



TRUST - Supporting and Valuing EU Regulatory Compliance with a Seal of TRUST and Co-designed Online Services based on Trustable LLM

D1.1 - Requirements Report

WP1 - End-User Requirements & Architecture Co-Design

Lead beneficiary	Bundesverband IT-Mittelstand e.V. (BITMi)
Lead author	Anna Brodmann (BITMi)
Contributors	All Partners
Submission date	30/09/2026
Version	1.2
Dissemination level	PU



**Funded by
the European Union**

Funded by the European Union (EC grant no. 101299091). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them

Document information

Project details

Project title	TRUST - Supporting and Valuing EU Regulatory Compliance with a Seal of TRUST and Co-designed Online Services based on Trustable LLM
Project acronym	TRUST
Grant Agreement No.	101299091
Call	HORIZON-CL4-2025-03
Type of action	HORIZON Innovation Actions
Topic	HORIZON-CL4-2025-03-DATA-13
Project start date	1 June 2026
Project duration	36 months

Deliverable details

Deliverable number	D1.1
Deliverable title	Requirements Report
Related WP	WP1 - End-User Requirements & Architecture Co-Design
Related deliverable(s)	D1.3, D1.4, D2.1, D2.9, D4.1, D5.1, D6.5
Status	Final
Dissemination level	PU
Lead beneficiary	BITMi
Lead author	Anna Brodmann
Contributors	All Partners
Reviewers	EAMBES

Document history

Document ID:	TRUST_D1.1_Requirements Report_v1.2.docx
--------------	--

Version	Date	Editor(s)	Changes
0.1	16/06/2026	Deliverable Leader (BITMi)	First draft with TOC, bullets explaining content, responsibilities and timeline

Version	Date	Editor(s)	Changes
0.2	23/06/2026	BITMi	ToC, timeline and responsibilities approved.
0.3	07/07/2026	BITMi	Methodology chapter
0.4	20/07/2026	BITMi	Pillar 1 chapter
0.5	29/07/2026	BITMi	Pillar 2 chapter
0.6	12/08/2026	BITMi	Pillar 2 chapter
0.7	19/08/2026	BITMi	Results and minor revisions
0.8	28/08/2026	Deliverable Leader (BITMi)	Version ready for internal review
0.9	23/09/2026	Deliverable Leader (BITMi)	Version ready for quality check
0.95	25/09/2026	UPM	Quality assurance check
1.0	29/09/2026	Deliverable Leader (BITMi)	Final check and improvements
1.1	29/09/2026	Mandat International (MI)	Final review version circulated to BITMi
1.2	30/09/2026	Mandat International (MI)	Final comments incorporated; final version for submission

Quality control and approvals

Role	Who / Partner	Approval date
Deliverable leader	Anna Brodmann / BITMi	29.09.2026
Quality manager	EAMBES	25.09.2026
Project coordinator	Nareamah Perret / MI	30.09.2026

List of acronyms

Abbreviation / acronym	Description
AAP	Applications Agent Plane
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
CICA	Canadian Institute of Chartered Accountants
CMA	Compliance Monitoring Agent
CMM	Capability Maturity Model
CMS	Compliance Management System
CPA	Certification Process Assistant
CRA	Cyber Resilience Act
CSRD	Corporate Sustainability Reporting Directive
CSV	Comma-Separated Values
DGA	Data Governance Act
DORA	Digital Operational Resilience Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EDPB	European Data Protection Board
EEA	European Economic Area
EHDS	European Health Data Space (Regulation)
ELAL	Enhanced LLM Abstraction Layer
ELSDS	European Legal Semantic Data Space
ESG	Environmental, Social, and Governance
EU	European Union
FINMA	Swiss Financial Market Supervisory Authority
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation
GPT	Generative Pre-trained Transformer
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
LLM	Large Language Model
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (Spanish Data Protection Act)
LRA	Legal Risk Analyser

Abbreviation / acronym	Description
LSSI-CE	Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (Spanish E-Commerce and Information Society Services Act)
NIS2	Directive on measures for a high common level of cybersecurity across the Union (Second Network and Information Security Directive)
OPRCS	Online Platform of Regulatory Compliance Services
PMM	Privacy Maturity Model
RCA	Regulatory Compliance Assistant
RCE	Regulatory Checker/Evaluator
ROA	Regulatory Obligations Analyser
RRA	Regulatory Reports Assistant
RRAG	Reinforced RAG Model
RSS	Really Simple Syndication
SME	Small and Medium-sized Enterprise
TIA	Transfer Impact Assessment
UX	User Experience
WP	Work Package

Contents

Document information.....	2
<i>Project details</i>	<i>2</i>
<i>Deliverable details.....</i>	<i>2</i>
Document history	2
Quality control and approvals	3
List of acronyms	4
Contents	6
List of tables	8
Executive summary	9
1. Introduction	10
1.1 <i>Purpose of the document</i>	<i>10</i>
1.2 <i>Relation to other project work</i>	<i>10</i>
1.3 <i>Structure of the document.....</i>	<i>11</i>
2. Main content.....	13
2.1 <i>Methodology for Requirement Gathering.....</i>	<i>13</i>
2.1.1 <i>Approach Overview</i>	<i>13</i>
2.1.2 <i>Surveys</i>	<i>14</i>
2.1.3 <i>Focus Groups</i>	<i>15</i>
2.1.4 <i>Data Analysis.....</i>	<i>16</i>
2.2 <i>Pillar 1: Requirements for LLM Reliability (ELAL)</i>	<i>17</i>
2.2.1 <i>Objective of this section</i>	<i>17</i>
2.2.2 <i>Stakeholder Input.....</i>	<i>17</i>
2.2.3 <i>Key Requirements</i>	<i>21</i>
2.2.4 <i>Validation Needs.....</i>	<i>23</i>
2.3 <i>Pillar 2: Requirements for AI-Based Compliance Services (OPRCS & AAP).....</i>	<i>24</i>
2.3.1 <i>Objective.....</i>	<i>24</i>
2.3.2 <i>Stakeholder Input.....</i>	<i>24</i>
2.3.3 <i>Key Requirements</i>	<i>28</i>
2.3.4 <i>Validation Needs.....</i>	<i>38</i>
2.4 <i>Pillar 3: Requirements for Seal of Trust Certification Schemes</i>	<i>40</i>

2.4.1	Objective.....	40
2.4.2	Stakeholder Input.....	40
2.4.3	Key Requirements.....	41
2.4.4	Validation Needs.....	44
3.	Results / findings	44
3.1	<i>Prioritized End-User and Stakeholder Requirements.....</i>	44
3.1.1	Objective of the Section.....	44
3.1.2	Prioritized Key findings	44
3.1.3	Gaps in Requirement Coverage	48
3.2	<i>Challenges and Lessons Learned.....</i>	49
3.2.1	Challenges Faced During Requirement Gathering.....	49
3.2.2	Unresolved Issues Requiring Input from Other Work Packages	49
3.2.3	Improvements for Future Phases.....	50
4.	Conclusions.....	50
	References	53
	Annexes.....	55
	<i>Annex 1 - SME Survey: Questionnaire</i>	55
	<i>Annex 2 - SME Survey: Results</i>	59
	<i>Annex 3 - DPO Survey: Questionnaire.....</i>	82
	<i>Annex 4 - DPO Survey: Results.....</i>	86
	<i>Annex 5 – SME Focus Group Interview Guidelines</i>	116
	<i>Annex 6 - SME Focus Group - Workshop 1</i>	118
	<i>Annex 7 - SME Focus Group - Workshop 2</i>	123
	<i>Annex 8 – DPO Focus Group Interview Guidelines</i>	128
	<i>Annex 9 - DPO Focus Group - Workshop 3.....</i>	131
	<i>Annex 10 - DPO Focus Group - Workshop 4</i>	139

List of tables

Table 1: Trust without human oversight	18
Table 2: Reliability	18
Table 3: Handling of multiple regulations	19
Table 4: Legal accountability	20
Table 5: Data privacy	21
Table 6: Data leak prevention	22
Table 7: SME's perspective on the current compliance landscape	25
Table 8: DPO's perspective on the current compliance landscape	27
Table 9: Regulatory Updates.....	28
Table 10: Regulatory Scope	30
Table 11: ROA	31
Table 12: LRA.....	32
Table 13: RRA.....	35
Table 14: CPA - Target Certifications	38
Table 15: Motivation for Certifications.....	40
Table 16: SME Constraint for Certifications	43
Table 17: Convergence of End-user's needs	45
Table 18: End-user's conflicting needs.....	46

Executive summary

The TRUST project addresses the challenges faced by the more than 24 million European companies subject to 144,000 European Union (EU) regulations. Although artificial intelligence (AI) has the potential to ease compliance, its adoption by small and medium-sized enterprises (SMEs) is hindered by concerns about large language model (LLM) hallucinations, the cost of adoption, and the rapid evolution of technology. This report identifies the essential requirements of various stakeholder groups, including European SMEs, Data Protection Officers (DPOs), engineers, auditors, and compliance professionals, to ensure the TRUST platform effectively supports compliance workflows while maintaining transparency, reliability, and human oversight.

Using a pragmatic mixed-methods requirements-elicitation approach that combines descriptive survey data with qualitative stakeholder workshops, this report identifies areas of convergence and divergence among stakeholder groups. Across the participants consulted, recurring priorities include more reliable and verifiable LLM outputs and visible human oversight. In other areas, needs differ systematically by user role and professional context: SME participants emphasize simplification and accessibility, while DPOs and other compliance professionals require more configurable, professional-grade functionality. These differences are documented as design inputs for subsequent co-design and development phases.

The findings directly inform three priority workstreams of the TRUST project: the first pillar (LLM reliability) benefits from requirements for reducing hallucinations and preventing data leaks. The second pillar (AI-based compliance services) receives specifications for six co-designed services that address the documented users' needs. Finally, the third pillar (certification and governance) receives input for compliance certification standards and governance frameworks.

Overall, this report translates stakeholder input into requirements and design inputs across all three pillars of the TRUST project. Convergence on human-in-the-loop mechanisms and transparent AI behaviour provides a clear direction for further specification, while documented differences between user groups support the development and validation of role-specific platform features. These findings directly inform ongoing technical, compliance, and co-design workstreams and provide an evidence base for iterative requirements refinement.

Keywords:

AI-Assisted Regulatory Compliance; Human-in-the-Loop Oversight, LLM Reliability, Hallucination Prevention, Stakeholder Requirements

1. Introduction

1.1 Purpose of the document

This document establishes the basis for the TRUST system by identifying user-driven requirements and addressing the essential needs of European SMEs, Data Protection Officers (DPOs), engineers, auditors and certification bodies in using AI-driven tools for regulatory compliance. It should be noted that this report covers the first phase of requirements gathering. This phase involved two of the four use case groups set out in the TRUST project proposal: SME representatives and DPOs. The Engineers and Medical Research Use Case, targeting engineers and compliance officers from hospitals and medical research organisations, is scheduled to commence at M13, as set out in the project proposal. Its participants will contribute to an expanded requirements baseline in subsequent deliverables. Therefore, the findings presented here should be read as an initial, partial baseline that will be enriched and validated as the remaining use cases are activated.

The report is intended for all members of the TRUST project, providing them with a clear outline of user requirements for the project's various components. It thereby directly contributes to the modularity, scalability and interoperability of the TRUST system, ensuring that the Enhanced LLM Abstraction Layer (ELAL), the Online Platform of Regulatory Compliance Services (OPRCS) and the Seal of Trust certification schemes are grounded in real-world needs and validated through iterative testing.

1.2 Relation to other project work

This report forms an integral part of the three-pillar approach of the TRUST project. For Pillar 1 (LLM reliability) the report informs the development of the ELAL, including the Reinforced RAG Model and Compliance Monitoring Agent (CMA), by capturing requirements for LLM reliability, reducing hallucinations, and preventing data leaks. For Pillar 2 (AI-Based Compliance Services) this report supports the Online Platform of Regulatory Compliance Services (OPRCS) and its Applications Agent Plane (AAP), which will host six co-designed services (e.g. the Regulatory Compliance Assistant, the Legal Risk Analyser and the Certification Process Assistant) to address priority needs identified through surveys, focus group workshops and co-design sessions.

For Pillar 3 (Seal of Trust) the report provides the input necessary to specify certification schemes that align with end-user expectations and regulatory standards.

The findings of this report will directly inform three corresponding tasks.

- For T3.1 Co-design support the report provides the outline and initial starting point for the iterative feedback workshops to establish a set of specifications for

the different services, as well as recommendations for the platform's overall functioning.

- T3.8 (Regulatory Reporting Assistant) will be supported by providing a list of end users' needs for the automation of accurate and timely reports that also meet the specific requirements of regulatory bodies.
- For T4.2 (Seal of TRUST Certification Criteria Specification), this report will provide end-user requirements to inform the selection of regulatory frameworks to be addressed by the certification schemes for compliance evaluation, taking into account the stakeholders' interests, needs, and practical expectations, with particular attention to their applicability for SMEs.

The findings of this report will further inform collaboration between WPs, particularly between WPs 2, 3, 4 and 5, to ensure that the needs and expectations of end users form the guiding principles of the project.

1.3 Structure of the document

This document is structured into four major chapters, designed to guide readers from the methodological foundations of requirement gathering through to consolidated findings, challenges, and conclusions. The logical flow of the document mirrors the progression from raw stakeholder input to structured, actionable requirements that will feed directly into the workstreams of the TRUST project.

The document follows a deliberate progression from evidence collection, through requirement synthesis, to actionable output. First, stakeholder needs are captured through quantitative surveys and qualitative focus group workshops. A convergent mixed-methods design is applied to ensure insight is both broad and deep. These outputs are then mapped against the three TRUST service pillars to ensure that the needs of all stakeholder groups are systematically addressed within the platform's design. Next, requirements are triangulated, prioritised and assessed for coverage gaps, conflicting needs and unresolved issues requiring cross-work package coordination. Finally, the findings are translated into forward-looking recommendations and downstream inputs for the TRUST system's technical and certification workstreams.

Chapter Overview

This document is structured into four major chapters.

- Chapter 1 – Introduction provides the contextual foundation for the report. It outlines the purpose of the deliverable, its relation to other project work across the three TRUST pillars, and the structure of the document itself.
- Chapter 2 – Main Content constitutes the analytical core of the report. It is organised around the three TRUST pillars and follows a logical progression from methodology to requirements

- Chapter 3 – Results and Findings synthesises the outputs of the requirement gathering process into consolidated, prioritised findings.
- Chapter 4 – Conclusions summarises the main outcomes of the deliverable, identifies challenges addressed and outstanding, and outlines the next steps in alignment with the TRUST project roadmap.

