

SUPPLEMENTARY MATERIAL TO THE PAPER "TOWARDS A GOAL-CENTRIC ASSESSMENT OF REQUIREMENTS ENGINEERING METHODS FOR PRIVACY BY DESIGN": OVERVIEW OF THE INTERVIEW RESULTS

ID	Method character.	Goals	Questions	Metrics
11	MC1: Legal knowledge	understand how data was classified (G1.1) understand kinds of processing applicable to data (G1.2)	How do the legal and the technical experts interact? (Q1.1)	ability to classify data (M1.1) clarity of data classification (M1.2) automation of data classification (M1.3)
	MC2: Traceability	version control and ownership (G1.3)	How information about specifications persists? (Q1.2) How does legal interpretation evolve? (Q1.3) Is legal documentation available? (Q1.4)	clarity of ownership in documentation (M1.4)
	MC3: Concerns' separat.	prioritizing compliance (G1.4) balancing need for agility and compliance (G1.5)	What is the need for processing the data? (Q1.5) Can goals be achieved without processing data? (Q1.6) Who is the stakeholder of data processing? (Q1.7) How long data will be used? (Q1.8)	compliance of internal data users (M1.5)
	MC4: Spec. transp.	clear mapping of GDPR sensitive data (G1.6) identifying the level of data sensitivity (G1.7) knowing data processing period (G1.8) identifying purposes of processing (G1.9)	Is it clear how data was classified? (Q1.10) Do stakeholders have access to the data classification? (Q1.11) Do stakeholders understand the data classification? (Q1.12)	proportion of classified data (M1.6) classification understandability (M1.7)
	MC5: Spec. flexibility.	identify components requiring flexibility (G1.10) establish review process with GDPR experts (G1.11)	Is GDPR implementation clearly documented? (Q1.13) Is there a change management process in place? (Q1.14)	portion of tagged system components (M1.8)
	Other goals	automation of compliance controls (G1.12) communication (G1.13)	How to hold on to GDPR compliance over time? (Q1.15) Can non-data specialists understand GDPR compliance? (Q1.16)	NA
12	MC1: Legal knowledge	clear mapping of legal norms on IT system (G2.1)	NA	how have we mapped all the requirements (M2.1)
	MC2: Traceability	"updateability"/modifiability of traceability (G2.2) consistency (G2.3) ease of implementation (G2.4)	NA NA NA	"proportion of compliant data sources/systems" (M2.2) NA NA
	MC3: Concerns' separat.	NA NA	NA NA	"tracking progress of implementation" (M2.3) progress of changes/updates (M2.4)
	MC4: Spec. transp.	documenting all the systems (G2.5) documenting types of data processed (G2.6)	Is all the data and data processing documented? (Q2.1) NA	percentage of data mapped (M2.5) NA
	MC5: Spec. flexibility.	NA	NA	time to implementing changes (M2.6)
	Other goals	identification of the data type (G2.7)	NA	data sensitivity (M2.7)
13	MC1: Legal knowledge	avoiding risks of non-compliance (G3.1)	NA	NA
	MC2: Traceability	optimal investment to manage non-compliance (G3.2)	Does your interpretation meet the financial risk? (Q3.1)	time and resources for traceability implementation (M3.1)
	MC3: Concerns' separat.	NA	NA	NA
	MC4: Spec. transp.	passing audit (G3.3) improving communication (G3.4)	Can you explain reasons for your design decisions? (Q3.2) NA NA	explainability of design decisions (M3.2) NA ratio of system changes to changes in regulations (M3.3)
	MC5: Spec. flexibility.	NA	NA	NA
14	MC1: Legal knowledge	understanding of design goals (G4.1) understanding the required design flexibility (G4.2)	NA NA	NA NA
	MC2: Traceability	implementation and change history (G4.3)	How compliance was implemented? (Q4.1) Why design was implemented in this way? (Q4.2)	time and resources for traceability implementation (M3.1)
	MC3: Concerns' separat.	merging compliance with business operations (G4.4)	How hard you put the bar of being compliant? (Q4.3)	NA
	MC4: Spec. transp.	privacy impact assessment (G4.5)	NA	NA
	MC5: Spec. flexibility.	effective implementation of changes (G4.6)	NA	speed for implementing change (M4.2) lines of code requiring refactoring to implement change (M4.3)
15	MC1: Legal knowledge	NA	NA	NA
	MC2: Traceability	making sure that software works correctly (G5.1)	Are we collecting data before users give permission? (Q5.1) Does Cookie banner satisfy GDPR requirements? (Q5.2) Does customer requested to provide consent? (Q5.3)	NA
	MC3: Concerns' separat.	NA	NA	NA
	MC4: Spec. transp.	effective communication on system compliance (G5.2) faster execution of business processes (G5.3)	NA	NA
	MC5: Spec. flexibility.	fast implementation of changes (G5.4) adaptability (G5.5)	Can we implement the changes in reasonable time? (Q5.4)	time (M5.1) difficulty of changes implementation (M5.2)
	Other goals	assuring web marketing needs (G5.6) assuring personal data protection (G5.7)	How can we collect data? (Q5.5) What data can we collect? (Q5.6)	NA

