more than 10
☐ I am studying to become a software developer

6. How would you rate your overall experience with modeling tools?(e.g. Modelio)

*

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Poor	☐	☐	☐	☐	☐	Excellent

7. How would you rate your overall experience with UML ? *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Poor	☐	☐	☐	☐	☐	Excellent

Privacy in General

8. I am well aware of the software engineering process stages. *

Να επισημαίνεται μόνο μία έλλειψη.

☐ Yes
☐ No

9. Do you think Privacy is important? *

Να επισημαίνεται μόνο μία έλλειψη.

☐ Yes
☐ No

10. Are you familiar with Privacy in general *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Not at all	☐	☐	☐	☐	☐	Very familiar

11. How familiar are you with Privacy Policies? *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Not at all	☐	☐	☐	☐	☐	Very Familiar

12. Are you familiar with the General Data Protection Regulation? (GDPR) *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Not at all	☐	☐	☐	☐	☐	Very familiar

about it)

14. How much time do you devote on defining the Privacy Policy when designing a system? *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
None (haven't thought about it)	☐	☐	☐	☐	☐	Much (I constantly think about it)

15. How often do the following happen to you? (Software Development - wise) *

Να επισημαίνεται μόνο μία έλλειψη ανά σειρά.

	Never	Rarely	Sometimes	Often	Always
Developed a system with no privacy consideration at all	☐	☐	☐	☐	☐
Had to make minor design changes after considering privacy regulations	☐	☐	☐	☐	☐
Had to make major design changes after considering privacy regulations	☐	☐	☐	☐	☐
Had to make minor implementation changes after considering privacy regulations	☐	☐	☐	☐	☐
Had to make major implementation changes after considering privacy regulations	☐	☐	☐	☐	☐

16. How important do you consider is to define the Privacy Policy of a system in the early stages of the software engineering process? *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Not at all	☐	☐	☐	☐	☐	Critical

17. Do you have a good knowledge of the users' rights regarding Privacy in software systems? *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Not good	☐	☐	☐	☐	☐	Very good

Formal Methods in General

As explained at the beginning, in software Engineering validation is being done by using auditing, exhaustive testing, automated script execution and other methods that are not strict enough to verify systems' property satisfaction, i.e., they cannot quarantine a specific condition, including privacy policy compliance.

In computer science "Formal methods" are mathematical approaches including languages and tools, used for the rigorous specification and modelling of systems, and verification of specific properties. For instance, they could ensure that a system is compliant with its privacy policy, handling personal data as it should.

18. How familiar are you with Formal Methods? *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5
Not much	☐	☐	☐	☐	☐
Very much					

19. Do you use Formal Methods during the modelling phase of your systems? *

Να επισημαίνεται μόνο μία έλλειψη ανά σειρά.

	Never	Rarely	Sometimes	Often	Always
Answer:	☐	☐	☐	☐	☐

20. Do you use Formal Methods to validate/test your systems? *

Να επισημαίνεται μόνο μία έλλειψη ανά σειρά.

	Never	Rarely	Sometimes	Often	Always
Answer:	☐	☐	☐	☐	☐

21. Having in mind that Formal Methods can help you guarantee privacy in your software system, would you use them, if there was an easy way for that? *

Να επισημαίνεται μόνο μία έλλειψη.

☐ Yes

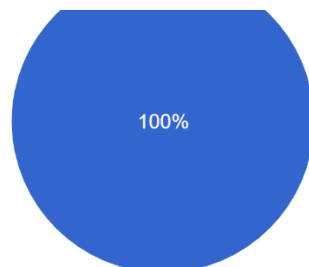
☐ No

22. If there was a graphical tool where you could define a privacy policy in an easy-to-use diagram-based way (e.g. UML-like), that would then automatically (no interaction needed by you) transform that policy into a formal method definition towards validating privacy compliance, would you use it during the system design stage? *

Να επισημαίνεται μόνο μία έλλειψη.