Navigation Guide by Role and Work Package

Reader Profile	Recommended Sections
All Readers	Chapter 3 (Results) Chapter 4 (Conclusions)
WP1 – Architecture Co-Design	Section 2.2.2 (Stakeholder Input) Section 2.3.2 (Stakeholder Input) Section 2.4.2 (Stakeholder Input)
WP2 – ELAL Development	Section 2.2 (Pillar 1)
WP3 – OPRCS & Compliance Services	Section 2.3 (Pillar 2)
WP4 – Seal of Trust Certification	Section 2.4 (Pillar 3)
WP5 – End User Qualification	Section 2.2.2 (Stakeholder Input) Section 2.3.2 (Stakeholder Input) Section 2.4.2 (Stakeholder Input)
SME Representatives	Section 2.2.3 (Key Requirements) Section 2.3.3 (Key Requirements) Section 2.4.3 (Key Requirements)
DPOs and Legal Consultants	Section 2.4 (Pillar 3)
Auditors and Certification Bodies	Section 2.2.4 (Validation Needs) Section 2.3.2 (Validation Needs) Section 2.4.2 (Validation Needs)
Project Management / Coordinators	Chapter 1 (Introduction)

Annexes and Appendices

Readers seeking to review the original survey instruments, focus group discussion guides, or raw statistical outputs are directed to the relevant annexes for full methodological transparency.

The following annexes are included at the end of this document:

- Annex 1 - SME Survey: Questionnaire
- Annex 2 - SME Survey: Results
- Annex 3 - DPO Survey: Questionnaire
- Annex 4 - DPO Survey: Results

- Annex 5 – SME Focus Group Interview Guideline
- Annex 6 - SME Focus Group - Workshop 1
- Annex 7 - SME Focus Group - Workshop 2
- Annex 8 – DPO Focus Group Interview Guidelines
- Annex 9 - DPO Focus Group - Workshop 3
- Annex 10 - DPO Focus Group - Workshop 4

2. Main content

2.1 Methodology for Requirement Gathering

2.1.1 Approach Overview

The requirement gathering process for the TRUST project employed a pragmatic mixed-methods approach, combining quantitative surveys with qualitative stakeholder workshops. The purpose of combining these instruments was not to produce statistically representative estimates or a standalone qualitative research study, but to support requirements elicitation by capturing both structured patterns in stakeholder priorities and contextual explanations of user needs.

The stakeholder groups consulted in this phase comprised SME representatives and DPOs. In accordance with the project proposal, the Engineers and Medical Research Use Case and the European Certification Use Case are planned to commence at M13. As this report is filed in M4, input from these groups could not be incorporated yet. These requirements will be revisited, validated and extended once the additional stakeholder groups have been engaged.

The survey data provide descriptive, comparable information within the respondent sample, while the workshops provide qualitative insight into experiences, expectations, tensions, and proposed solutions. Triangulating these sources supports the identification of converging and diverging requirements while recognising the limitations of each instrument when used in isolation [1, p. 102].

This methodological combination was calibrated to the applied purpose of the deliverable: informing the design and subsequent validation of TRUST services. The stakeholder groups represent distinct perspectives within the regulatory compliance ecosystem, but the samples are not treated as statistically representative of the wider European population. Surveys and workshops were conducted during the same requirements-gathering phase. Quantitative results were used as a descriptive baseline, while workshop discussions provided contextual depth and helped explain why particular needs, constraints, and preferences emerged.

2.1.2 Surveys

Surveys were utilised as the foundational quantitative instrument in the requirement gathering process. They were designed as a structured, self-administered online questionnaire targeting key stakeholder groups, including internal and external DPOs, SME representatives, auditors, and certification bodies.

The implementation of the survey instrument was informed by the understanding that online surveys offer significant advantages in terms of reach, speed, and cost-effectiveness, enabling rapid distribution across diverse professional networks [2, p. 73]. However, in accordance with methodological concerns articulated in the relevant literature, particular care was exercised to ensure the survey's distribution was directed towards a clearly defined and adequately describable demographic, namely, professional networks comprising DPOs, compliance practitioners and SMEs, as opposed to an indiscriminate public audience. To this end distribution was facilitated through relevant professional associations and partner networks of the TRUST consortium across EU member states. However, as noted in [3, p. 576], "results of online surveys must be regarded as tentative when the surveys are distributed to an unknown audience and when voluntary participation in the survey can result in respondents with biases selecting themselves into the sample".

The SME survey collected 92 data records. Active respondents who were relevant to compliance predominantly identified as members of SMEs (47.27%), followed by other roles, such as members of the compliance team (16.36%) and data protection officers (3.64%). In terms of organisational structure, 46.15% of SME respondents reported having no internal compliance team, while 25% had a dedicated team. Of those with a team, 50% comprised two to five people, while 29.17% relied on a single compliance officer. Geographically, the SME sample was concentrated in Germany (87.5%), with smaller numbers from Finland, France and Ireland.

The DPO survey collected 118 records, with respondents primarily identifying as internal DPOs (employees: 47.5%), external DPOs (consultants: 32.5%), materialised DPOs (5%) and other roles (15%). Of the DPOs working within organisations, 50.94% had an internal compliance team. Of these, 60% were supported by a team of two to five people, while 26% were supported by a single compliance officer. The DPO sample was more geographically diverse, with the main countries represented being France (45.12%), Spain (29.27%) and Germany (13.41%). In terms of sector, DPOs primarily operated in IT (17.72%), health and life sciences (13.92%), energy and utilities (8.86%), media and content (8.86%), and financial services (7.59%). A substantial proportion (37.97%) identified as belonging to other or cross-sector contexts.

It should be noted that neither survey sample is statistically representative of the wider European population. The results are intended to provide a descriptive baseline of the respondent groups' priorities and challenges.

The design of the survey was conducted in accordance with the established principles for the development of questionnaires in the field of applied social research. The questions were formulated to be clear, non-leading, and appropriately scaled, with a combination of closed-ended (Likert-scale) items and open-ended prompts to allow respondents to articulate nuanced concerns [4, pp. 1-2]. The survey comprised multiple sections covering: respondent background and organisational context; current compliance challenges; the importance of specific regulatory frameworks; most time-consuming compliance tasks; and desired features of AI-powered compliance tools.

2.1.3 Focus Groups

Focus group workshops constituted the central qualitative instrument for requirements elicitation, providing a structured yet exploratory environment in which stakeholders could articulate, debate, and refine their needs and expectations regarding TRUST's services. In this report, 'qualitative' refers to the collection and thematic interpretation of open stakeholder input for applied requirements elicitation and co-design; it does not imply that the workshops constitute a standalone qualitative research study. In total, four workshops (W1-W4) were conducted with distinct stakeholder cohorts. Stakeholder homogeneity within the workshops was used to facilitate productive discussion among participants with comparable professional contexts [5, p. 6].

A focus group discussion is defined as "an interactive discussion between six to eight [...] participants, led by a moderator and focusing on a specific set of issues. The aim of a focus group discussion is to gain a broad range of views on the research topic over a 60–90 minute period, and to create an environment for participants to express their views" [6, p. 136]. This makes the method well suited to the objectives of the project, given its established value for research on group norms, meanings and processes and its capacity to "clarify, extend, qualify or challenge data collected through other methods" [7, p. 2]. It has also been noted that a single focus group discussion can generate around seventy percent of the same issues as a series of in-depth interviews with the same number of people [8, p. 378], making it an efficient mechanism for comprehensive requirements elicitation.

The workshops were structured around moderated discussion guides organised around thematic areas relevant to each user segment. Questions were formulated to allow participants to explain their experiences and priorities in their own terms before discussion moved toward more specific TRUST-related topics. Because the sessions were also designed for requirements elicitation and co-design, they were necessarily informed by the project's service concepts. The resulting data should therefore be interpreted as stakeholder input within an applied design context rather than as fully unframed exploratory research [9, pp. 327-328].

All focus group sessions followed a modified funnel structure, commencing with broader contextual questions and progressively moving toward more specific topics related to the TRUST service pillars. This approach is consistent with the recommendation that in applied research focused on eliciting substantial content,

discussions should progress "from more general, participant-oriented questions to more specific, researcher-oriented questions" [10, p. 172].

The DPO-oriented focus groups were additionally structured to explore the professional landscape of data protection compliance, including the daily operational challenges faced by DPOs, current approaches to regulatory monitoring and reporting, and expectations for AI-assisted compliance tools.

The focus groups, which were oriented towards SMEs, addressed the specific challenges faced by smaller organisations in meeting EU regulatory obligations. These challenges included resource constraints, a lack of dedicated compliance expertise, and limited budgets. The SME sessions were conceived to be less technically detailed than the DPO sessions, recognising that SME representatives may possess varying degrees of familiarity with regulatory frameworks.

However, both sets of focus groups were aligned around the six TRUST tools and underlying ELAL to ensure that the findings could be mapped directly onto the platform's architecture.

2.1.4 Data Analysis

Survey data were analysed descriptively using frequency distributions and mean ratings across relevant item categories. These results were used to provide a preliminary indication of priorities and recurring challenges within the respondent sample; they are not intended to support statistical generalisation to the wider population. Workshop transcripts and moderator notes were analysed using a structured thematic approach. Coding focused on recurring needs, concerns, tensions, proposed solutions, and stakeholder-specific priorities. The analysis combined deductive categories derived from the TRUST service architecture with themes emerging from the workshop material. This pragmatic approach supports transparent requirements elicitation without claiming a standalone grounded-theory study.

The quantitative and qualitative strands were first reviewed separately and then compared during interpretation [12, pp. 63-64]. Following a joint-display logic [13], survey patterns were used to indicate prevalence and relative priority within the respondent sample, while workshop themes provided context and explanations for the mechanisms, motivations, and boundary conditions behind those patterns. An integrated results matrix was used to juxtapose the two evidence strands and identify convergence, divergence, and stakeholder-specific requirements. This integration supports traceability from stakeholder evidence to requirements while avoiding claims of statistical representativeness beyond the available samples [14, p. 5].

The consolidated outputs were subsequently mapped against the three TRUST service pillars (Requirements for LLM Reliability (ELAL), Requirements for AI-Based Compliance Services (OPRCS & AAP), and Requirements for Seal of Trust

Certification Schemes) with a view to generating actionable requirements for each component of the platform. The structuring of requirements on a pillar-based system ensures that the needs of DPOs, SMEs, auditors and certification bodies are systematically addressed within the platform's design. In instances where divergent needs were identified among the stakeholder groups, the existence of such tensions was documented as open issues to be given full consideration during the development process.

2.2 Pillar 1: Requirements for LLM Reliability (ELAL)

2.2.1 Objective of this section

This chapter provides a comprehensive definition of the end-user and stakeholder requirements for the Enhanced LLM Abstraction Layer (ELAL). The documented end-user requirements directly inform the design of two primary ELAL components: the Reinforced RAG Model (RRAG) and the Compliance Monitoring Agent (CMA). The requirements can be considered within the context of three core dimensions: LLM reliability, accountability and data privacy.

2.2.2 Stakeholder Input

AI as a tool

The most important concern highlighted by all groups of end users is that human authority must be preserved throughout any AI-assisted compliance workflow. Only 9.38% of SME survey respondents indicated a willingness to use AI without human oversight. In contrast, 53.13% rejected unsupervised AI use outright, while 43.75% only accepted it for specific, bounded tasks. In order to establish trust in the products provided, human oversight must be a visible component of the systems architecture rather than a nominal feature, since, as a Workshop 3 participant put it, “human oversight is paramount to reliability”. The SME survey confirmed this attitude since 87.5% of respondents identified human-in-the-loop as the primary mechanism for building trust in a compliance AI tool. Additionally, SMEs in Workshop 2 identified the risk of uncritical adoption of AI-generated suggestions as a significant systemic danger. As the participant put it: “I think about 95 percent of the companies that might use it will say: ‘Yes, that was proposed.’ And then I’ll just adopt it.” (Workshop 2). Hence, outputs must clearly differentiate between AI-generated legal and non-legal information, risk alerts and final (legal) judgements.

Overall participants firmly position AI as a tool, rather than a process or decision-maker, and advocate handling it accordingly. As one participant put it: “For compliance work, AI should support decision-making, not replace professional responsibility” (Workshop 4).

Table 1: Trust without human oversight

Survey Question	Finding
SME Q015: Trust without human oversight	Yes: 9.38% No: 53.13%; Only for specific tasks: 43.75%
SME Q018: Prerequisites for trust in a compliance AI tool	Human-in-the-loop: 87.50%; Transparency in AI decisions: 84.38%; Explainability: 78.13%; Auditability: 68.75%

Reliability as a prerequisite for trust

Across all workshop sessions and survey instruments, participants consistently identified LLM reliability as the foremost challenge to the confident adoption of AI-assisted compliance tools. Hallucinations and incorrect legal sources were the most frequently cited concerns. In the SME survey, 78.13% of respondents cited hallucinations and invented results as a primary concern about using AI for compliance purposes. Among DPO survey respondents, this figure was 82.61%.

These concerns are largely rooted in participants' existing experiences with their current AI solutions. One participant who implemented a homemade AI tool for compliance noted that "AI given sources to court decisions are often poor, so the AI experience is it also" (Workshop 4). Reliability was therefore one of the highest-rated features in the SME survey, with 67.74% of respondents rating it 5 out of 5. Among DPO respondents, 71.43% rated reliability 5/5.

Table 2: Reliability

Survey Question	Finding
SME Q017: Concerns about AI for compliance	Hallucinations: 78.13%; Reliability: 65.63%; Lack of transparency: 62.5%; Data privacy: 68.75%
DPO Q017: Concerns about AI for compliance	Hallucinations: 82.61%; Data privacy: 84.78%; Reliability: 60.87%; Lack of transparency: 50%; Cost: 23.91%
Survey Question	Finding
SME Q009: Importance of features – Reliability	Maximally important (5/5): 67.74% Very important (4/5): 19.35%

DPO Q009: Importance of features – Reliability	Maximally important (5/5): 71.43% Very important (4/5): 26.19%
---	---

Cross-LLM validation

Cross-LLM validation was raised by SME participants as a possible way to increase trust and make uncertainty more visible. One participant proposed a secondary, independent AI model that would cross-check the primary model's output and present a confidence score from 0 to 100: "It would probably also help me if I were told how confident it is. A scoring from zero to a hundred. If it says ninety percent confident, okay; if it says sixty percent confident, well, then I'd better check again. [...] It should probably be a different AI that checks this" (Workshop 1). This should be treated as a user-proposed design idea rather than a validated requirement. Although no user-facing reliability score is currently planned, the suggestion is conceptually related to TRUST's existing technical approach of comparing outputs across multiple LLMs. Any user-facing scoring mechanism would require separate technical assessment and validation before adoption.