ID	Method character.	Goals	Questions	Metrics
16	MC1: Legal knowledge	balance business and compliance needs (G6.1) finding consensus (G6.2) bringing the required expertise together (G6.3) performing gap analysis when required (G6.4) team understands and can implement compliance (G6.5)	How to implement compliance? (Q6.1) How to map to technology? (Q6.2) What legal requirements are relevant? (Q6.3)	NA
	MC2: Traceability	executing governance (G6.6) having proofs for inspections and when issues arise (G6.7)	Why do you do it? (Q6.4) Have we done the best we were able to do? (Q6.5) Have we missed something? (Q6.6) Why did the gap in compliance emerge? (Q6.7) Is there a risk, do we know it and can we manage it? (Q6.8)	GDPR requirements - controls mapping (M6.1) number and severity of compliance gaps (M6.2)
	MC3: Concerns' separat.	NA	NA	NA
	MC4: Spec. transp.	compliance/system is implemented as expected (G6.8)	Have we missed anything? (Q6.9)	NA
	MC5: Spec. flexibility.	identification of components requiring updates (G6.9) identifying what new vulnerabilities are relevant (G6.10)	Is it relevant for the company? (Q6.10) Do we have blockers/technical debt? (Q6.11)	NA
	Other goals	prevent personal data breaches (G6.11) control IT infrastructure and its evolution (G6.12) have a correct interpretation (G6.13)	NA	amount of incidents (M6.3)
17	MC1: Legal knowledge	implementation of system according to requirements (G7.1) advising clients about GDPR compliance of solutions (G7.2)	Is solution or particular settings GDPR compliant? (Q7.1)	compliance functionality availabil. (M7.1)
	MC2: Traceability	optimization of compliance implementation process (G7.3)	NA	NA
	MC3: Concerns' separat.	identifying components requiring GDPR compliance (G7.4) not making things more complex (G7.5) avoid additional expenditures and limitations (G7.6)	Should we implement GDPR compliance controls? (Q7.2) Are we obliged to implement it? (Q7.3)	necessity to implement (M7.2)
	MC4: Spec. transp.	everything should be clear to responsible roles (G7.7) full understanding of requirements to each specific task (G7.8)	Can we achieve GDPR compliance for our system? (Q7.4) Have we done everything correctly? (Q7.5)	clarity to responsible (M7.3)
	MC5: Spec. flexibility.	NA	NA	NA
	Other goals	processing as much data as possible (G7.9) automation of external GDPR compliance checks (G7.10)	NA	NA
18	MC1: Legal knowledge	address GDPR as early as possible (G8.1) making GDPR requirements clear to roles involved (G8.2) higher quality of service (G8.3)	What kind of data is processed? (Q8.1) Does the customer work in a regulated industry? (Q8.2)	NA
	MC2: Traceability	guarantee that specifications comply with GDPR (G8.4)	How easy is it to use traceability to implement change? (Q8.3) How easy is it to trace requirements towards GDPR goal? (Q8.4) How easy is it to track system to GDPR goals? (Q8.5)	GDPR coverage (M8.1)
	MC3: Concerns' separat.	explicit identification of GDPR requirements (G8.5) logic and functionality separation (G8.6) audits facilitation (G8.7)	What mechanisms isolate compliance and business changes? (Q8.6)	number of compliance issues (M8.2) frequency of reviews (M8.3) degree of separation (M8.4) stakeholders' feedback (M8.5) ease of documentation review (M8.6)
	MC4: Spec. transp.	facilitating compliance reviews (G8.8) improvement of communication (G8.9) reducing risk of non-compliance (G8.10) balancing different requirements and limitations (G8.11) resolving conflicts between requirements (G8.12) common understanding between stakeholders (G8.13)	How GDPR compliance is achieved? (Q8.7) How easy is to review documentation for compliance? (Q8.8) Is there a process in place for implementing changes? (Q8.9)	
	MC5: Spec. flexibility.	modular design (G8.14) adaptability of engineering processes (G8.15)	Are there mechanisms for targeted changes? (Q8.10) How easy is to modify system spec. to reflect changes? (Q8.11)	NA
	Other goals	manageability of non-compliance cases (breaches) (G8.16) manageability of GDPR duties (e.g., consent) (G8.17)	Is there any process towards data subject requests? (Q8.12) Do you have valid agreements with subcontractors? (Q8.13)	fulfillment time (M8.7)
19	MC1: Legal knowledge	awareness and responsibility (G9.1) security of organization (G9.2)	How well are you aware about GDPR? (Q9.1) What are the applicable GDPR demands? (Q9.2)	requirements readability (M9.1) number of compliant systems (M9.2)
	MC2: Traceability	control over compliance (G9.3) visibility and identif. of compliance gaps (G9.4) clarity of compliance status (G9.5)	What controls are in place? (Q9.3) Is there a req.-system mapping and how often is it updated? (Q9.4) Who is responsible for compliance? (Q9.5)	number of gaps (M9.3) coverage of GDPR norms (M9.4) coverage of data processing systems (M9.5)
	MC3: Concerns' separat.	keep business running (G9.6)	NA	NA
	MC4: Spec. transp.	compliance simplification (G9.7) avoid penalties (G9.8) common understanding (G9.9) efficient compliance (G9.10)	How communication is implemented? (Q9.6)	number of communication channels (M9.6)
	MC5: Spec. flexibility.	monitor gaps in compliance (G9.11)	How the awareness about changes and their impact is implemented? (Q9.7)	time since update (M9.7) detection time (M9.8)
	Other goals	compliance efficiency (G9.12)	Do we need this data? (Q9.8)	volume of personal data (M9.9)