☐ Yes

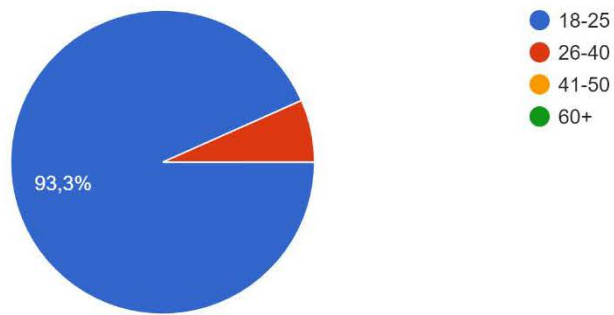
☐ No



NO

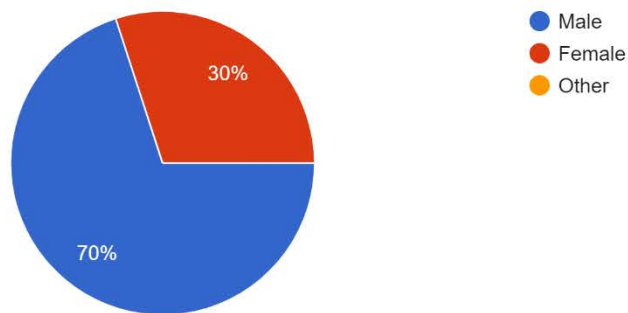
1. Age Range

30 απαντήσεις



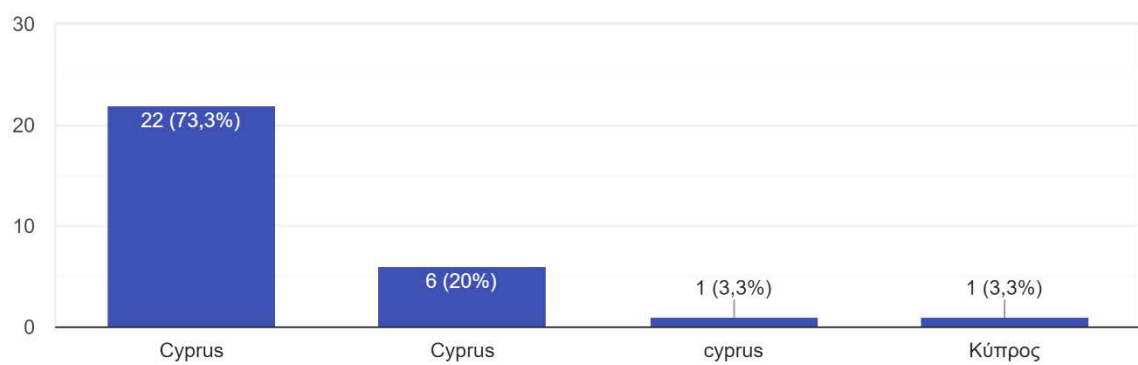
2. Gender

30 απαντήσεις



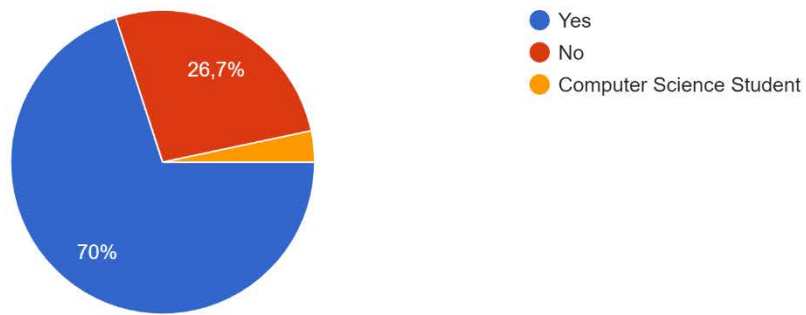
3. Country:

30 απαντήσεις



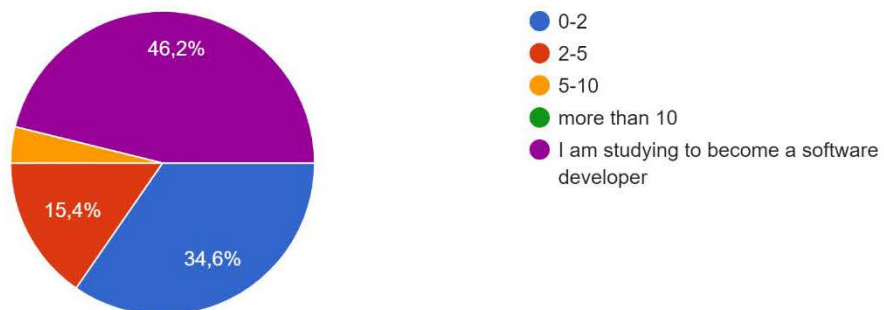
4. Are you a software developer?

30 απαντήσεις



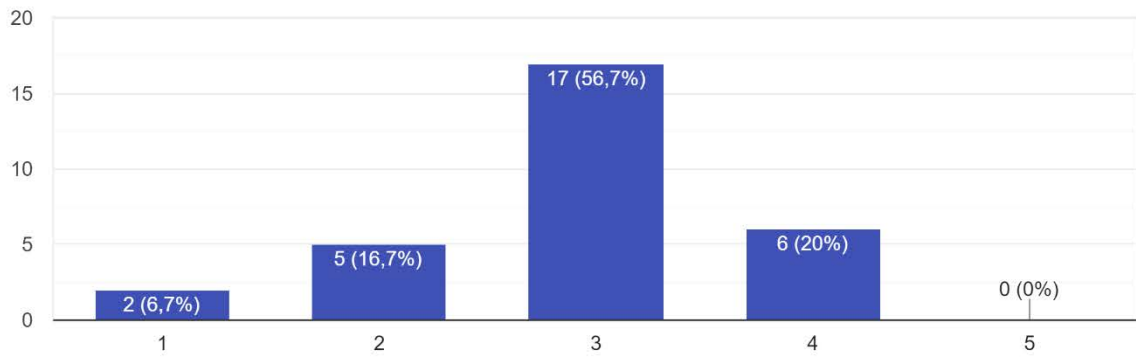
5. If yes, how many years of experience do you have as a software developer?

26 απαντήσεις



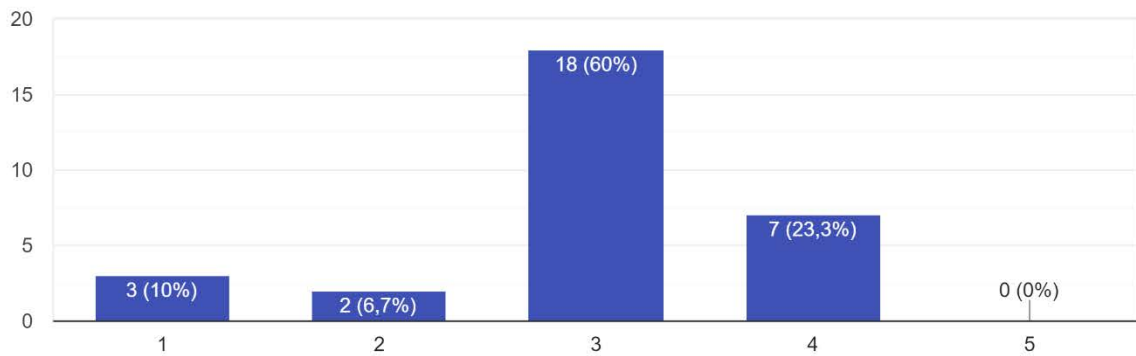
6. How would you rate your overall experience with modeling tools?(e.g. Modelio)

30 απαντήσεις



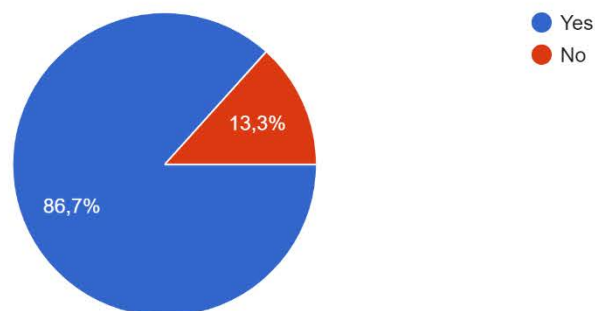
7. How would you rate your overall experience with UML ?