Handling of multiple regulations

Handling multiple, partially overlapping regulations (e.g. GDPR, AI Act and NIS2) simultaneously emerged as one of the most significant challenges for SMEs and DPOs alike. Within SME Q009, the ability to handle multiple regulations received the highest share of maximum ratings (70.97%); 65.91% of DPO respondents also assigned the maximum score. This provides strong evidence within the available samples that multi-regulatory handling should be treated as a high-priority capability. The ELAL should therefore be designed to support multi-regulatory compliance queries while maintaining accuracy and controlling hallucination risk.

Table 3: Handling of multiple regulations

Survey Question	Finding
SME Q009 Ability to handle multiple regulations	Maximally important (5/5): 70.97% Very important (4/5): 22.58%
DPO Q009 Ability to handle multiple regulations	Maximally important (5/5): 65.91% Very important (4/5): 27.27%

Inconsistency because of prompting styles

Inconsistency in quality of outputs depending on the prompting style and the version of the model was identified as a further challenge. One participant highlighted that many prompts were needed and that the LLM model was often confused, providing incorrect information or sources. Additionally, participants questioned how consistent the quality of the Trust tools could be with an LLM-agnostic approach (Workshop 2).

Anti-sycophancy design

Anti-sycophancy UX design, intended to reduce the risk of users uncritically accepting AI-generated outputs, was raised as a specific design principle in Workshop 4. The underlying user need is clear: outputs should invite scrutiny, surface uncertainty, and make verification straightforward. Anti-sycophancy should therefore be treated as a candidate cross-cutting design principle to be specified and validated jointly with WP2/WP3, rather than as a non-negotiable requirement derived from the workshop alone. Possible implementation choices include the communication of confidence and uncertainty, citation verification, wording that distinguishes recommendations from conclusions, and prompts that encourage review where consequential decisions are involved.

Legal accountability

Participants from both DPO and SME groups stressed that legal and professional responsibility for compliance decisions cannot simply be delegated to an AI system. The DPO survey reinforced the importance of responsibility for incorrect outputs and meaningful human oversight as aspects that current AI-based compliance tools do not sufficiently address. DPOs did not reject AI for compliance work; rather, the AI-comfort score (3.73 / 5 versus 3.75/ 5 for SMEs) is consistent with the workshop observation that expert users may be willing to use AI under clearly defined conditions of reliability, traceability, and human responsibility. The available data do not establish a causal explanation for the difference in comfort scores.

Table 4: Legal accountability

Survey Question	Finding
DPO Q011: Comfort with AI for compliance	Mean: 3.73 / 5
SME Q011: Comfort with AI for compliance	Mean 3.75 / 5
DPO Q017: Concerns about AI in compliance	Other: “Outdated or incomplete legal sources, insufficient traceability of conclusions, lack of meaningful human oversight, and uncertainty about responsibility for incorrect compliance recommendations”
Survey Question	Finding
DPO Q019: What else is important to you?	“[...] It would also be important to clarify the role of human review, allocation of responsibility for incorrect outputs, data retention and confidentiality, security and incident management, interoperability and data portability, and safeguards against

	vendor lock-in. For DPOs and legal professionals, the ability to evidence why a conclusion was reached, which sources were used and who validated the result is essential.”
--	---

Data privacy

Stakeholders identified data privacy and confidentiality as critical safeguarding concerns. In SME Q017, 68.75% selected data privacy as a concern about using AI for compliance; in SME Q009, 64.52% rated data privacy and confidentiality protection as maximally important as a tool feature. 78.57% of DPO respondents rated the feature maximally important. Participants additionally demanded protection against unauthorised external access and objected to the use of inputs for model training without explicit consent (Workshops 2 and 4). Regarding data localisation, participants expressed a strong preference for EU-hosted infrastructure, with some describing this as an absolute condition (Workshop 4).

Table 5: Data privacy

Survey Question	Finding
DPO Q009: Data privacy and confidentiality	Maximally important (5/5): 78.57%
SME Q009: Data privacy and confidentiality	Maximally important (5/5): 64.52%

2.2.3 Key Requirements

2.2.3.1 Reinforced RAG Model (RRAG)

Contextual enrichment

Contextual enrichment through verified legal sources was identified as one of the most important requirements for reducing hallucinations. Participants consistently demanded that every AI output be grounded in authoritative, up-to-date regulatory documentation (Workshop 1). Therefore, the RRAG must retrieve and contextualise responses, ensuring that outputs are anchored to official, traceable sources rather than statistical inference alone.

Transparent citation

Transparent citation and source traceability, or the “Possibility to check sources” (Workshop 4), were deemed indispensable by all stakeholder groups. The tool must provide direct, verifiable links to source documents rather than merely paraphrased references. DPO respondents further specified that this must extend to version control and update timestamps. They noted that an AI tool without datestamped legal sources cannot be trusted for compliance purposes (Workshop 4). Consequently, the RRAG

must retrieve and surface direct, verifiable source links alongside every generated output, including metadata such as version numbers and update timestamps. This requires the retrieval pipeline to index not only document content but also provenance metadata.

2.2.3.2 Compliance Monitoring Agent (CMA)

Model training

Participants demanded that the ELAL does not enable LLMs to silently learn from user inputs. As one participant in Workshop 2 put it: “There should be no ‘learning’ of the LLM model.” This confirms the necessity of the CMA within the ELAL, since it is designed to ensure that data transfer only occurs with explicit and informed user consent. Consequently, no user data will be processed for unauthorised LLM training through the TRUST products.

Data leak prevention

Preventing confidential data from leaking to LLMs was expressed as a strong requirement across stakeholder groups. Survey results likewise indicate that data privacy and confidentiality are important concerns, although the share assigning maximum importance differs by group. Participants pointed out that, in compliance contexts, uncontrolled transfer of sensitive personal or organisational data to external LLMs may create GDPR compliance and security risks. One survey respondent specifically called for “data retention and confidentiality, security, and incident management” to be addressed as core design requirements. Accordingly, the CMA should detect and flag relevant data transfers before they occur, while privacy and security by design should serve as default principles throughout the project's development cycle.

Table 6: Data leak prevention

Survey Question	Finding
DPO Q009: Data privacy and confidentiality	Maximally important (5/5): 78.57% Very important (4/5): 16.67%
SME Q009: Data privacy and confidentiality	Maximally important (5/5): 64.52% Very important (4/5): 19.35%
Survey Question	Finding
DPO Q017: AI concerns	Hallucinations: 82.61%; Data privacy: 84.78%; Reliability: 60.87%; Lack of transparency: 50%; Cost: 23.91%
SME Q017: AI concerns	Hallucinations: 78.13%; Reliability: 65.63%;

	Lack of transparency: 62.5%; Data privacy: 68.75%
DPO Q019: What else is important to you?	[...] It would also be important to clarify the [...] data retention and confidentiality, security and incident management, interoperability and data portability, and safeguards against vendor lock-in. [...]

2.2.4 Validation Needs

Traceable Accuracy Testing

All AI outputs must be verifiable against original legal source documents. Validation must demonstrate that citations and metadata are real, correctly applied and not paraphrased or statistically inferred.

Cross-Prompting Consistency

Given participant concerns about prompt-dependent variability, the ELAL must be tested for output consistency across different prompting styles and user expertise levels.

Independent AI Reliability Scoring

A user-facing reliability score generated by a secondary AI model was proposed by one workshop participant. It is retained here as a candidate validation and UX concept, not as an established acceptance criterion. WP2 should assess whether such a score would be technically meaningful, sufficiently calibrated, and understandable to users before it is considered for implementation or acceptance testing.

Human-in-the-Loop Review as a Testable Component

Validation must confirm that no compliance output can be exported without a completed and logged human review step. This must be tested through end-to-end workflow scenarios in which the review gate is deliberately bypassed, verifying that the system structurally prevents such circumvention.

Disclaimer and Liability Boundary Validation

Clear AI-generated content disclaimers with explicit liability boundaries must be validated prior to deployment, since stakeholders were concerned that without these safeguards, organisations would uncritically adopt AI outputs.

Data Leakage Prevention Testing

The CMA must be validated through scenario-based testing to confirm that no personal or confidential data is transferred to LLMs without explicit user consent. This testing must align with GDPR Article 25 compliance standards and AI Act requirements.

2.3 Pillar 2: Requirements for AI-Based Compliance Services (OPRCS & AAP)

2.3.1 Objective

This chapter defines the end-user and stakeholder requirements for the Online Platform of Regulatory Compliance Services (OPRCS) and its underlying Applications Agent Plane (AAP). The requirements documented here address three core user needs: reducing the administrative and cognitive burden of regulatory compliance, providing actionable and reliable intelligence across a growing body of overlapping EU regulations, and enabling organisations to demonstrate and manage their compliance status in a structured, auditable and human-overseen manner.

2.3.2 Stakeholder Input

2.3.2.1 *SME's perspective*

Across all workshops, SME participants painted a consistent picture of compliance as an activity that is under-resourced, fragmented and reactive. They perceived regulatory environments as overwhelming, ambiguous and difficult to navigate. Regulations were described as being both vague and numerous, and as spanning multiple legal domains. This lack of clarity can lead to either inaction, which blocks all data use, or a disproportionate effort, such as repeatedly obtaining consent for minor tasks (Workshop 1). Crucially, failing to recognise the existence of a regulation renders all other compliance activities futile.

To cope with this ambiguous environment, participants in both SME workshops deploy ad hoc, improvised or person-dependent processes. Whether implemented by a managing director searching through documents, a custom-built ChatGPT agent or an entirely self-developed product, these workarounds are fragile, unreliable and unsustainable (Workshop 1 and 2), as confirmed by low satisfaction scores in the SME survey, current processes are recognised as inadequate.

The SME survey revealed that 46% of respondents do not have a compliance team at all, and most rely on manual documents or improvised tools. Due to this structural resource deficit, responsibility for compliance is neither clearly assigned nor consistently held. It drifts between IT-department, data protection and management, ultimately defaulting to whoever cannot refuse it (Workshop 2). Compliance processes depend on one person and human expertise spanning multiple sectors is identified as essential but currently lacking (Workshop 1). This structural vulnerability is exacerbated by the risk of institutional knowledge loss during staff turnover, particularly when experienced personnel retire, as there is no continuous process or permanent access to previously made compliance decisions (Workshop 2).

The structural challenge of concentrating compliance responsibility in a single individual results in SMEs exhibiting reactive rather than proactive compliance behaviour, driven by severe resource, time and budget constraints.

Table 7: SME's perspective on the current compliance landscape

Survey Question	Finding
SME Q002: Internal compliance team	No internal compliance team: 46.15% Internal compliance team: 25%
SME Q003: People dedicated to compliance	One person compliance team: 29.17% 2–5-person compliance team: 50%
SME Q007: Tools currently used	Manual spreadsheets: 62.5%; AI-powered tools: 50%
SME Q008: Satisfaction with current compliance tools	Mean 3.19 / 5
SME Q005: Biggest obstacles to achieving compliance	Time-consuming manual processes: 62.5%; Lack of internal expertise: 40.63% Complexity of regulations and legal jargon: 68.75%; Lack of clear guidance or best practices: 65.63%; Frequent changes in regulations: 59.38%
SME Q006: Most time-consuming compliance tasks	Monitoring regulations: 67.74%; Auditing: 58.06%

2.3.2.2 DPO's perspective

Due to their professional expertise, DPOs have a different view of the current compliance landscape. On the one hand, understanding regulations is not as much of a burden for them, but on the other hand, they face structural deficits in terms of internal communication. For instance, they struggle to secure executive buy-in and obtain corporate appreciation for compliance work, frequently finding it difficult to get CEOs to listen and to successfully train general team members to understand compliance requirements.

When it comes to outward-facing challenges, DPOs identified a broad and overlapping set of EU regulations as their primary compliance issue, with the AI Act being rated as the most burdensome, followed by NIS2 and the GDPR. Cross-mapping between the GDPR, the AI Act and national laws was specifically highlighted as a critical unmet need. However, the cross-mapping of these overlapping regulatory regimes is positioned as a future priority that will require coordinated efforts beyond the current project scope, potentially in partnership with other regulatory technology initiatives. As a result of this regulatory overlap a set of highly repetitive manual tasks for the different regulations consume a disproportionate amount of time for DPOs. These

tasks include managing Data Subject Access Requests (DSARs), manually deleting data, conducting first-level AI use-case reviews and identifying contradictions across extensive documentation (Workshop 4).

Additionally, the pace of regulatory change poses an additional systemic challenge for SMEs. Keeping up with daily updates, new enforcement decisions and evolving guidelines, particularly at the intersection of technology and law, was described as unmanageable without automated support (Workshop 3).

DPOs were also explicit about the nature of the assistance they sought. Rather than tools that replace professional judgement, participants consistently demanded tools that eliminate procedural burden while preserving human control over decisions with legal consequences (Workshops 3 and 4).

In addition to these operational issues, DPOs presented a different set of internal structural challenges. A recurring theme across the workshops was the difficulty of securing executive buy-in and corporate appreciation for compliance work. DPOs frequently found it hard to get CEOs to listen to them and to successfully train general team members to understand compliance requirements. In most companies, any compliance investment must be justified, proportionate and auditable, which creates further constraints on limited resources (Workshop 3). In larger organisations in particular, obtaining sponsorship for compliance investment was described as especially difficult.

Compounding these internal communication challenges, SMEs were noted to frequently deprioritise compliance entirely, only acting when legally obligated and typically without sufficient budget to do so (Workshop 3). Taken together, these structural deficits point to a systemic gap in the organisational embedding of compliance as a function, a gap that technology alone cannot fully resolve, although the DPOs expressed several suggestions for Trust products that have the potential to significantly ease their burden.

Another structural issue is the late integration of compliance into project workflows. Currently, compliance is rarely embedded in product or project design from the outset. This means that teams have to address privacy and cybersecurity concerns reactively, after key decisions have already been made (Workshop 3). Consequently, embedding compliance at the beginning of every project, rather than as an end-stage reaction, was identified as a design imperative that would reduce risks, save time, and make governance across privacy, cybersecurity, and AI more manageable (Workshop 3 participant).