Supplementary Material to the Paper "Towards a Goal-Centric Assessment of Requirements Engineering Methods for Privacy by Design": Interview results

ID	Method character.	Goals	Questions	Metrics
I10	MC1: Legal knowledge	clarity of GDPR requirements (G10.1) concreteness of GDPR requirements (G10.2) track changes (G10.3)	Does it work same in different situations? (Q10.1) Is specification complete ? (Q10.2) Is anything missing? (Q10.3) Are checks on system reaction to user input are in place? (Q10.4)	agile process KPIs (M10.1) ability to visualize scenario (M10.2) sufficiency of information for developers (M10.3)
	MC2: Traceability	stay on track in case of changes (G10.4) identifying where changes are required (G10.5) compliance testability (G10.6) ensure that processes support compliance implementation (G10.7)	Is compliance implementation testable? (Q10.5)	passed tests (M10.4)
	MC3: Concerns' separat.	clarity of what in specification is GDPR-relevant (G10.8)	NA	NA
	MC4: Spec. transp.	compliance testability (G10.9) specification understandability (G10.10) specification completeness (G10.11) specification describes resulting software (G10.12)	NA	NA
	MC5: Spec. flexibility.	selecting the right abstractions (G10.13) traceability to support evolution (G10.14) breaking things down to smaller parts (G10.15) separation of concerns (G10.16)	Can we break it down further? (Q10.6) What can change in legal requirements? (Q10.7) What is unlikely to change in legal requirements? (Q10.8)	module size (M10.5) modules complexity (M10.6) change rate (M10.7) number of scenarios and test cases (M10.8)
I11	MC1: Legal knowledge	references to regulations (G11.1) providing context for GDPR requirements in future (G11.2) accessibility of legal knowledge (G11.3) feeling confident about compliance (G11.4) improving communication of requirements (G11.5) spending the right effort (G11.6) save time in next project (G11.7)	Are we implementing compliance right? (Q11.1) Did we misunderstand it? (Q11.2) What is good enough to implement compliance? (Q11.3) Who can access data and how? (Q11.4) What I need to do in the development process? (Q11.5) Do we invest too much effort? (Q11.6)	number of data subject requests (M11.1)
	MC2: Traceability	develop what is required (G11.8) not to develop what is not needed (G11.9) not developing something wrong (G11.10) not forgetting to develop something (G11.11) ensuring software fulfills specification (G11.12) maintain traceability (G11.13)	Where requirements come from? (Q11.7) Is specification correct? (Q11.8) Is system implemented as specified? (Q11.9) Do test cases pass? (Q11.10) Is customer happy with the implemented system? (Q11.11)	bugs' number (M11.2) incidents' numbers (M11.3)
	MC3: Concerns' separat.	fulfilling certification and validation (G11.14) ease of identifying what needs to be changed (G11.15) providing proofs (G11.16) visibility through "living compliance" (G11.17)	Do I comply with the stated requirements? (Q11.12) Can I identify req-s, functions for implementation? (Q11.13) Is documented compliance evaluation available? (Q11.14)	number of components requiring compliance (M11.4) how many new components were added (M11.5) incidents' number (M11.6) time to report incidents (M11.7)
	MC4: Spec. transp.	ease to know what we are implementing (G11.18) ease to know how we are implementing (G11.19) choosing and discussing different solutions (G11.20) ease of implementing updates (G11.21) providing access to external auditor (G11.22)	Can I get an overview of relevant requirements? (Q11.15) What is the origin of requirements? (Q11.16) Do I know where requirements were implemented? (Q11.17)	
	MC5: Spec. flexibility.	minimizing costs of changes and updates (G11.23) good architecture of system (G11.24) not to miss anything (G11.25) identifying unnecessary work (G11.26) facilitating recertification (G11.27)	What is the change required? (Q11.18) Where change is required? (Q11.19) Which code requires update? (Q11.20) Which test cases require update? (Q11.21) Which documentation requires update? (Q11.22)	compliance completeness (M11.8) number of components requiring compliance (M11.9)
	Other goals	synthesizing best practices for compliance (G11.28)	NA	NA

Supplementary Material to the Paper "Towards a Goal-Centric Assessment of Requirements Engineering Methods for Privacy by Design": Interview results