30 απαντήσεις



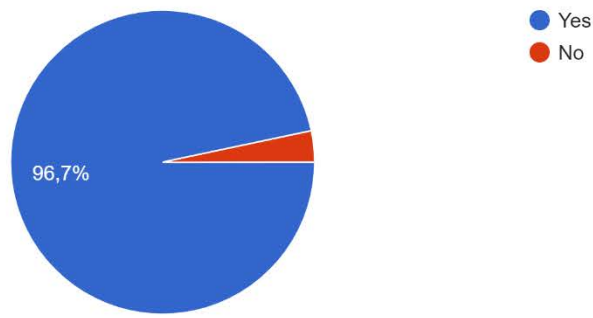
8. I am well aware of the software engineering process stages.

30 απαντήσεις



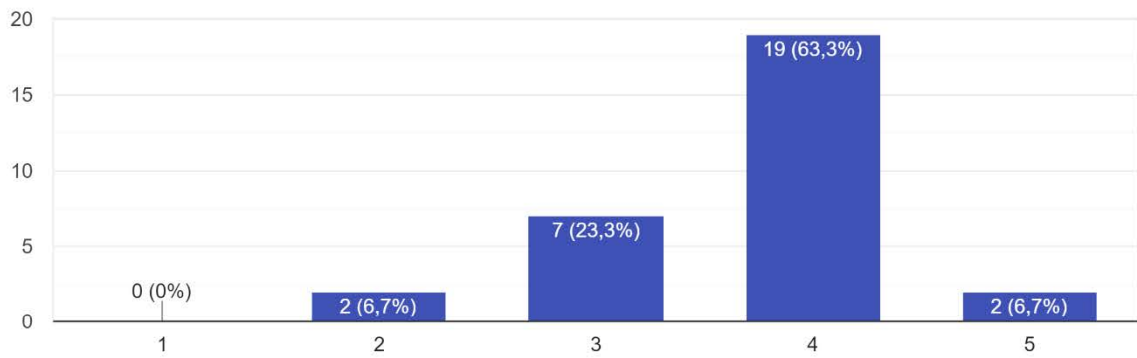
9. Do you think Privacy is important?

30 απαντήσεις



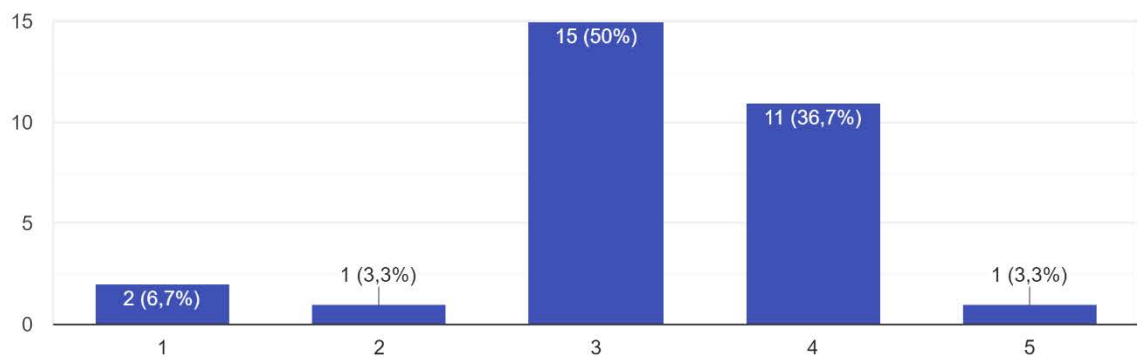
10. Are you familiar with Privacy in general

30 απαντήσεις



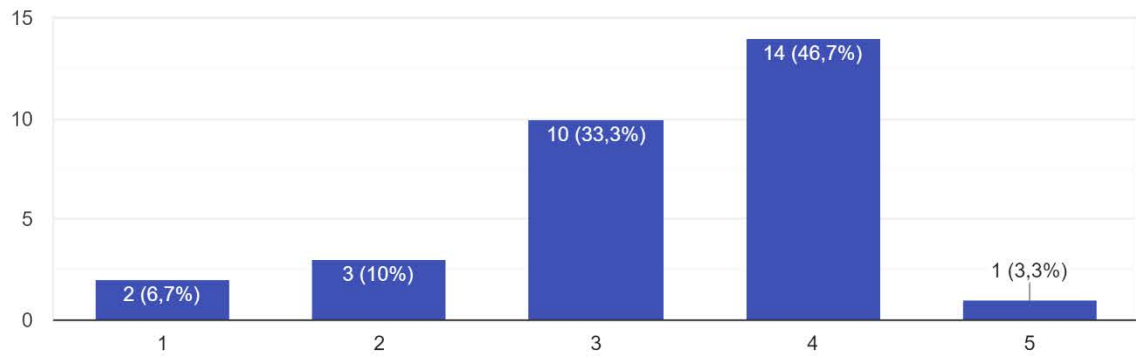
11. How familiar are you with Privacy Policies?