DPO participants also expressed a strong preference for open architecture, calling for a vendor-agnostic, community-driven solution with native APIs and an open-source format. This solution should be capable of connecting with downstream data sources and audit tools (Workshop 3). In terms of the tool's design, DPOs explicitly demanded that outputs be presented in a way that minimises the risk of uncritically adopting AI-

generated content. This anti-sycophancy principle emerges directly from the recognised tendency of large language models to produce responses that flatter or confirm user expectations. In practice this should influence decisions relating to the communication of confidence levels, the display and verification of citations and sources, the wording of recommendations and how the system responds when a user appears to accept outputs without question. The aim is to create a tool that acts as an intellectual counterpart to the user, rather than simply telling them what they want to hear.

Table 8: DPO's perspective on the current compliance landscape

Survey Question	Finding
DPO Q022: Biggest obstacles to achieving compliance	Documentation & reporting: 4–5/5 Cross-border complexity: 2–3/5 Technology adaptation 3–4/5 SME-specific guidance 4–5/5
DPO Q009: Importance of Feature - Customisable templates for reports	Maximally important (5/5): 38.64% Very important (4/5): 43.18%
DPO Q009: Importance of Feature - Ability to handle multiple regulations	Maximally important (5/5): 65.91% Very important (4/5): 27.27%
DPO Q009: Importance of Feature - Collaboration features	Maximally important (5/5): 25.58% Very important (4/5): 41.86%
DPO Q024: Importance of AI Act compliance	Maximally important (5/5): 68.89% Very important (4/5): 8.89%
Survey Question	Finding
DPO Q024: Importance of Data Governance Act (DGA) compliance	Maximally important (5/5): 12.82% Very important (4/5): 10.26% Moderate (3/5): 35.9%
DPO Q024: Importance of GDPR compliance	Maximally important (5/5): 82.22% Very important (4/5): 13.33%
DPO Q025: Most time-consuming tasks	Monitoring regulatory updates: 31.11% Risk analysis and assessment: 82.22% Generating compliance reports: 68.89% Auditing and internal reviews: 57.78% Ensuring data privacy and security: 48.89%
Workshop finding: Preferred AI task delegation	Document tracking, first drafts, checklists, regulatory monitoring, Data Protection

	Impact Assessment (DPIA) creation, data inventory/processing registry updates]
--	--

2.3.3 Key Requirements

2.3.3.1 Regulatory Compliance Assistant (RCA)

The RCA was ranked as the highest priority tool in the SME workshops on the basis that, if an organisation is unaware of a regulation, none of the other compliance services can offer meaningful assistance (Workshop 1).

Currently, the existing channels for compliance information, such as newsletters, authority websites and AI-generated updates, systematically fail in practice for most SMEs. The information provided by these channels is not pre-filtered for business relevance, is delivered to the wrong people within organisations, and is often ignored due to time constraints and overflowing inboxes (Workshop 1). The fundamental issue is the lack of contextualised, targeted, timely delivery of actionable information.

Table 9: Regulatory Updates

Survey Question	Finding
SME Q006: Most time-consuming task	Monitoring regulations: 67.74%
SME Q007: Tools currently used	Manual spreadsheets/documents: 62.5%
SME Q008: Satisfaction	Mean: 3.19/5
DPO Q025: Most time-consuming tasks	Monitoring regulatory updates: 31.11% Risk analysis and assessment: 82.22% Generating compliance reports: 68.89% Auditing and internal reviews: 57.78% Ensuring data privacy and security: 48.89%

Core Functionality

The service must continuously, i.e. bi-weekly or monthly monitor changes to laws and regulations, translating them into clear, easy-to-understand summaries. Rather than reproducing full legal documents, it should detect new or upcoming changes by comparing previous and updated versions of regulatory documents and then create simple summaries explaining the key changes in plain language. This addresses one of the key pain points for SMEs, namely the difficulty of understanding legal jargon.

To further ease understanding, participants want automated and centralised regulatory update tracking tailored to their company's products, services, and business model (Workshops 1 and 2). Therefore, users of the RCE should be able to manually filter the regulations for which they wish to receive updates or opt in to receiving notifications based on the information provided by uploaded documents.

Notification Design

Although stakeholders were highly specific about how notifications should be delivered, their needs varied greatly depending on their role within the company. Both SMEs and DPOs disliked standard email notifications due to inbox clutter. SMEs preferred the inclusion of notifications in existing workflows, such as Slack, Notion, and Really Simple Syndication (RSS) feeds, to allow for lightweight or customisable integration (Workshops 1 and 2). DPOs, on the other hand, need a flexible, customisable notification system with a centralised dashboard and the ability to opt in to specific laws and geographic jurisdictions (Workshops 3 and 4).

However, for both groups, updates should be categorised by degree of importance (high, medium or low) and focus on differences and changes only. Rather than sending full documents, there should be user-level configuration of detail depth.

Storage and Continuity

Permanent storage, such as a knowledge base, wiki or Slack archive, was specifically recommended by SMEs in Workshop 2 to prevent knowledge loss during staff absences or turnover. This addresses the structural vulnerability whereby compliance responsibility is often managed by a single individual who has to manually sift through documents, taking time away from core activities.

Scope and Coverage

The breadth of regulations identified across both survey respondents and workshop participants confirms that the tool must accommodate a wide and overlapping regulatory portfolio. GDPR emerged as the highest-priority regulation, rated at maximum importance by 82.22% of DPO survey respondents, while further regulations including NIS2, the Digital Operational Resilience Act (DORA), the Data Act, the Cyber Resilience Act (CRA), the Corporate Sustainability Reporting Directive (CSRD), the European Health Data Space Regulation (EHDS) and the EU Omnibus were consistently cited as burdensome across workshops (Workshop 3 and 4).

National laws represent an additional mandatory layer of scope, with respondents explicitly identifying Spanish legislation as relevant alongside EU frameworks. Cross-mapping, especially of GDPR, AI Act, NIS2 and national laws was highlighted as a critical unmet need, as the regulations are written separately but heavily influence one another, creating compliance gaps that cannot be addressed in isolation. As of now, a cross-mapping this extensive is beyond the boundaries of the current project scope. While its value to compliance professionals is clearly evidenced by the findings, it is acknowledged as a priority area for future development and collaboration across the broader regulatory technology landscape.

Table 10: Regulatory Scope

Survey Question	Finding
DPO Q024: Importance of AI Act compliance	Maximally important (5/5): 68.89% Very important (4/5): 8.89%
DPO Q024: Importance of GDPR compliance	Maximally important (5/5): 82.22% Very important (4/5): 13.33%
DPO Q024: Importance of NIS2 compliance	Maximally important (5/5): 43.9% Very important (4/5): 34.15%
DPO Q024: Importance of DORA compliance	Maximally important (5/5): 21.62% Very important (4/5): 16.22% Not important (1/5): 35.14%
DPO Q024: Importance of Data Act compliance	Maximally important (5/5): 21.95% Very important (4/5): 17.07% Moderate (3/5): 41.46%
DPO Q024: Importance of CRA compliance	Maximally important (5/5): 26.32% Very important (4/5): 26.32% Not important (1/5): 21.05%
DPO Q024: Importance of EHDS compliance	Maximally important (5/5): 11.11% Very important (4/5): 16.67% Not important (1/5): 44.44%
DPO Q024: Importance of DGA compliance	Maximally important (5/5): 12.82% Very important (4/5): 10.26% Moderate (3/5): 35.9%
Survey Question	Finding
DPO Q024: Other regulations	Spanish national laws (the Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), LSSI-CE)
DPO Q022: Challenge of Cross-border complexity	2–3/5
Workshop finding: Most burdensome regulations overall	AI Act, NIS2, GDPR, DORA, Data Act, CRA, CSRD, EHDS, EU Omnibus

2.3.3.2 Regulatory Obligations Analyser (ROA)

Across the workshops, the ROA was widely accepted as a valuable tool for translating complex legal language into actionable, auditable criteria. Participants, especially SMEs, consistently emphasised the importance of translating legal text into accessible, plain language. This is not just a stylistic preference, but a functional requirement for compliance work. It enables non-DPO participants to understand and fulfil their regulatory obligations, as understanding legal jargon is one of their key obstacles.

For DPOs, however, the value proposition of the ROA is somewhat different. Rather than grappling with the interpretation of legal text, DPOs are confronted with the challenge of implementing that interpretation across their organisations.

Table 11: ROA

Survey Question	Finding
SME Q010: Most valuable TRUST tool	Compliance gap analysis and scoring (RCE): 53.13%
SME Q016: Tasks to hand over to AI	Monitoring and tracking regulatory updates: 100%; Automating repetitive and time-consuming tasks: 100%
SME Q005: Biggest obstacles	Understanding legal jargon: 68.75%

Plain-Language Translation

The ROA should function as both a reference encyclopedia and an interactive chatbot for non-binding compliance queries. It should translate legal texts into clear, visual, concise action lists that include infographics with concrete examples explaining why specific regulations apply (Workshop 2).

While the value of such visual communication tools is clearly recognized, the development of infographics falls outside the current project scope and is identified as a feature to be considered in future iterations of the platform.

As a key UX feature, a quick-toggle button allowing users to switch between the official legal text and the simplified version was requested (Workshop 1).

Personalisation and Contextualisation

Since most SMEs rely on a single person to manage complexity under immense structural resource deficits (see 2.3.2), it is paramount for the ROA to provide individualised examples based on specific company profiles, rather than generic explanations, to foster understanding.

Additionally, displaying legal sources in plain language, as outlined in 2.3.2, and providing explanations of why a requirement does or does not apply to the user's organisation are central requirements to enhance trust.

Obligation Management

In Workshop 3, the DPOs explicitly requested that the ROA automatically generate obligation registers, set clear deadlines, establish risk scoring, assign task owners, and provide checklists. These should facilitate internal workflows and ease internal communication when it comes to compliance requirements.

They specified that a core feature should be an automated obligation register with cross-mapping between the GDPR, the AI Act and national laws, accompanied by clear deadlines, risk scoring, assigned owners, evidence templates and practical action checklists.

Some participants of Workshop 3 also requested a 'one-click' analysis of existing documentation and assistance in maintaining a data inventory register for DPIAs and data breach tracking.

Table 12: LRA

Survey Question	Finding
DPO Q028: Ability to demonstrate accountability in disputes	Maximally important (5/5): 52.5% Very important (4/5): 20%
DPO Q028: Increased customer trust	Maximally important (5/5): 39.02% Very important (4/5): 24.39%
DPO Q028: Competitive differentiation	Maximally important (5/5): 12.82% Very important (4/5): 28.21% Moderate (3/5): 33.33%
DPO Q022: Costs (financial resources required for compliance)	Maximally challenging (5/5): 13.33% Less important (2/5): 31.11%
DPO Q022: Time burden of compliance activities	Maximally challenging (5/5): 27.27% Very challenging (4/5): 45.45%
DPO Q009: Automated monitoring of compliance status	Maximally important (5/5): 43.18% Very important (4/5): 36.36%
Survey Question	Finding
DPO Q009: Customisable dashboards for tracking compliance metrics	Maximally important (5/5): 25% Very important (4/5): 43.18%
DPO Q029: Open-ended benefits of showcased compliance	"Would strengthen the organisation's credibility as a legal and privacy advisory provider, support client due diligence, improve the traceability of professional

	decisions, and reduce reputational and liability risks"
--	---

2.3.3.3 Legal Risk Analyser (LRA)

The LRA was well received across all workshops for its proactive risk management function, with quarterly notifications suggested as a practical default. DPO participants in particular require tools to help them visualise legal risk in order to communicate more effectively with management and justify compliance measures (Workshop 3). This is reflected in the survey's rating of accountability demonstration as maximally important, and the qualitative open-ended responses explicitly linking compliance visibility to liability reduction and credibility confirm the broader strategic framing of compliance as a financial and reputational risk management tool.

Specifically, the DPOs highlighted the demand for financial risk quantification to be used as a compliance tool (Workshop 3). In their experience, boards and executives respond better to financial than legal arguments when discussing compliance risks. Therefore, the tool should calculate the total cost of realistic data breaches, which often exceed regulatory fines, and present this information visually in a 'one-pager' or heat map. The need for executive-facing risk communication tools is not present in SME-focused workshops, where the participants are the decision-makers themselves.

Visual Risk Communication

The SME participants asked for an easy-to-read three-stage traffic light system (green/yellow/red) to visually communicate the highest penalties or compliance risks at a glance.

DPOs on the other hand require a more detailed dashboard displaying compliance percentages alongside the colour-coded traffic light scoring system mapping directly to required remedial actions.

Financial Impact Quantification

Calculation of the financial impact of risks, like the cost of data breaches, was specifically requested to help compliance professionals justify compliance budget allocations to management.

Risk Prioritisation Logic

Risk scoring should consider legal impact, deadlines, risk level, sector relevance and whether immediate action is required.

Risk-scoring models directly mapped to specific (AI) use cases and compliance management system (CMS) tracking were requested, particularly by DPO workshop participants (Workshop 3).

Enforcement Intelligence

From the DPOs' perspective, the ideal tool would be a comprehensive fines tracker that covers all relevant EU data regulations, equivalent to the GDPR Enforcement Tracker, but expanded to include the AI Act, NIS2, CRA, and related frameworks.

2.3.3.4 *Regulatory Checker / Evaluator (RCE)*

The RCE was described as highly valuable, particularly when it can analyse actual company data to identify specific compliance gaps in existing documentation. Participants of all workshops generally agree that the AI should collect standardised information via a guided questionnaire, generate a structured draft, and submit it to a human reviewer who makes the final decision. Overall, there is agreement on a two-tier compliance gap evaluator: first, a brief, scored summary, followed by a detailed, action-oriented report with legal sources.

The importance of preserving human understanding throughout this process was made explicit by one SME survey respondent: "I'm all for AI tools that help me locate and/or understand legal texts. It's also fine to have AI tools scan full-text sources and pre-fill forms. However, if I need to sign anything, I'd like to see the form inputs and understand what I'm submitting there. Please do not build a tool that black-boxes me out of the decision loop" (SME Survey).

Gap Identification and Text Proposal

The RCE should not only identify gaps, but also actively propose concrete modifications to the text. For example, if it has access to a document repository, it should identify missing paragraphs in a privacy policy and draft the replacement text to be inserted (Workshop 1).