ID	Method character.	Goals	Questions	Metrics
I12	MC1: Legal knowledge	clarity to avoid misinterpretation (G12.1) stakeholders understand what is required (G12.2)	Is specification understandable? (Q12.1) Is specification easy to misinterpret? (Q12.2) What should be done? (Q12.3)	specification clarity (M12.1)
	MC2: Traceability	facilitating auditors to trace from start to implementation (G12.3) reaction to changes in regulations (G12.4)	Can I easily show or discuss compliance implementation? (Q12.4)	NA
	MC3: Concerns' separat.	maintainability (G12.5) scalability (G12.6)	In case of changes of software will compliance hold? (Q12.5)	scalability (M12.2)
	MC4: Spec. transp.	understandability of specification to experts and auditors (G12.7) optimal effort (G12.8) clear definition of personal data processed (G12.9) clear specification of privacy policies (G12.10) implementation of security controls to prevent breaches (G12.11)	Do we have enough security? (Q12.6) Isn't security effecting user friendliness too much? (Q12.7)	NA
	MC5: Spec. flexibility.	ease of compliance tracking (G12.12) ease of identifying what requires changes (G12.13)	Can I find compliance implementation easily? (Q12.8) How easy is to make changes without impacting other components? (Q12.9)	NA
	Other goals	assuring data subject rights (G12.14) transparency of data processing (G12.15)	NA	NA
I13	MC1: Legal knowledge	not exposing to legal risk (G13.1) achieving minimal legal requirements (G13.2)	What does the law require? (Q13.1) How can system deliver what is required? (Q13.2) Is the delivered functionality sufficient? (Q13.3)	test results by domain expert (M13.1)
	MC2: Traceability	ensuring compliance (G13.3) documenting compliance (G13.4)	Is there a responsible person? (Q13.4) Is there up to date documentation? (Q13.5)	NA
	MC3: Concerns' separat.	addressing legal concerns (G13.5) satisfy data subjects' concerns (G13.6)	Are you sure you identified all the personal data? (Q13.6)	response to data subject requests (M13.2)
	MC4: Spec. transp.	translate between business, technical and legal (G13.7) communicate in language that each party understands (G13.8)	What is required legally? (Q13.7) What is implemented technically? (Q13.8) Has compliance implementation been delivered? (Q13.9) Is compliance understood? (Q13.10) Is documentation available? (Q13.11) Has everyone been informed? (Q13.12)	every stakeholder signed off (M13.3)
	MC5: Spec. flexibility.	awareness about compliance when system is modified (G13.9)	Are GDPR requir. incorporated into system requir. and test cases? (Q13.13)	NA
	Other goals	addressing business needs (G13.10)	NA	frequency of regulatory updates (M13.4)
I14	MC1: Legal knowledge	involved roles understand the goals to be achieved (/;) enable decisions on how to implement compliance (G14.2) delegate teams autonomy to develop different solutions (G14.3)	Can teams provide different options to fulfill GDPR? (Q14.1) Can we identify impacted processes and systems? (Q14.2)	team autonomy enablement (M14.1) autonomy in offering solutions (M14.2)