30 απαντήσεις



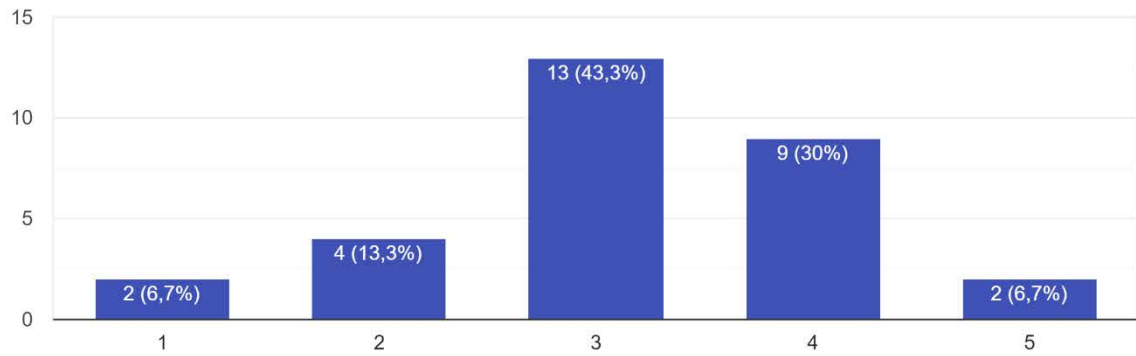
12. Are you familiar with the General Data Protection Regulation? (GDPR)

30 απαντήσεις



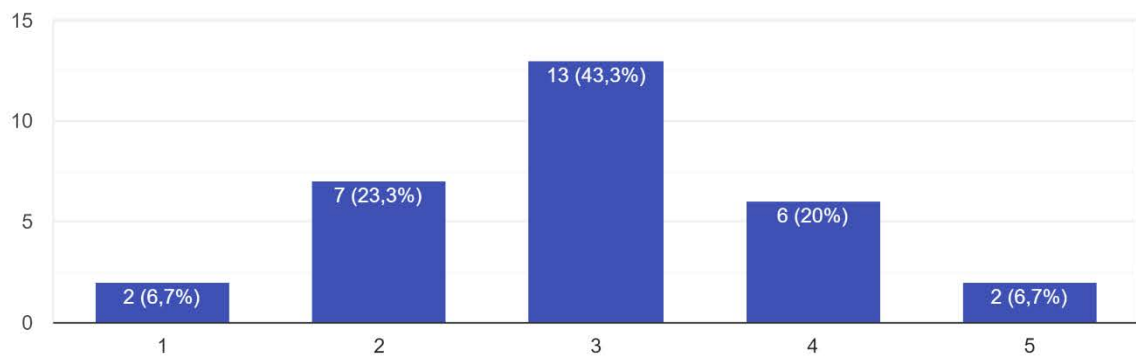
13. How much time do you devote on applying Privacy when designing a system?