Visual Communication of Compliance Status

Participants expressed a strong preference for a highly visual presentation of compliance gaps to facilitate easy communication between DPOs and non-specialist stakeholders (Workshop 3). For their own use, DPOs requested a dashboard displaying compliance percentages alongside a colour-coded, visual traffic light scoring system that maps directly to required remedial actions (Workshop 4). Ideally, the RCE and LRA could use the same or similar designs to make the transition from generalised legal risks to company-specific compliance evaluations as smooth as possible, enabling an understanding of how these two areas are connected.

2.3.3.5 *Regulatory Reports assistant (RRA)*

The survey and workshop findings both indicate that report generation is a highly demanded feature. The moderate AI-control score is consistent with the workshop observation that many users want substantial AI assistance without relinquishing human authorship or review. Across the available evidence, DPOs and SMEs show willingness to use AI for report drafting alongside a strong preference for human oversight. The findings therefore support structured AI assistance within a human-

authorised process, while the precise degree of automation should remain configurable and subject to further validation (see Section 2.3.2).

Participants have different views on how much control should be delegated to AI in reporting, both between and within the DPO and SME groups according to personal preferences. One participant prefers full automation (“click and done”, Workshop 3), while another prefers concise AI summaries with tags and references that retain human authorship (Workshop 1). A third participant recognises that reporting is a multi-phase process (Workshop 1). The tension between these differing expectations, efficiency, and control is a key design consideration.

DPO Participants as expected articulate highly sophisticated reporting requirements that reflect their professional contexts. These reports must be configurable according to the target audience (supervisory authorities versus corporate stakeholders) (Workshop 3) and incorporate version control and audit trails (Workshop 4). They should also include Capability Maturity Model scoring to track compliance progression (Workshop 3). Reports must serve both expert compliance personnel and non-compliance audiences. These requirements significantly exceed the report generation preferences expressed in the SME workshops.

In terms of reporting, desired features include one-click generation of an executive facing summary, Transfer Impact Assessment (TIA) analysis across multiple regulations, per-country Fundamental Rights Impact Assessment (FRIA) analysis of fundamental rights, and AI-backed drafting support that does not replace the human assessor. Automated DPIA completion is the most desired feature by far — a highly specific, expert-level requirement entirely absent from SME group discussions.

Table 13: RRA

Survey Question	Finding
DPO Q009: Automated DPIA/TIA/FRIA completion	Maximally important (5/5): 46.51% Very important (4/5): 39.53%
DPO Q009: Customisable templates for reports	Maximally important (5/5): 38.64% Very important (4/5): 43.18%
DPO Q025: Most time-consuming tasks	Generating compliance reports (DPIA, TIA, FRIA):
Survey Question	Finding
DPO Q009: Automated document completion (DPIA, TIA, FRIA)	Maximally important (5/5): 46.51% Very important (4/5): 39.53%
DPO Q010: Most valuable TRUST tool	Risk scoring and legal data analysis (LRA): 66.67%

DPO Q016: Tasks to hand over to AI	Generating compliance reports (DPIA, TIA, FRIA): 86.67%
SME Q012: Desired level of AI control over compliance workflow	Mean: 3.31 / 5
SME Q015: Trust without human oversight	No 53.13%
SME Q018: Trust mechanisms	Human-in-the-loop: 87.5%

Guided Report Creation

As mentioned in the previous section, the workshops revealed a genuine and productive tension between automation and control that the tool design must accommodate. The convergent requirement resolves this tension: Creation of reports via a guided questionnaire completed by the DPO or other authorised user, incorporating evidence and recommendations, followed by a mandatory human review before finalisation. The questionnaire should feature interactive links to source materials for further verification. This approach has the advantage of being accessible for SMEs, who often do not have the resources to write reports, while also supporting DPOs without limiting their autonomy.

Rather than writing final reports autonomously, the tool should surface best practice knowledge and highlight inconsistencies, serving as a reliable backup draft.

Audience Customisation and Documentation

The tool should enable users to select their target audience (e.g. supervisory authorities vs. corporate stakeholders) and automatically adjust the content and tone accordingly. DPOs especially request a “one-click” executive summary report with built-in evidence and recommendations to ease internal communication (Workshop 3).

They also request version control, audit trails, obligation mapping and clear summaries showing risks, actions, owners and deadlines to be part of the RRA (Workshop 4). It is also important to note that the reporting interface should accommodate the entire lifecycle of reporting and its various phases (Workshop 1).

2.3.3.6 Certification Process Assistant (CPA)

The CPA was described as a helpful bridge for communication with auditors and certification authorities, simplifying the certification preparation process.

Human-in-the-loop as a Non-Negotiable

The most emphatic requirement for the CPA was that human review was absolutely mandatory, since the human compliance manager remains ultimately liable. Participants in both DPO workshops strongly agreed that the CPA must have clearly defined boundaries and capabilities, and that AI-generated outputs must never be

presented as final or legally authoritative (Workshops 3 and 4). Participants specifically requested an explicit acknowledgement that AI-generated information may not always be complete or fully accurate.

To build trust, the tool must feature verifiable evidence and source citations with validation links, accurate timestamps indicating when legislation was last reviewed or updated, and a clearly visible human-in-the-loop review process at all times (Workshop 3). Furthermore, participants noted that under frameworks such as the AI Act, organisations cannot easily deflect liability by simply stating that content is AI-generated. This makes the traceability and auditability of every certification output a legal necessity rather than a design preference (Workshop 3).

Certification Readiness Tracking

A simple checklist of requirements to tick off for certification processes was specifically requested for less sophisticated users, especially SMEs (Workshop 2). Professional DPOs, on the other hand, require real-time evidence collection, continuous monitoring, and automated checklist tracking to streamline the certification process end-to-end (Workshop 4).

Participants from both groups suggest automated gap analyses displaying completion rates alongside clear explanations of missing items, as well as a 'certification readiness score' supported by auto-generated evidence portfolios (Workshop 4). Wizards, interpretation detail checklists, and maturity assessments tailored to the specific certification being targeted were additionally requested, with particular emphasis on a maturity check that dynamically adapts based on which certification the organisation is aiming for (Workshop 3).

Participants also emphasised the importance of a direct feedback loop. The CPA should assess submitted applications and provide clear, actionable feedback, explaining why an application might be rejected. This will enable compliance teams to learn from the audit process and make iterative improvements (Workshop 3). The accreditation process for DPOs was identified as being especially time-consuming, and automating the initial assessment of whether applications are accepted or not was seen as a way to significantly increase efficiency (Workshops 3 and 4). Further requested as standard features to support end-to-end process management were visual progress updates and document tracking with deadline reminders (Workshops 3 and 4).

Target Certifications

When it comes to certifications, participants' companies are currently prioritising International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 42001 (AI management systems) and ISO/IEC 27001 (information security management), with some also focusing on sustainability statement requirements (Workshop 4).

Additionally, the European Data Protection Seal under Article 42 of the GDPR was identified as a core certification objective, given its direct relevance to the CPA's primary user base of Data Protection Officers (DPOs) and legal compliance professionals (Workshops 3 and 4).

The American Institute of Certified Public Accountants / Canadian Institute of Chartered Accountants (AICPA/CICA) Privacy Maturity Model (PMM) was also raised as a relevant framework, reflecting the need for the tool to accommodate internationally recognised privacy programme assessments alongside EU-specific certifications (Workshop 4).

Table 14: CPA - Target Certifications

Certification / Framework	Scope
ISO/IEC 42001	AI management systems
ISO/IEC 27001	Information security management
ISO/IEC 27000 (series)	Information security (noted as not initially listed but explicitly requested)
European Data Protection Seal	GDPR compliance certification for products and services
AICPA/CICA Privacy Maturity Model (PMM)	Privacy programme assessment and maturity benchmarking
Sustainability statements / CSRD-aligned reporting	Corporate sustainability reporting and Environmental, Social, and Governance (ESG) disclosure
Pan-European certification (proposed)	The ideal certification would be a cross-border certification recognised by public authorities and regulatory agencies across EU member states.

2.3.4 Validation Needs

Regulatory Compliance Assistant (RCA)

The RCA must be tested for its ability to deliver timely, relevant and correctly filtered regulatory updates, validated against user-level notification preferences, and confirmed integration with existing workflow tools such as Slack, Teams and RSS feeds. While integration across a wide range of platforms is a desirable long-term goal, it is not feasible to incorporate every notification platform within the current project scope. The initial focus will therefore be placed on email as the primary notification channel, given its universality and ease of implementation. Subject to available resources, notification support will be progressively extended to the most frequently

requested platforms, prioritizing those that emerge as highest in demand among the project's target user groups.

Regulatory Obligations Analyser (ROA)

The ROA must be validated on its ability to produce accurate, plain-language translations of legal texts, with systematic spot-checks against original legal sources to confirm fidelity and completeness.

Legal Risk Analyser (LRA)

The LRA must be tested for the accuracy of risk scoring and financial impact calculations, benchmarked against known fines and enforcement decisions in the GDPR Enforcement Tracker and equivalent datasets.

Regulatory Evaluator (RCE)

The RCE must be tested for its ability to correctly identify compliance gaps, using company data, and for the quality and accuracy of its proposed text modifications against verified expert outputs.

Regulatory Reports assistant (RRA)

The RRA must be validated for output quality and completeness of AI-generated reports, with human reviewers assessing whether reports can reliably serve as backup drafts. The reports must be validated for their coverage of TIA multi-regulation analysis and FRIA country-level fundamental rights mapping.

Certification Process Assistant (CPA)

The CPA must be tested for the accuracy of gap analyses and readiness scores, and specifically whether auto-generated evidence portfolios meet real auditor and certification body expectations.

Legal compliance of the tool itself

The legal and local requirements compliance of the OPRCS platform must be addressed proactively during development and verified before release.

Usability as a validation criterion

The complexity of the system and the use of English terminology must not put off medium-sized customers. UX simplicity is an explicit, testable acceptance criterion, not just a design aspiration.

2.4 Pillar 3: Requirements for Seal of Trust Certification Schemes

2.4.1 Objective

This chapter aims to define the requirements of end users and stakeholders for the Seal of Trust certification schemes. Based on focus group workshops and surveys with DPOs and SMEs, it identifies the functional, methodological and market positioning requirements that any viable certification scheme must fulfil. These requirements apply to both the omnibus and generic models.

2.4.2 Stakeholder Input

Motivation for Certification

Workshop participants are actively pursuing a variety of certifications. DPO participants described these compliance certifications as serving multiple strategic functions, such as building market trust, protecting reputation, securing internal buy-in and maintaining accountability. The three main reasons that were ranked were accountability, competitive advantage, and market trust (Workshop 4).

However, participants candidly admitted that organisations are generally only willing to invest in voluntary certification when they expect tangible competitive or procurement benefits, and when the certification is endorsed by a recognised market authority (Workshop 4). Participants in matrix structures face particular difficulty in securing internal sponsorship for certification investment (Workshop 3). Notably, willingness to invest varies significantly by certification: participants indicated focused allocation of resources towards ISO/IEC 42001 and ISO/IEC 27001 specifically, with some additionally prioritising sustainability statement requirements. Broader or less strategically relevant certifications attract little organisational commitment (Workshop 4).

Table 15: Motivation for Certifications

Certification / Framework	Scope
DPO Q028: Motivation for Certification - Demonstrate accountability in disputes	Maximally important (5/5): 50% Very important (4/5):30.56%
DPO Q028: Motivation for Certification - Competitive differentiation	Maximally important (5/5): 13.51% Very important (4/5): 27.03% Moderate (3/5): 35.14%
DPO Q028: Motivation for Certification - Access to new business partnerships	Maximally important (5/5): 13.51% Very important (4/5): 18.92% Moderate (3/5): 32.43%

Survey Question	Finding
DPO Q028: Motivation for Certification - Easier participation in public tenders and procurement	Maximally important (5/5): 10% Very important (4/5): 22.5% Moderate (3/5): 37.5%
DPO Q028: Motivation for Certification - Faster regulatory audits	Maximally important (5/5): 34.15% Very important (4/5): 31.71%
DPO Q028: Motivation for Certification - Increased customer trust and confidence in data practices	Maximally important (5/5): 39.02% Very important (4/5): 24.39%
DPO Q028: Motivation for Certification - Improved data quality leading to better business decisions	Maximally important (5/5): 25% Very important (4/5): 35%
DPO Q028: Motivation for Certification - Access to data spaces, platforms and systems	Maximally important (5/5): 10.53% Very important (4/5): 28.95% Less important (2/5): 28.95%
DPO Q028: Motivation for Certification - Simplified cross-border operations within the EU	Maximally important (5/5): 22.5% Very important (4/5): 22.5%
DPO Q028: Motivation for Certification - Increased employee confidence in internal data handling	Maximally important (5/5): 20.51% Very important (4/5): 33.33% Moderate (3/5): 25.64%
DPO Q029: Open-ended benefits of showcased compliance	"Would strengthen the organisation's credibility as a legal and privacy advisory provider, support client due diligence, improve the traceability of professional decisions, and reduce reputational and liability risks"

Pain Points in Certification Workflows

Current certification processes are perceived by SMEs as opaque and complex. The desire for a simple checklist of requirements reflects how inaccessible existing certification pathways are for SME users (Workshop 1).

Classification challenges are an additional structural issue: determining whether a company or product falls under a specific regulation or qualifies for exemptions (e.g. under the AI Act) was described as “highly complex” (Workshop 2).

2.4.3 Key Requirements

2.4.3.1 Consolidated Regulatory Scope

As participants noted in Workshop 4, compliance certifications serve to “build market trust, protect reputation, secure internal buy-in and maintain accountability”. They believe that these functions are best served by a unified, pan-European certification

standard recognised by public authorities and regulatory agencies, rather than a patchwork of individual national or sector-specific certifications (Workshop 3).

Participants were clear about the regulatory and certification scope they expect the tool to address. Stakeholders confirmed that they are actively pursuing ISO/IEC 42001 (AI management systems) and ISO/IEC 27001 (information security management), with some also focusing on sustainability statements and CSRD-related reporting requirements (see Table 14: CPA – Target Certifications).

2.4.3.2 *Certification Methodology*

The developed criteria must then be operationalised into a certification readiness framework and validated against the expectations of real auditors and the criteria of formal certification bodies. This multi-stage validation process is a stakeholder requirement in itself: participants will not trust a certification scheme whose criteria have not been demonstrated to have survived independent legal and practical scrutiny (Workshop 3).