	MC2: Traceability	software maintainability (G14.4) development team knows legal goals (G14.5) teams can autonomously measure goals' achievement (G14.6)	What GDPR compl. goals do we want to achieve in our company? (Q14.3) Do you know what are the strategies to achieve these goals? (Q14.4) Whom to ask if you don't know how to achieve these goals? (Q14.5)	frequency of requests about compliance (M14.3) number of options considered (M14.4)
	MC3: Concerns' separat.	facilitate collaboration (G14.7) breaking down GDPR into something specific (G14.8) involvement of legal experts (G14.9)	Do we have an interpretation for our company? (Q14.6) What does compliance mean for business and engineering? (Q14.7) Do we have an interpretation for each business model? (Q14.8)	NA
	MC4: Spec. transp.	shift left of compliance assessments (G14.10)	Do we need to reverse engineer? (Q14.9) Can we directly understand how compliance was implemented? (Q14.10)	if every question can be answered (M14.5)
	MC5: Spec. flexibility.	plan required resources (G14.11) capturing different types of changes (G14.12) reacting to different types of changes (G14.13) involving required stakeholders (G14.14) employing the right tools/methods (G14.15) identifying the impact on system (G14.16)	NA	NA

Supplementary Material to the Paper "Towards a Goal-Centric Assessment of Requirements Engineering Methods for Privacy by Design": Interview results

ID	Method character.	Goals	Questions	Metrics
115	MC1: Legal knowledge	translate legal goals into business, technical requirements (G15.1) good documentation available to roles involved (G15.2) documenting decisions and solutions (G15.3) help involved roles understand GDPR in their context (G15.4)	Do you have personal data in your system? (Q15.1) For what purposes do you use personal data? (Q15.2)	responsibilities in place (M15.1) documentation availability (M15.2) sufficient knowledge and awareness (M15.3) use of compliance information (M15.4)
	MC2: Traceability	documentation (G15.5) roles involved have knowledge and awareness (G15.6)	Is it related to GDPR compliance? (Q15.3) Does it effect the processing of personal data? (Q15.4)	ability to identify GDPR concerns (M15.5)
	MC3: Concerns' separat.	understand gaps and risks (G15.7) identify countermeasures to address high costs (G15.8)	Where do I have to be compliant? (Q15.5)	
	MC4: Spec. transp.	find GDPR norms addressed with specification (G15.9) awareness about the implementation effort (G15.10)	How does it relate to my business? (Q15.6) What is required to achieve compliance? (Q15.7)	effort required (M15.6)
	MC5: Spec. flexibility.	documentation (G15.11) open architecture (G15.12)	Is particular service reusable? (Q15.8) Can we implement changes easily? (Q15.9)	implementation rate (M15.7) reuse of compliance services across systems (M15.8)
	Other goals	compliance effectiveness (G15.13) have an overview of compliance implementation (G15.14) ongoing measurement of compliance effectiveness (G15.15) addressing incomplete compliance and exceptions (G15.16)	Is compliance implemented effectively? (Q15.10) What do I need to achieve compliance in my company? (Q15.11)	NA

Supplementary Material to the Paper "Towards a Goal-Centric Assessment of Requirements Engineering Methods for Privacy by Design": Interview results