30 απαντήσεις

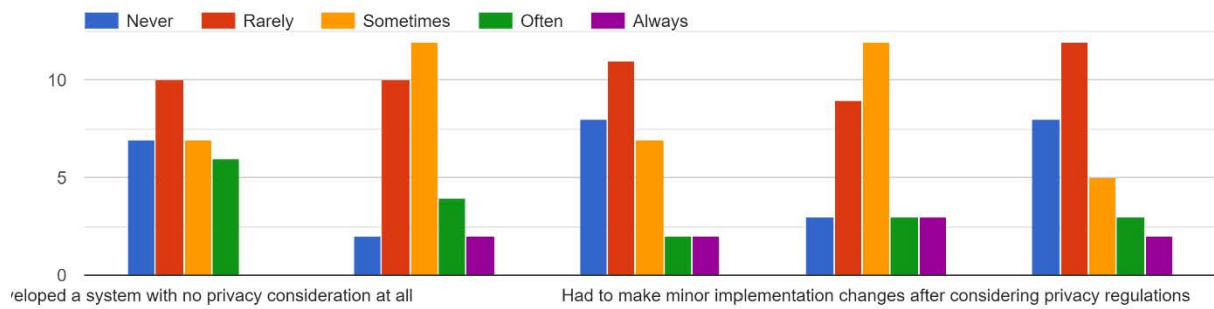


14. How much time do you devote on defining the Privacy Policy when designing a system?

30 απαντήσεις

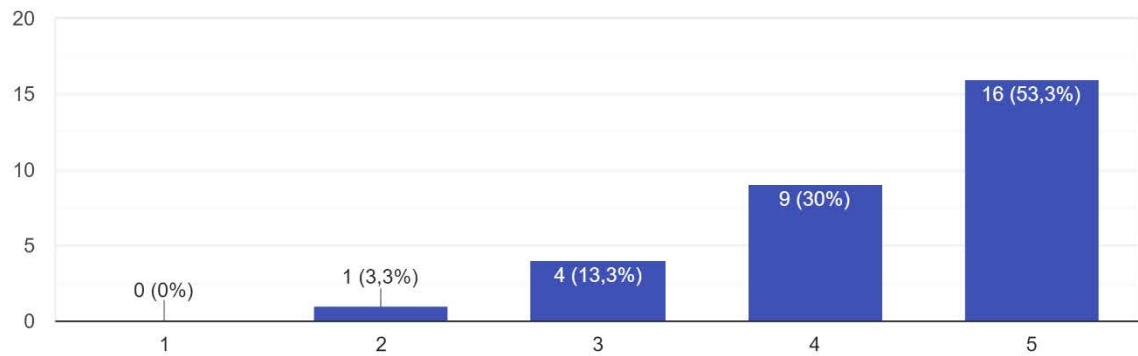


15. How often do the following happen to you? (Software Development - wise)



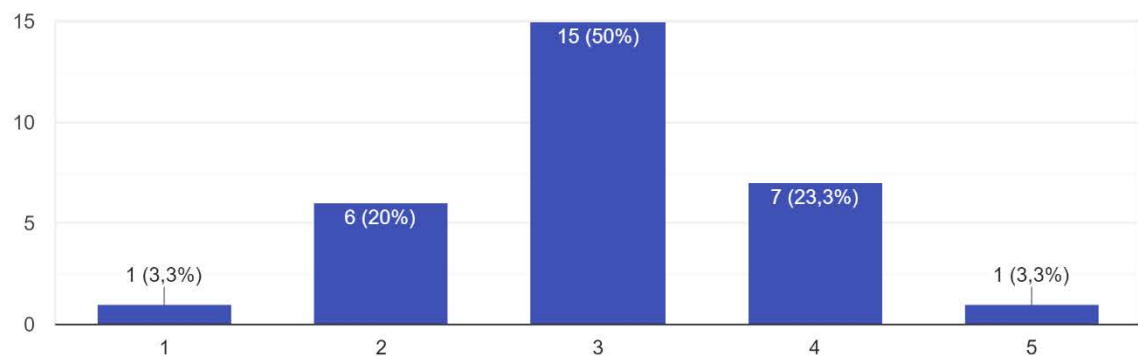
16. How important do you consider is to define the Privacy Policy of a system in the early stages of the software engineering process?

30 απαντήσεις



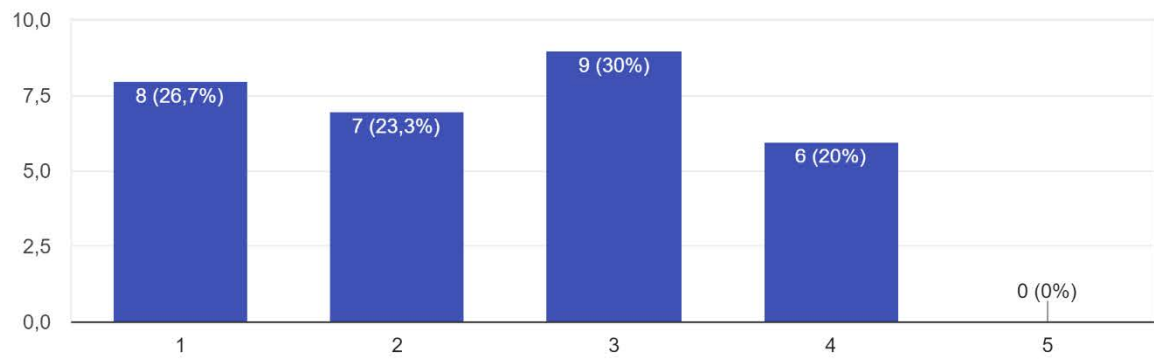
17. Do you have a good knowledge of the users' rights regarding Privacy in software systems?

30 απαντήσεις



18. How familiar are you with Formal Methods?

30 απαντήσεις



19. Do you use Formal Methods during the modelling phase of your systems?

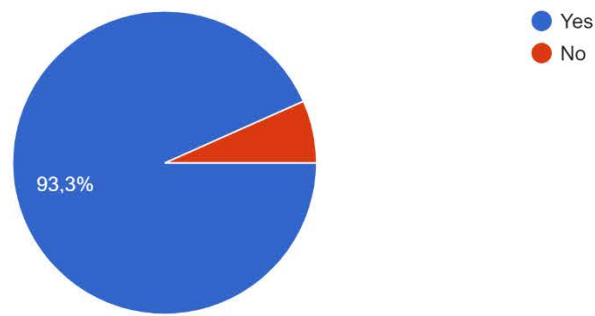


20. Do you use Formal Methods to validate/test your systems?



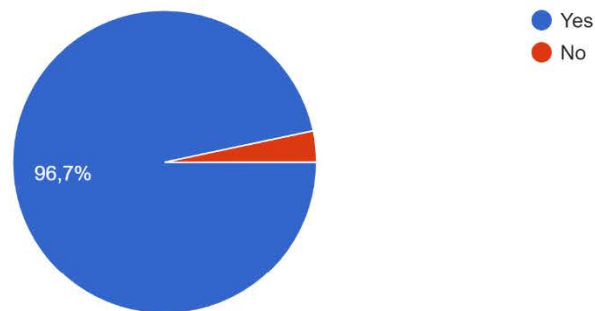
21. Having in mind that Formal Methods can help you guarantee privacy in your software system, would you use them, if there was an easy way for that?

30 απαντήσεις



22. If there was a graphical tool where you could define a privacy policy in an easy-to-use diagram-based way (e.g. UML-like), that would th...ould you use it during the system design stage?