Participants specifically requested that the certification methodology include simple checklists with yes/no options, legal sources and plain-language explanations of why requirements apply or do not apply, including exclusion logic (Workshop 3). While the intent to provide accessible and actionable compliance outputs is acknowledged, strictly binary yes/no responses are not feasible from a criteria-drafting methodology perspective, as the complexity of regulatory requirements rarely allows for such absolute determinations. The Seal of TRUST certification outputs will therefore aim to deliver well-reasoned and clearly communicated conformity assessments, ensuring transparency and legal grounding without creating unreasonable expectations regarding the nature of compliance evaluation.

For less sophisticated users, particularly SMEs, it was described as the minimum viable interface to have a straightforward checklist of requirements to tick off (Workshop 4). SME survey respondents reinforced this need: 68.75% identified the complexity of regulations and legal jargon as the main obstacle to achieving compliance, while 65.63% cited a lack of clear guidance or best practices (see Table 7: SMEs' perspective on the current compliance landscape).

2.4.3.3 *Market Recognition*

A recurring requirement across the DPO workshops was that the omnibus scheme must have genuine market recognition. Participants noted that organisations were motivated to pursue certifications such as the Europrivacy Certification because of its pan-European recognition (Workshop 3). The tool should establish a highly accessible, trusted and unified baseline across Europe that actively prevents weak links in supply chains (Workshop 3).

This is not merely a quality target, but also a strategic positioning requirement to motivate SMEs to pursue it (Workshop 3). DPO participants candidly admitted that voluntary certification is only pursued when tangible benefits are expected, such as

strengthening a competitive position or winning public tenders (Workshop 3). Therefore, the omnibus scheme cannot be designed in isolation from market and procurement realities; it must be positioned from the outset as a supply-chain trust anchor, not just a compliance tick-box exercise.

2.4.3.4 Cost, Accessibility, and the SME Constraint

Perhaps the most practically significant cross-cutting requirement is cost and accessibility for SME users. As participants noted in Workshop 3, "SMEs in particular often do not prioritise compliance and only act when obliged, typically without large budgets". Cost-effectiveness was rated 5/5 by 46.88% of SME survey respondents, indicating that the certification process must be financially viable for organisations without dedicated compliance budgets. This resource constraint means the certification process must be realistic for a single compliance officer in an SME to complete without extensive external support. The word cloud showing the top motivations for compliance certification confirms that SMEs are motivated to certify, but only if the process is proportionate to their resources and delivers tangible, recognised outcomes.

Table 16: SME Constraint for Certifications

Certification / Framework	Scope
SME Q009: Features of a compliance tool – Cost effectiveness	Maximally important (5/5): 46.88% Very important (4/5): 18.75%
SME Q009: Features of a compliance tool - User-friendly interface and ease of use	Maximally important (5/5): 48.39%; Very important (4/5): 25.81%; Moderate (3/5): 19.35%
SME Q005: Biggest obstacles to achieving compliance	Complexity of regulations and legal jargon: 68.75%; Lack of clear guidance or best practices: 65.63%; Time-consuming manual processes: 62.5%; Lack of internal expertise: 40.63%
Workshop finding: Top motivations for certification (word cloud)	Trust, Transparency, Competitive Advantage, Building Trust, Customer Reassurance, Customer Requirement, ESG Rating, Winning Contracts, Reputational Enhancement, "Being on the Safe Side"

2.4.4 Validation Needs

Supply-Chain and Procurement Recognisability

Is the Seal of Trust recognised by public procurement authorities, platform operators, and supply-chain gatekeepers? Validation requires formal engagement with at least a representative sample of procurement bodies and platform operators to confirm that the scheme's criteria and branding meet the threshold for acceptance in tender and onboarding processes.

Auditor validation

The readiness score and evidence portfolio features must be validated against real auditor expectations and formal certification body criteria before release.

Practicality

Can a single certification body in an SME realistically complete the certification process without extensive external support? This is a formal validation criterion for both the omnibus and generic model.

Usability

Certification tools must be accessible to non-expert users, including medium-sized companies unfamiliar with complex English technical terminology. Simplicity of UX is a formal test criterion.

3. Results / findings

3.1 Prioritized End-User and Stakeholder Requirements

3.1.1 Objective of the Section

This section provides a concise synthesis of the requirements-elicitation results. Survey findings and workshop themes were reviewed separately and then compared during interpretation. Where the two evidence strands converge, the report treats this as stronger support for a requirement within the available samples. Where they diverge, tensions are explicitly documented. The purpose is to prioritise design inputs and identify areas requiring further validation, not to claim statistical representativeness or a standalone qualitative research outcome.

3.1.2 Prioritized Key findings

Transparency, Human Oversight, and AI Architecture

Stakeholder groups converged on a fundamental requirement: AI must support human decision-making rather than replace it. SME participants prioritized pragmatic verification mechanisms (source links, confidence scoring), while DPO participants articulated a comprehensive legal and architectural framework encompassing

verifiable sources with timestamps and audit trails. Notably, DPOs argued that AI Act disclaimers alone are insufficient for liability deflection (see 2.2.2).

LLM Reliability and AI Output

Reliability concerns were grounded in participants' professional experience rather than abstract technical concerns. Survey data support the prominence of this issue within the respondent samples: 78.13% of SMEs and 82.61% of DPOs cited hallucinations as a primary concern. Workshop participants additionally requested transparent source citations, version control, and update timestamps. Together, these findings support a requirement for verifiable and traceable outputs, while legal interpretations raised by participants should be validated through the project's dedicated compliance work.

Automation of repetitive tasks

Automation of repetitive tasks emerged as one of the highest-priority capability areas across the consulted groups. Quantitative results show strong demand for monitoring, report generation, risk scoring, and related repetitive tasks. Workshop data add an important distinction: general users primarily want automation to reduce burden, while expert users want it to handle routine complexity and preserve their capacity for judgement-intensive work. This supports layered functionality and role-sensitive configuration as a design direction to be tested in subsequent co-design phases.

Table 17: Convergence of End-user's needs

Dimension	Quantitative Finding	Qualitative Theme
Hallucination concern	SME: 78.13%; DPO: 82.61%	Custom AI workarounds; source-citation verification practices
Transparent, verifiable AI output	83.33% trust condition	Source links; confidence scoring; anti-sycophancy
Human-in-the-loop oversight	86.67% trust condition	Legal non-delegability; AI Act Article 14
AI Acceptance (conditional)	SME Mean 3.75; DPO Mean 3.73	Acceptance under accountability conditions, not unconditional rejection
Data privacy and confidentiality	SME 64.52% 5/5; DPO 78.57% 5/5	GDPR self-compliance; no training without consent
Self-referential compliance	Not directly measured	Tool must comply with the standards it enforces
Audit trails and accountability	70% trust condition	Immutable logs; version control; traceability of professional decisions

Multi-regulation handling	SME 23.91% 5/5; DPO 65.91% 5/5	AI Act/GDPR/NIS2 cross-mapping as critical unmet need
Open/sovereign infrastructure	Not directly quantified	Primarily expert users; LLM-agnostic and EU-sovereign architecture

Conflicting Needs

The difference in opinion between SME users and expert compliance professionals (DPOs and legal consultants) is not just a matter of degree; it reflects two fundamentally different mental models of what a compliance tool should be (see 2.3.2).

SME participants consistently defined success in terms of radical simplification. The primary concern of SME participants was cognitive accessibility rather than analytical depth: they wanted legal texts to be translated into plain, understandable language with clear, step-by-step instructions (Workshops 1 and 2).

DPO participants, however, defined success in exactly the opposite terms. They required a tool capable of generating cross-framework obligation registers, automating DPIAs, TIAs and FRIAs, and deploying CMM scoring to assess organisational readiness across multiple regulatory dimensions simultaneously.

These needs may be difficult to reconcile within a single undifferentiated interface. Designing primarily for one profile could reduce usability or usefulness for the other. The findings therefore support testing a layered or role-adaptive platform design that exposes additional complexity where the user profile and task require it. This remains a design hypothesis to be validated through prototype testing rather than a fixed architectural conclusion.

Table 18: End-user's conflicting needs

Dimension	SMEs	DPOs
Relationship to compliance	External obligation to be managed efficiently; only acted upon when legally required and typically without large budgets	Primary professional identity and legal responsibility; tool must support expert capacity without replacing legal judgement
Compliance role conception	Offload compliance entirely; minimise user engagement; compliance managed by single individual diverting time from core business	Support expert capacity with precision tooling; offload repetitive tasks while retaining final legal judgement
Primary regulatory concern	GDPR experienced as vague, burdensome, and disproportionate; even minor B2B tasks trigger compliance overhead	AI Act rated most burdensome; entire EU regulatory portfolio managed simultaneously; cross-

		mapping between frameworks is a critical unmet need
Operational pain points	Information overload and lack of relevance; knowledge loss during staff turnover; compliance responsibility passed between departments; resource target of max. two hours per month	Bogged down by manual busy-work; early-stage integration failures; compliance treated as afterthought rather than by-design
Organisational challenge	Resource and knowledge deficits; person-dependent, improvised processes; difficulty knowing which regulations apply and what exemptions exist	Coordination complexity across distributed and international teams; difficulty securing executive buy-in;
Definition of success	A "one-pager" or structured checklist any employee can act on immediately; pre-made forms handed out before laws enter into force	Automated data mapping and monitoring; actionable obligation registers; sovereign and open-source infrastructure that guarantees data protection
Dimension	SMEs	DPOs
Most desired tool	Regulatory change notification ranked 1st by large margin and was described as essential to avoid relying on "luck" for updates	Risk scoring and document management ranked joint first in W3; Automated monitoring ranked first but closely followed by risk scoring and document management in W4
Infrastructure preferences	Basic integrations (Slack, Teams, Comma-Separated Values (CSV), RSS); low-friction, embeddable in existing workflows; open-source licensing raised as a question but not a design demand	Open-source, vendor-agnostic, LLM-agnostic, EU-sovereign architecture; tool must be runnable on self-hosted models; downstream-connectable via native APIs; community-driven with open architecture
Language and accessibility	Plain-language translation is a minimum requirement; English technical terminology flagged as a deterrent for medium-sized companies; yes/no checklists with exclusion logic essential	Plain language also valued for sharing outputs with non-compliance personnel, but secondary to analytical depth and configurability
Cost and scalability	Cost-effectiveness rated 5/5 by 46.67% of SME respondents; scalability to accommodate business growth rated 5/5 by only 20% — immediate utility	No equivalent cost constraint expressed; investment framed around professional accountability,

	outweighs long-term architectural concerns	liability deflection, and operational risk of inadequate tooling
Preferred notification channel	Slack and Microsoft Teams strongly preferred over email; RSS feeds for lightweight integration; customisable output formats (e.g., CSV)	Centralised dashboard as primary interface; direct email for high-priority changes only; opt-in scope tailoring by country, sector, and specific law; push notifications via platform as additional channel
Certification engagement	Rarely raised spontaneously; when mentioned, motivated by market recognition, winning contracts, and competitive advantage rather than internal compliance culture	Strategic and specific: ISO/IEC 42001 and ISO/IEC 27001 actively targeted; certification readiness score and auto-generated evidence portfolios explicitly requested; feedback loop on rejected applications demanded

3.1.3 Gaps in Requirement Coverage

Sector-specific regulatory needs

Participants from healthcare, finance, transportation, and chemical industries identified highly domain-specific obligations like DORA, the Swiss Financial Market Supervisory Authority (FINMA), the European Health Data Space Regulation, that require dedicated coverage beyond the current instrument design. The limited representation of these sectors reduces the generalisability of current findings for regulated industries.

Large enterprise and in-house compliance functions

The expert survey sample was skewed toward consultancy roles. In-house compliance functions within large enterprises and public sector bodies remain underrepresented, creating a gap in understanding their tool requirements and governance constraints.

Technical integration depth

While integration with existing tools was rated positively, the specific technical integration requirements like APIs, data models, workflow triggers, and identity management remain unspecified and require dedicated elicitation in subsequent phases.

Engineers and medical research professionals

The Engineers and Medical Research Use Case is scheduled to begin at M13 as defined in the project proposal. Requirements specific to sector regulations such as the European Health Data Space (EHDS), the Medical Device Regulation (MDR), and the In Vitro Diagnostic Regulation (IVDR) are therefore not represented in the current phase. Their inclusion in subsequent requirement-gathering and validation activities will be essential for ensuring the TRUST platform addresses the compliance needs of the biomedical engineering sector.

3.2 Challenges and Lessons Learned

3.2.1 Challenges Faced During Requirement Gathering

Stakeholder availability and sample representativeness

Both the general and expert survey samples were limited in size, and the expert survey was particularly constrained and skewed toward consultancy professionals. This reduced the representativeness of roles across diverse sectors and organisation sizes. Focus group participation was similarly constrained for certain segments, limiting the depth of structured discussion available for triangulation with survey data.

Structural complexity of compliance as a domain

The requirement gathering process itself surfaced a core challenge: compliance is not a single domain but an intersecting set of organisational, informational, legal, and technical problems. Qualitatively, this translated into difficulty capturing requirements at the right level of abstraction: requirements that are appropriate for a novice user (plain-language summaries) are qualitatively different from those appropriate for a DPO (cross-framework FRIA mapping), yet both emerge from the same underlying compliance burden.

Conflicting priorities between participant groups

The divergence between SME users seeking simplified automation and expert users demanding professional-grade infrastructure created genuine tension in requirement prioritisation during workshops. This tension could not be fully resolved within the current phase and requires explicit architectural mediation in subsequent design phases.

Fundamental scepticism from a minority of participants

A minority expressed fundamental scepticism about whether AI-based tools could deliver on stated goals. One respondent noted: "I'm very pessimistic that an AI-based tool could reach the targets you describe. My experience over the last years is that every effort to less bureaucracy achieves the opposite." While not representative of the majority, this view signals the importance of expectation management and the need for demonstrable early-stage value delivery.

3.2.2 Unresolved Issues Requiring Input from Other Work Packages

Anti-sycophancy UX and human-in-the-loop oversight (WP2/WP3):

The expert-level requirement for anti-sycophancy design and multi-layered human-in-the-loop oversight requires dedicated technical specification and implementation design beyond the scope of requirement gathering.

Cybersecurity and Regulatory Compliance by Design (WP1/WP2)

Embedding cybersecurity and regulatory compliance principles directly into the system design requires the establishment of a dedicated guideline and framework. This

includes identifying regulatory and security baselines and mapping compliance safeguards to architecture components.

3.2.3 Improvements for Future Phases

Iterative joint display validation:

Following the joint display methodology, requirements captured in this phase should be validated iteratively through integrated quantitative/qualitative instruments as technical prototypes become available. Joint displays should be incorporated as standard tools in future validation cycles.

Expanded and diversified participant recruitment:

Future surveys and focus groups should actively recruit compliance professionals from large enterprises, public sector bodies, and regulated industries to address the representativeness gap identified in this phase.

Prompt engineering and tool literacy as a co-design input:

Given the documented sensitivity of tool performance to prompt quality, future phases should incorporate structured prompt engineering guidance and templating features (designed with and for non-expert users) as an explicit co-design input rather than a post-hoc addition.

4. Conclusions

This deliverable establishes an initial, user-driven requirements baseline for the TRUST system. It addresses the needs expressed by participating SMEs, DPOs, compliance professionals, auditors, engineers and certification stakeholders in relation to AI-driven regulatory compliance tools. Using a pragmatic mixed-methods requirements-elicitation approach that combines descriptive survey data with qualitative stakeholder workshops, the report identifies, compares and prioritises requirements and design inputs across the three TRUST pillars: LLM reliability (ELAL), AI-based compliance services (OPRCS and AAP), and the Seal of Trust certification schemes.

The requirements-gathering process revealed substantial convergence within the consulted stakeholder groups on several dimensions, notably the need for more reliable and verifiable LLM outputs and visible human oversight. These findings have been translated into requirements and candidate design inputs for further specification and validation. The report also highlights important differences between SME users and DPOs: SME participants emphasised simplification and accessibility, while DPO participants required more configurable, professional-grade functionality. These differences support exploration of a layered platform design in subsequent

development phases rather than assuming that a single interface model will meet all needs.

The findings of this report will serve as direct input for the WPs within the TRUST project:

- WP1 - Compliance by Design Report: The requirements captured in this deliverable will inform the embedding of cybersecurity and regulatory compliance principles into the TRUST system architecture.
- WP2 - Enhanced LLM Abstraction Layer (ELAL): This report informs the development of the Reinforced RAG Model (RRAG) and the Compliance Monitoring Agent (CMA) by capturing requirements for LLM reliability, hallucination reduction, and data leak prevention.
- WP3 - Online Platform of Regulatory Compliance Services (OPRCS): All of the six co-designed compliance services will be developed in direct response to the prioritised requirements documented here. Additionally, this report provides the outline and starting point for iterative feedback workshops to establish specifications for the different TRUST services in the scope of T3.1 (Co-Design Support).
- WP4 - Seal of Trust Specification: User-driven input from this report will directly inform T4.2 (Seal of TRUST Certification Criteria Specification), ensuring that certification schemes align with end-user expectations and regulatory standards.
- WP5 - End User Qualification: The requirements and documented user profiles in this report will underpin the use case qualification plan and testing activities from M13 onwards.

In alignment with the TRUST project roadmap, the following steps are recommended to follow up on the work presented in this deliverable:

Iterative validation through joint display methodology

Requirements identified in this phase should be validated iteratively through integrated quantitative/qualitative instruments as technical prototypes become available, rather than treated as fixed inputs.

Commencement of co-design and testing sessions

As communicated to workshop participants, co-design and testing sessions with initial demos and prototypes are scheduled to begin from Autumn 2026, taking place approximately every eight weeks until the end of the project.

Expanded and diversified participant recruitment

Future surveys and focus groups should actively recruit compliance professionals from large enterprises, public sector bodies, and regulated industries to address the representativeness gap identified in this phase.

In summary, this deliverable has successfully established the requirement baseline for the TRUST system and laid the groundwork for a user-centred, iterative development approach. The findings presented herein ensure that the TRUST platform's technical components are grounded in real-world needs and positioned to deliver demonstrable value to the more than 24 million European companies subject to EU regulatory obligations.

References

- [1] C. H. Meydan und A. Handan , „The role of triangulation in qualitative research: Converging perspectives,“ in *Principles of conducting qualitative research in multicultural settings*, IGI Global Scientific Publishing, 2024, pp. 101-132.
- [2] A. Bhattacharjee, *Social Science Research: Principles, Methods, and Practices*, Global Text Project, 2012.
- [3] C. Andrade, „The Limitations of Online Surveys,“ *Indian Journal of Psychological Medicine*, pp. 575-576, 6 2020.
- [4] J. Sandesh, S. Dubey und S. Jain, „Designing and validation of questionnaire,“ *International dental & medical journal of advanced research 2.1*, pp. 1-3, 2016.
- [5] A. Caroline Tynan und J. Drayton, „CONDUCTING FOCUS GROUPS — A GUIDE FOR FIRST-TIME USERS,“ *Marketing Intelligence & Planning*, Vol. 6 No. 1, pp. 5-9, 1988.
- [6] I. Hutter, M. Hennink und A. Bailey, *Qualitative Research Methods*, Onbekend : SAGE Publishing Inc., 2011.
- [7] M. Lokanath , „Focus group discussion in qualitative research,“ *Techno Learn 6.1*, pp. 1-5, 2016.
- [8] E. Gammie, S. Hamilton und V. Gilchrist, „Focus group discussions,“ in *The Routledge companion to qualitative accounting research methods*, 2017, pp. 372-386.
- [9] H. Mahama und K. Rihab , „Field interviews,“ in *The Routledge companion to qualitative accounting research methods* , 2017, pp. 321-338.
- [10] D. L. Morgan, „Focus groups and social interaction,“ in *The SAGE Handbook of Interview Research*, J. F. Gubrium, J. A. Holstein, A. B. Marvasti, K. D. McKinney , 2012, pp. 161-176.
- [11] A. Strauss und J. Corbin, *Basics of qualitative research techniques*, 1998.
- [12] N. Ziegler und K. Le , „Mixed methods designs,“ in *Second language assessment and mixed methods research*, 2016, pp. 51-84.

- [13] T. C. Guetterman, R. Sakakibara und S. Fàbregues, „Visuals in joint displays to represent integration in mixed methods research: A methodological review.,“ *Methods in Psychology*, p. 100080, 2021.
- [14] M. T. McCrudden, G. Marchand und P. A. Schutz, „Joint displays for mixed methods research in psychology,“ *Methods in Psychology*, pp. 1-9, 2021.
- [15] J. W. Creswell and . J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Sage Publications, 2017.
- [16] D. L. Morgan, „Focus groups and social interaction,“ in *The Sage handbook of interview research: The complexity of the craft*, 2012, pp. 161-176.

Annexes

Annex 1 - SME Survey: Questionnaire

Section 1: Background & Context

1. Which category best describes your current role?
(Dropdown: *Member of an SME, Data protection officer, Member of compliance team, Member of a certification authority, Other*)
2. In which country is your organisation (mainly) based?
(Dropdown: *[EU-Countries]*)
3. Do you have an internal compliance team?
(Yes/No/Partially)
 - a. If yes: How many people are dedicated to compliance?
(Dropdown: *1, 2-5, 6-10, 10+, I don't know, No Answer*)

Section 2: Current Compliance Challenges

4. Which EU regulations are most relevant to your business?
(Multi-select)
 - a. GDPR
 - b. AI Act
 - c. Digital Services Act
 - d. Digital Markets Act
 - e. Sector-specific Regulation
 - f. Other (please specify)
5. What are the biggest obstacles to achieving compliance?
(Multi-select)
 - a. Lack of internal expertise or knowledge
 - b. Complexity of regulations and legal jargon
 - c. Frequent changes in regulations
 - d. Time-consuming manual processes
 - e. Integration with existing systems or workflows
 - f. Lack of clear guidance or best practices
 - g. Difficulty in monitoring and tracking compliance status
 - h. Other (please specify)
6. What are the most time-consuming compliance tasks for your team?
(Multi-select)
 - a. Monitoring regulations
 - b. Understanding legal jargon
 - c. Risk analysis
 - d. Generating reports
 - e. Auditing
 - f. Ensuring data privacy

- g. Other (please specify)
- 7. What compliance tools do you currently use?
(Multi-select)
 - a. Manual spreadsheets or documents
 - b. Consultants or external legal advisors
 - c. Legal/ compliance software
 - d. AI-powered tools (e.g., chatbots, automated compliance checkers)
 - e. Custom-built internal tools
 - f. Industry-specific compliance platforms
 - g. None
 - h. I don't know
 - i. Other (please specify)
- 8. How satisfied are you with your current compliance tools?
(Scale: 1 = Very Dissatisfied, 5 = Very Satisfied)
- 9. How important is each of the following features for a compliance tool?
(Scale for each: 1 = Not Important, 5 = Very Important)
 - a. Reliability
 - b. Integration with existing tools and workflows
 - c. Customizable templates for reports and assessments
 - d. Data privacy and confidentiality protection
 - e. Cost-effectiveness and budget-friendly pricing
 - f. User-friendly interface and ease of use
 - g. Scalability to accommodate business growth
 - h. Training and support resources (e.g., tutorials, customer service)
 - i. Ability to handle multiple regulations (e.g., GDPR, AI Act,...)
 - j. Automated monitoring of compliance status
 - k. Collaboration features for teams and external partners
 - l. Access to a centralized knowledge base or regulatory library
 - m. Customizable dashboards for tracking compliance metrics
 - n. Automated document completion (e.g., DPIA, TIA, FRIA templates)
 - o. Proactive risk management and mitigation / traceability/auditability suggestions
 - p. Other (please specify)
- 10. Which of the following TRUST tools would be most valuable to your organization?
(Multi-select)
 - a. Real-time alerts for regulatory updates (RCA)
 - b. Plain-language summaries of legal obligations (ROA)
 - c. Risk scoring and legal data analysis (LRA)
 - d. Automated report generation (RRA)
 - e. Compliance gap analysis and scoring (RCE)
 - f. Auditor collaboration tools (CPA)
 - g. All of them
 - h. None of them

Section 3: AI & Automation Readiness

11. How comfortable are you with using AI for compliance tasks?
(Scale: 1 = Not comfortable, 5 = Very comfortable)
12. How much control do you want AI to have over your compliance workflow?
(Scale: 1 = Fully manual, 5 = Fully automated)
13. Have you used AI chat assistants (e.g., for legal or compliance queries)?
(Yes/No)
 - a. If yes: What was your experience? (Open-ended)
14. Would you trust an AI tool to handle compliance tasks without human oversight?
(Yes/No/Only for specific tasks)
 - a. If yes / specific tasks:
Which tasks would you hand over to an AI assistant?
(Multi-select)
 - i. Monitoring and tracking regulatory updates
 - ii. Translating complex regulatory obligations into actionable steps
 - iii. Analysing regulatory risks and providing risk scores
 - iv. Generating compliance reports (e.g., DPIA, TIA, FRIA)
 - v. Assessing compliance gaps and providing scoring
 - vi. Facilitating certification processes (e.g., GDPR Seal, ISO standards)
 - vii. Automating repetitive and time-consuming tasks (e.g., data entry, document completion)
 - viii. Providing real-time alerts for new or updated regulations
 - ix. Offering plain-language summaries of legal requirements
 - x. Assisting in audits and compliance checks
 - xi. Managing and organizing compliance documentation
 - xii. Identifying applicable regulations for my business
 - xiii. Suggesting proactive risk management strategies
 - xiv. Integrating compliance workflows with existing tools
 - xv. Providing training and guidance on compliance processes
 - xvi. Other (please specify)

15. What concerns do you have about using AI for compliance?

(Multi-select)

- a. Hallucinations / invented results
- b. Data privacy
- c. Reliability
- d. Lack of transparency
- e. Cost
- f. Other (please specify)

16. What would make you trust a compliance AI tool?

(Multi-select)

- a. Transparency in how the AI makes decisions
- b. Auditability (ability to trace and review AI decisions)
- c. Human-in-the-loop (human oversight and intervention)
- d. Proven accuracy and reliability
- e. Certifications (e.g., ISO, GDPR compliance seals)
- f. Explainability of AI decisions (clear reasoning provided)
- g. Reduction of hallucinations and errors in AI outputs
- h. Structured and well-organized responses
- i. Anonymous and secure data processing
- j. Fast processing and response times
- k. Other (please specify)

Section 4: Any Other Business

17. Which questions did we forget? What else is important to you?

(Open-ended)

Annex 2 - SME Survey: Results

Number of records in this query:	92	
Total number of data points in this survey:	92	
Percentage:	100,00%	
Summary for Q00		
Which category best describes your current role?		
Answer	Number	Percentage
Member of an SME (A001)	26	47,27%
Data protection officer (A002)	2	3,64%
Member of compliance team (A003)	9	16,36%
Member of a certification authority (A005)	0	0,00%
Other (A004)	18	32,73%
Summary for Q001		
In which country is your organisation (mainly) based?		
Answer	Number	Percentage
Austria (A001)	0	0,00%
Belgium (A002)	0	0,00%
Bulgaria (A003)	0	0,00%

Croatia (A004)	0	0,00%
Cyprus (A005)	0	0,00%
Czech Republic (A006)	0	0,00%
Denmark (A007)	0	0,00%
Estonia (A008)	0	0,00%
Finland (A009)	1	1,79%
France (A010)	1	1,79%
Germany (A011)	49	87,50%
Greece (A012)	0	0,00%
Hungary (A013)	0	0,00%
Ireland (A014)	1	1,79%
Italy (A015)	0	0,00%
Latvia (A016)	0	0,00%
Lithuania (A017)	0	0,00%
Luxembourg (A018)	0	0,00%
Malta (A019)	0	0,00%
Netherlands (A020)	0	0,00%
Poland (A021)	0	0,00%
Portugal (A022)	0	0,00%
Romania (A023)	0	0,00%
Slovakia (A024)	0	0,00%
Slovenia (A025)	0	0,00%
Spain (A026)	0	0,00%
Sweden (A027)	0	0,00%
Other (A028)	4	7,14%
Summary for Q002		

Do you have an internal compliance team?		
Answer	Number	Percentage
Yes (A001)	13	25,00%
No (A002)	24	46,15%
Partially (A003)	11	21,15%
Does not apply (A004)	4	7,69%
Summary for Q003		
How many people are dedicated to compliance?		
Answer	Number	Percentage
1 (A001)	7	29,17%
2-5 (A002)	12	50,00%
6-10 (A003)	1	4,17%
10+ (A004)	3	12,50%
I don't know (A005)	1	4,17%
Summary for Q004		
Which EU regulations are most relevant to your business?		
Answer	Number	Percentage
GDPR (SQ001)	26	78,79%
AI Act (SQ002)	24	72,73%
Digital Services Act (SQ003)	14	42,42%
Sector-specific Regulation (SQ004)	8	24,24%
Digital Markets Act (SQ005)	6	18,18%