30 απαντήσεις



Παράρτημα Β

Σε αυτό το παράρτημα παρουσιάζεται ολόκληρος ο κώδικας αναφορικά με την μετατροπή της γραφικής δήλωσης μίας πολιτικής σε Τυπική Γλώσσα.

```
function formalMethod() {
  var check = targets.length / 2;
  console.log("count so far: " + connectors.length);
  console.log("targ. so far: " + targets.length);
  if (connectors.length !== targets.length - 1) {
    alert("This is not a valid diagram. Please check the instructions below.
    Make sure that all elements are connected");
    return;
  }

  var json = stage.toJSON();
  var undefined;
  const obj = JSON.parse(json);
  const array = obj["children"][0]["children"];

  const TargetTypes = ["start", "end", "entity", "decision", "data"];
  const ConnectionTypes = ["continue", "send", "receive", "evaluate", "true",
  "false"];

  var false_flag=0;

  array.forEach((i) => {
    var flag = checkDouble(i["attrs"]["id"]);

    Checked.push(i["attrs"]["id"]);
    console.log(flag);
    if (flag && i["attrs"]["id"].charAt(0) === "t") {
      if (i["children"][1]["attrs"]["text"] === "\n\nSTART") {
        Targs.push({ id: i["attrs"]["id"], text: "Session =", type:
        TargetTypes[0] });
      }
      else if (i["children"][1]["attrs"]["text"] === "\n\nEND") {
        Targs.push({ id: i["attrs"]["id"], text: "END", type: TargetTypes[1]
        });
      }
      false_flag=1;
    }
    else if (i["children"][1]["attrs"]["text"].charAt(0) === "E") {
      Targs.push({ id: i["attrs"]["id"], text:
      i["children"][1]["attrs"]["text"], type: TargetTypes[2] });
    }
    else if (i["children"][0]["className"] === "RegularPolygon") {
      Targs.push({ id: i["attrs"]["id"], text:
      i["children"][1]["attrs"]["text"], type: TargetTypes[3] });
    }
    else if (i["children"][1]["attrs"]["text"].charAt(0) === "D") {
```

```

        Targs.push({ id: i["attrs"]["id"], text:
i["children"][1]["attrs"]["text"], type: TargetTypes[4] });
    }
}
    else if (flag && i["attrs"]["id"].charAt(0) === "c") {
        if (i["className"] === "Line" && i["attrs"]["dash"] === undefined &&
i["attrs"]["fill"] === "black" && i["attrs"]["stroke"] === "black") {
            Conns.push({ id: i["attrs"]["id"], from: i["attrs"]["name"][0], to:
i["attrs"]["name"][1], type: ConnectionTypes[0] });
        }
        else if (i["className"] === "Arrow" && i["attrs"]["dash"] !== undefined
&& i["attrs"]["fill"] === "black" && i["attrs"]["stroke"] === "black") {
            Conns.push({ id: i["attrs"]["id"], from: i["attrs"]["name"][0], to:
i["attrs"]["name"][1], type: ConnectionTypes[1] });
        }
        else if (i["className"] === "Arrow" && i["attrs"]["dash"] === undefined
&& i["attrs"]["fill"] === "black" && i["attrs"]["stroke"] === "black") {
            Conns.push({ id: i["attrs"]["id"], from: i["attrs"]["name"][0], to:
i["attrs"]["name"][1], type: ConnectionTypes[2] });
        }
        else if (i["className"] === "Line" && i["attrs"]["dash"] !== undefined
&& i["attrs"]["fill"] === "black" && i["attrs"]["stroke"] === "black") {
            Conns.push({ id: i["attrs"]["id"], from: i["attrs"]["name"][0], to:
i["attrs"]["name"][1], type: ConnectionTypes[3] });
        }
        else if (i["className"] === "Arrow" && i["attrs"]["dash"] !== undefined
&& i["attrs"]["fill"] === "green" && i["attrs"]["stroke"] === "green") {
            Conns.push({ id: i["attrs"]["id"], from: i["attrs"]["name"][0], to:
i["attrs"]["name"][1], type: ConnectionTypes[4] });
        }
        else if (i["className"] === "Arrow" && i["attrs"]["dash"] !== undefined
&& i["attrs"]["fill"] === "blue" && i["attrs"]["stroke"] === "blue") {
            Conns.push({ id: i["attrs"]["id"], from: i["attrs"]["name"][0], to:
i["attrs"]["name"][1], type: ConnectionTypes[5] });
        }
    }
});

Targs.forEach((targ) => {
    console.log("TARGETET: \n" + targ.id + " " + targ.type);
});
console.log(array[0]["attrs"]["dash"]);
Conns.forEach((cons) => {
    console.log("CONNECTOR: \n" + cons.id + " " + cons.type);
});

console.log(array);

const output = [];
Conns.forEach((c) => {

```

```

    if (c.type === ConnectionTypes[0] && findTarget(""+c.to).type ===
TargetTypes[1]) {//continue
        output.push("." + findTarget(""+c.to).text);
    }
    else if (c.type === ConnectionTypes[0] && findTarget(""+c.to).type !==
TargetTypes[1]) {//continue
        output.push(findTarget(""+c.from).text+"." + findTarget(""+c.to).text);
    }
    else if (c.type === ConnectionTypes[1]) {//send
        output.push(findTarget("" + c.from).text + "->" +
findTarget(""+c.to).text);
    }
    else if (c.type === ConnectionTypes[2]) {//receive
        output.push( findTarget("" + c.from).text +
":."+findTarget(""+c.to).text);
    }
    else if (c.type === ConnectionTypes[3]) {//evaluate
        output.push("." + "(" + findTarget(""+c.to).text + ")");
    }
    else if (c.type === ConnectionTypes[4]) {//true
        output.push("{true >>}");//findTarget("" + c.to).text
    }
    else if (c.type === ConnectionTypes[5]) {//false
        output.push(",false >> "); //+ findTarget("" + c.to).text
    }
});
console.log("-----")
output.forEach((c) => {
    console.log(c);
});

```

// any kind of extension (.txt,.cpp,.cs,.bat)

```
var filename = "FormalTranslation.txt";
```

```
var str="";
```

```
var prin="b";
```

```
var meta="a";
```

```
var prinR="b";
```

```
var metaR="a";
```

```
output.forEach((out)=>{
```

```
    if(out.charAt(0)==="S"){
```

```
        str+="Session = ";
```

```
    }
```

```
    else if(out.search("->") !==-1 && out.search(meta +"->") ===-1 ){
```

```
        prin = out.split("->")[0];
```

```
        meta = out.split("->")[1];
```

```
        str += prin + "->";
```

```
    }
```

```
    else if(out.search(meta+"->") !==-1){
```

```

    var piometa = out.split("<->")[1];
    str+= piometa+":<" +meta + ">";
}
else if(out.search("::") !==-1 && out.search(metaR + "::") ===-1 ){
    prinR = out.split("::")[0];
    metaR = out.split("::")[1];
    //str +=  + "<->";
}
else if(out.search(metaR+"::") !==-1){
    var piometaR = out.split("::")[1];
    str+= piometaR+ "<->"+prinR+":<" +metaR + ">";
}
else if(out.search(".") !==-1){
    str+=out;
}
else if(out.search("{") !==-1){
    str+=out;
}
else if(out.search(",f") !==-1){
    false_flag=1;
    str+=out;
}

});
str = str.replace('D}', 'D');

alert("Formal Translation will be downloaded");
downloadFile(filename,str);
}

```

Παράρτημα Γ

Σε αυτό το παράρτημα παρουσιάζεται η έρευνα αξιολόγησης του εργαλείου privacyDef.

PrivacyDef Tool Evaluation

Dear participant,

privacy in software is now mandatory due to the new General Data Protection Regulation (GDPR). The GDPR enforces rights and provisions for protecting users' personal data. A very important point is that systems should function according to their privacy policies, meaning that the data collection and processing should be done exactly as described in the respective privacy policy.

Example:

-
- Privacy Policy: "We will only use your phone number in order to inform you when the product you want is back in stock."
 - In order for the system to be compliant with its privacy policy, the phone number should only be used to inform the user when the product they want is back in stock.

In the context of my bachelor's thesis, I designed and developed an easy-to-use graphical tool to be used by software developers. The tool allows the user to define privacy policies in a graphical, diagram-based, intuitive way, and will then automatically translate the policy to the respective formal language definition, that can be used for formal verification of compliance. The translation will not require any interaction with the user.

The main target group of this survey, are software developers.

Consent Form

Thank you for considering participating in this survey for collecting the requirements of the project explained on the previous section.

Informed Consent Form:

This survey does not have any commercial purposes; the involved researchers do not have any monetary benefits by conducting it, and the results will be published in the form of reports and research papers based on the survey. We ask you to provide only anonymous data in this survey. All information will be safeguarded subject to any legal requirements.

This research will involve you completing a number of questions. The whole procedure is estimated to take about 10 minutes.

By responding to this questionnaire, you confirm the following:

- You have read and understood the purpose of the survey.
- You understand that taking part is voluntary. You can withdraw from the study at any time during the survey, and do not have to give any reasons for why you no longer want to take part.
- You agree that the answers you would give will be stored in digital form. Only the involved researchers will have access to this information, and this information will not be distributed to any other person or entity.

By completing this survey, you are consenting to participate in this study voluntarily. You are indicating that you have read the research description and that you agree to the terms as described.

If you have any comments or questions, please contact the persons responsible:

- Ioanna Theophilou, University of Cyprus, Cyprus (itheop02@ucy.ac.cy)
- Evangelia Vanezi, University of Cyprus, Cyprus (vanezievangelia@gmail.com)

Consent *

☐ Yes

☐ No

Πίσω

Επόμενο

Εκκαθάριση φόρμας

Task scenario:

You want to define your system privacy policy in a formal mathematics based policy language. However you are not familiar with the language and that would be very difficult for you, having also the risk of many mistakes.

You have been informed that PrivacyDef is a tool, that allows you to visually define policies, and then automatically translate them into the formal language, so you have decided to try it.

Visit the tool, and try to define the following privacy policy:

Website : thesis.in.cs.ucy.ac.cy/privacyDef/

(Connect to the VPN beforehand)

" Mental Health System "

You belong in the development team of the Mental health system which is used only by Doctors and Medical Security staff. This rule applies : "A doctor can state the death of a patient and the death is recognized by the system only when accepted by the Medical Security staff."

You want to make sure that the request is correctly received by the Medical Security staff.

Define the following privacy policy:

"The system will collect a request from a doctor containing the patient's identity, and this info will be saved in the database. The request can only be the statement of this patient's death. When this information is available in the database, then the Medical Security Staff can have access to this information, and send an "accept" message with the patient's identity to the database."

Instructions:

- Please watch first the demo video you were given
- Please remember to time yourself while defining the policy.

1. State the following: Have you seen the instruction's video? *

☐ yes

☐ No

2. Have you successfully completed the task? *

☐ Yes

☐ No

3. How long did it take to complete the task ? (in minutes) *

Η απάντησή σας

4. Please export your policy as an image and send it to the following email :
itheop02@ucy.ac.cy . State bellow if you sent it. *

☐ Yes

☐ No

5. Did you make any errors during the task? *

☐ Yes

☐ No

6. Please state any comments you would like to add about your experience with the tool.

Η απάντησή σας

[Πίσω](#)

[Υποβολή](#)

[Εκκαθάριση φόρμας](#)

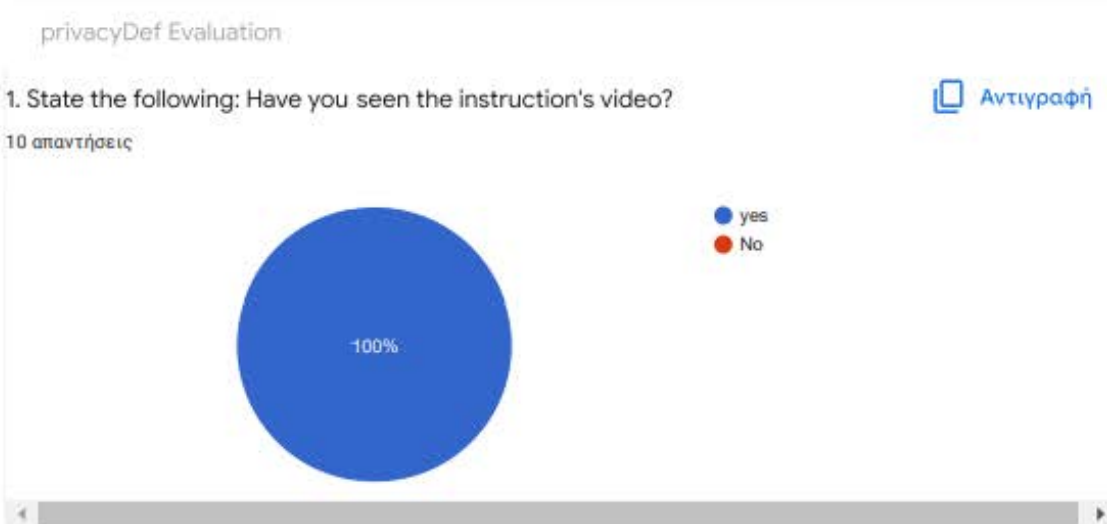
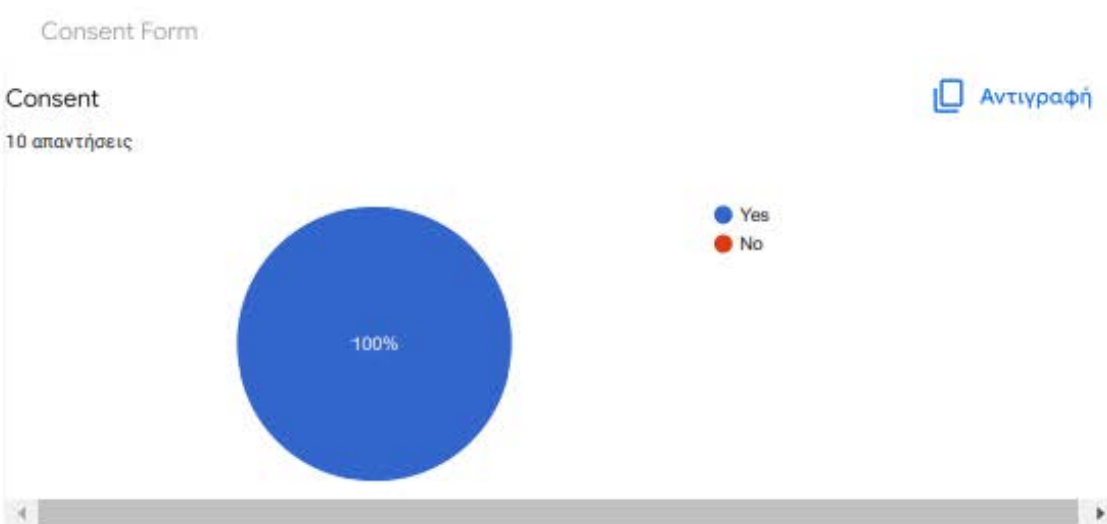
10 απαντήσεις

Αποδοχή απαντήσεων

Σύνοψη

Ερώτηση

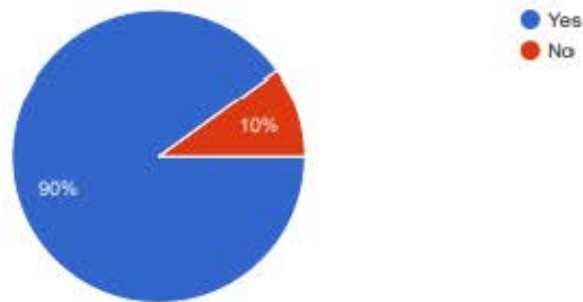
Ατομική



2. Have you successfully completed the task?

Αντιγραφή

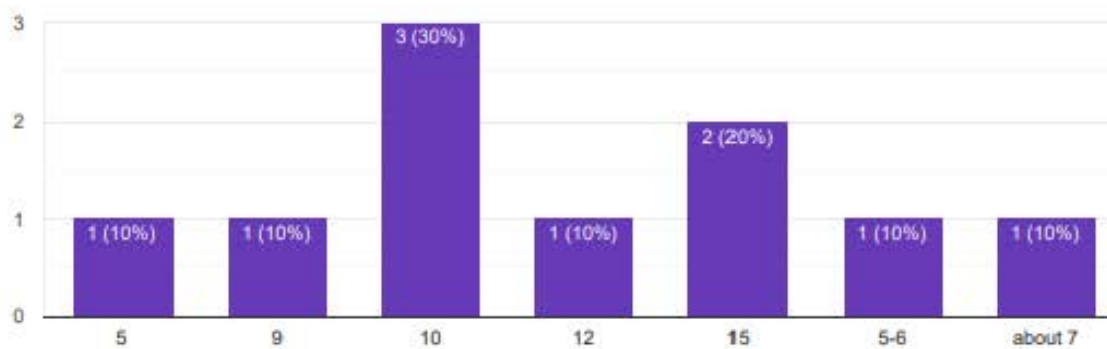
10 απαντήσεις



3. How long did it take to complete the task ? (in minutes)

Αντιγραφή

10 απαντήσεις



4. Please export your policy as an image and send it to the following email : itheop02@ucy.ac.cy . State bellow if you sent it.

Αντιγραφή

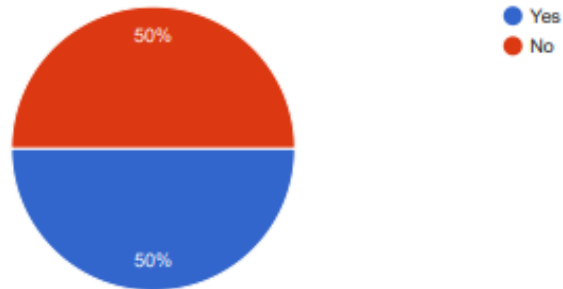
10 απαντήσεις



5. Did you make any errors during the task?

 Αντιγραφή

10 απαντήσεις



6. Please state any comments you would like to add about your experience with the tool.

6 απαντήσεις

More clear instructions. Maybe a manual with images

Its simple and intuitive.

The user interface is pretty clean and straightforward.

Very good experience

Bit difficult to understand at first use! An undo option will be good as well! And the sections (pallet, canvas) should be larger and take the whole space

It should be clearer that a valid diagram requires a sequential thinking of a scenario.