Otheres	10	30,30%
ID	Answer	
3	Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225); NIS2 Directive; Cyber Resilience Act (CRA); EU Cybersecurity Act; EU Cyber Solidarity Act; Critical Entities Resilience Directive (CER); Digital Operational Resilience Act (DORA); eIDAS 2.0 and the European Digital Identity Framework; Data Act; Data Governance Act; Interoperable Europe Act; ePrivacy Directive; Law Enforcement Directive; Open Data Directive; Product Liability Directive; General Product Safety Regulation; Machinery Regulation; European Accessibility Act; European Health Data Space Regulation; Radio Equipment Directive cybersecurity requirements; and sector-specific requirements concerning AI governance, cybersecurity, data protection, digital identity, operational resilience, incident response, product safety, interoperability, certification and conformity assessment, together with related ISO/IEC, ETSI, ENISA, NIST and CEN-CENELEC implementation standards and guidance.	
23	Compliance for Carriers (Transportation)	
24	All regulations concerning chemicals and hazardous substances	
48	DORA, FINMA	
66	NIS2	
67	CRA Cyber Resilience Act	
68	CRA	
75	We are Governance and Compliance IT Provider for IT Infrastructure	
86	CRA, NIS2	
90	BSI C5, ISO 27001, NIS-2	
Summary for Q005		
What are the biggest obstacles to achieving compliance?		
Answer	Number	Percentage
Lack of internal expertise or	13	40,63%

knowledge (SQ001)		
Complexity of regulations and legal jargon (SQ002)	22	68,75%
Frequent changes in regulations (SQ003)	19	59,38%
Time-consuming manual processes (SQ004)	20	62,50%
Integration with existing systems or workflows (SQ005)	12	37,50%
Lack of clear guidance or best practices (SQ006)	21	65,63%
Difficulty in monitoring and tracking compliance status (SQ007)	15	46,88%
Otheres	2	6,25%
ID	Answer	
3	Difficulty translating regulatory requirements into testable implementation controls, evidence obligations and accountable ownership; overlapping requirements across legal, sectoral and standards frameworks; limited source and version traceability; uncertainty about what constitutes sufficient evidence; and the lack of practical remediation, retesting and validated closure workflows, particularly for SMEs with limited resources.	
86	lawyers consider all regulation an opportunity to sell their services	

Summary for Q006		
What are the most time-consuming compliance tasks for your team		
Answer	Number	Percentage
Monitoring regulations (SQ001)	21	67,74%
Understanding legal jargo (SQ002)	17	54,84%
Risk analysis (SQ003)	17	54,84%
Generating reports (SQ004)	15	48,39%
Auditing (SQ005)	18	58,06%
Ensuring data privacy (SQ006)	8	25,81%
Otheres	2	6,45%
ID	Answer	
75	We deliver all Technical Views of Point to our Customer	
86	Tax	
Summary for Q007		
What compliance tools do you currently use?		
Answer	Number	Percentage
Manual spreadsheets or documents (SQ001)	20	62,50%
Consultants or external legal advisors (SQ002)	9	28,13%

Legal/ compliance software (SQ003)	7	21,88%
AI-powered tools (e.g., chatbots, automated compliance checkers) (SQ004)	16	50,00%
Custom-built internal tools (SQ005)	14	43,75%
Industry-specific compliance platforms (SQ006)	7	21,88%
None (SQ007)	2	6,25%
I don't know (SQ008)	0	0,00%
Otheres	1	3,13%
ID	Answer	
54	We are developers of GitCover - Git-native Compliance for SME and publisher of GCBok - GitCover Body of Knowledge for Git-native Compliance	
Summary for Q008		
How satisfied are you with your current compliance tools?		
Answer	Number	Percentage
1 (1)	2	2,17%
2 (2)	6	6,52%
3 (3)	12	13,04%
4 (4)	6	6,52%

5 (5)	5	5,43%
Total (Answers)	31	100,00%
Number of cases	0	0,00%
Arithmetic mean	3,19	
Standard deviation	1,14	
Summary for Q009(SQ002)[Reliability]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	1	3,23%
2 (A002)	0	0,00%
3 (A003)	3	9,68%
4 (A004)	6	19,35%
5 (A005)	21	67,74%
Summary for Q009(SQ003)[Integration with existing tools and workflows]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	2	6,67%
2 (A002)	1	3,33%
3 (A003)	7	23,33%
4 (A004)	12	40,00%
5 (A005)	8	26,67%
Summary for Q009(SQ004)[Customizable templates for reports and assessments]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	1	3,13%

2 (A002)	4	12,50%
3 (A003)	7	21,88%
4 (A004)	10	31,25%
5 (A005)	10	31,25%
Summary for Q009(SQ005)[Data privacy and confidentiality protection]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	2	6,45%
3 (A003)	3	9,68%
4 (A004)	6	19,35%
5 (A005)	20	64,52%
Summary for Q009(SQ006)[Cost-effectiveness and budget-friendly pricing]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	2	6,25%
3 (A003)	9	28,13%
4 (A004)	6	18,75%
5 (A005)	15	46,88%
Summary for Q009(SQ007)[User-friendly interface and ease of use]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	2	6,45%
3 (A003)	6	19,35%

4 (A004)	8	25,81%
5 (A005)	15	48,39%
Summary for Q009(SQ008)[Scalability to accommodate business growth]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	5	15,63%
3 (A003)	12	37,50%
4 (A004)	9	28,13%
5 (A005)	6	18,75%
Summary for Q009(SQ009)[Training and support resources (e.g., tutorials, customer service)]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	4	12,50%
3 (A003)	8	25,00%
4 (A004)	14	43,75%
5 (A005)	6	18,75%
Summary for Q009(SQ010)[Ability to handle multiple regulations (e.g., GDPR, AI Act,...)]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	1	3,23%
3 (A003)	1	3,23%
4 (A004)	7	22,58%

5 (A005)	22	70,97%
Summary for Q009(SQ011)[Automated monitoring of compliance status]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	1	3,33%
3 (A003)	3	10,00%
4 (A004)	13	43,33%
5 (A005)	13	43,33%
Summary for Q009(SQ012)[Collaboration features for teams and external partners]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	2	6,45%
2 (A002)	3	9,68%
3 (A003)	7	22,58%
4 (A004)	11	35,48%
5 (A005)	8	25,81%
Summary for Q009(SQ013)[Access to a centralized knowledge base or regulatory library]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	1	3,23%
3 (A003)	7	22,58%
4 (A004)	14	45,16%
5 (A005)	9	29,03%

Summary for Q009(SQ014)[Customizable dashboards for tracking compliance metrics]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	2	6,25%
2 (A002)	2	6,25%
3 (A003)	10	31,25%
4 (A004)	12	37,50%
5 (A005)	6	18,75%
Summary for Q009(SQ015)[Automated document completion (e.g., DPIA, TIA, FRIA templates)]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	4	13,33%
2 (A002)	1	3,33%
3 (A003)	5	16,67%
4 (A004)	11	36,67%
5 (A005)	9	30,00%
Summary for Q009(SQ016)[Proactive risk management and mitigation / traceability/auditability suggestions]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	2	6,90%
3 (A003)	10	34,48%
4 (A004)	9	31,03%
5 (A005)	8	27,59%

Summary for Q010		
Which of the following TRUST tools would be most valuable to your organization		
Answer	Number	Percentage
Real-time alerts for regulatory updates (RCA) (SQ001)	14	43,75%
Plain-language summaries of legal obligations (ROA) (SQ002)	15	46,88%
Risk scoring and legal data analysis (LRA) (SQ003)	12	37,50%
Automated report generation (RRA) (SQ004)	16	50,00%
Compliance gap analysis and scoring (RCE) (SQ005)	17	53,13%
Auditor collaboration tools (CPA) (SQ006)	10	31,25%
All of them (SQ007)	11	34,38%
None of them (SQ008)	2	6,25%
Otheres	2	6,25%
ID	Answer	
3	An integrated operational compliance layer connecting regulatory updates and legal obligations to implementation controls, accountable owners, evidence requirements, remediation actions, retesting and	

	validated closure, with source/version traceability and human decision oversight.	
86	'don't know. RCA and ROA can help, but RCA might cause a lot of noise whereas RCA might miss relevant stuff and so on.	
Summary for Q011		
How comfortable are you with using AI for compliance tasks?		
Answer	Number	Percentage
1 (1)	3	3,26%
2 (2)	2	2,17%
3 (3)	6	6,52%
4 (4)	10	10,87%
5 (5)	11	11,96%
Total (Answers)	32	100,00%
Number of cases	0	0,00%
Arithmetic mean	3,75	
Standard deviation	1,27	
Summary for Q012		
How much control do you want AI to have over your compliance workflow?		
Answer	Number	Percentage
1 (1)	3	3,26%
2 (2)	2	2,17%
3 (3)	11	11,96%
4 (4)	14	15,22%
5 (5)	2	2,17%
Total (Answers)	32	100,00%

Number of cases	0	0,00%
Arithmetic mean	3,31	
Standard deviation	1,03	
Summary for Q013		
Have you used AI chat assistants (e.g., for legal or compliance queries)?		
Answer	Number	Percentage
Yes	27	87,10%
No	4	12,90%
Summary for Q014		
What was your experience?		
Answer	26	100,00%
ID	Answer	
2	Rather good	
5	good	
7	Yes. I have used AI assistants extensively for legal, regulatory, compliance, governance and cybersecurity-related research. The experience has generally been positive. AI tools can help analyze large volumes of information, summarize legal and technical documents, identify relevant regulations and standards, and support drafting and review activities. However, outputs should always be independently verified, especially in legal, compliance, regulatory and high-risk contexts. AI is most valuable as a research and productivity assistant rather than as a final	

	decision-maker. The quality of results depends on transparency, source traceability, consistency, accuracy and the user's ability to validate the generated information.
11	The usage efficiency and efficacy are highly dependent on the engineering teams understanding of the use case and customer requirements. If not done properly, it becomes a barrier than enabler.
17	great
21	Given a detailed prompt and clear sources for RAG, I feel very confident that the results are OK. AI is a great timesaver.
23	Good.
24	Many prompts were needed, very often the LLM Model was confused and hallucinated with wrong information or wrong sources. For easier tasks (like text correction) the LLM Model is very strong. For other areas like research on specific areas, the LLM Model may start to mix up things.
27	overall positive
38	Access to know about processes, tools and experiences others
41	split resume: useful in collecting available data sources, but sometimes hallucinating, the proof of correctness needs nearly the same time which was saved before in data collection, that's why we modified an existing own no-coe checklist generator, which is much more useful now
48	Pretty fine output. With the "human in the loop" and finetuned prompts it's a great timesaver for me.
54	Different qualities based on models. Too expensive when provided by AI Companies - must be Local AI Hosting, since rules are guardrails, OSCAL/OPA is easy to follow by MCP Servers (locally hosted)
55	Yes, I regularly use AI chat assistants such as Microsoft Copilot to support a variety of business, compliance, and governance-related tasks. My experience includes: Reviewing and summarizing regulatory requirements (e.g., GDPR, ISO 27001, data protection, and information security standards).

	Preparing compliance-related documentation, policies, and audit evidence. Researching legal and contractual topics, such as data processing agreements (DPAs), cloud compliance requirements, and Microsoft licensing terms. Creating first drafts of customer communications, management summaries, risk assessments, and compliance reports. Analyzing technical and security documentation and translating complex requirements into actionable business recommendations. Supporting project planning and documentation for cloud migrations, document management systems, and Microsoft 365 environments. I use AI as a productivity and research assistant to accelerate information gathering and document preparation. However, for legal, compliance, and contractual decisions, all AI-generated information is validated against official sources and reviewed by subject-matter experts before being acted upon.	
62	Sehr gut, eigene Entwicklung	
65	Einfach in der Übersicht und Bedienung	
66	good	
67	It must be used with caution and the results must be verified	
68	Vibe from Mistral made good suggestions	
72	...	
75	My Own created AI "Anima" is managing my Bussines Backoffice also with Phone Calls , Mails and so on.	
77	nicht schlecht	
80	interesting tools for chip technology with modeling language eclipse papyrus	
82	Mixed	
86	mixed. Some answers ok, some haluzinating. AI is just a tool, sometimes it helps, sometimes not. A fool with a tool is still a fool.	
90	cannot live without anymore	

Summary for Q015		
Would you trust an AI tool to handle compliance tasks without human oversight?		
Answer	Number	Percentage
Yes (SQ001)	3	9,38%
No (SQ002)	17	53,13%
Only for specific tasks (SQ003)	14	43,75%
Summary for Q016		
Which tasks would you hand over to an AI assistant?		
Answer	Number	Percentage
Monitoring and tracking regulatory updates (SQ001)	17	100,00%
Translating complex regulatory obligations into actionable steps (SQ002)	13	76,47%
Analysing regulatory risks and providing risk scores (SQ003)	13	76,47%
Generating compliance reports (e.g., DPIA, TIA, FRIA) (SQ004)	14	82,35%
Assessing compliance gaps and providing scoring (SQ005)	11	64,71%

Facilitating certification processes (e.g., GDPR Seal, ISO standards) (SQ006)	9	52,94%
Automating repetitive and time-consuming tasks (e.g., data entry, document completion) (SQ007)	17	100,00%
Providing real-time alerts for new or updated regulations (SQ008)	13	76,47%
Offering plain-language summaries of legal requirements (SQ009)	14	82,35%
Assisting in audits and compliance checks (SQ010)	16	94,12%
Managing and organizing compliance documentation (SQ011)	14	82,35%
Identifying applicable regulations for my business (SQ012)	14	82,35%
Suggesting proactive risk management	12	70,59%

strategies (SQ013)		
Integrating compliance workflows with existing tools (SQ014)	13	76,47%
Providing training and guidance on compliance processes (SQ015)	12	70,59%
Otheres	0	0,00%
ID	Answer	
Summary for Q017		
What concerns do you have about using AI for compliance?		
Answer	Number	Percentage
Hallucinations / invented results (SQ001)	25	78,13%
Data privacy (SQ002)	22	68,75%
Reliability (SQ003)	21	65,63%
Lack of transparency (SQ004)	20	62,50%
Cost (SQ005)	16	50,00%
Otheres	4	12,50%
ID	Answer	

3	I don't have any concerns.	
4	I specialize in AI compliance. Using genAI for AI compliance is ridiculous.	
7	I just don't want anyone to steal knowledge.	
84	Negative ecological impact	
Summary for Q018		
What would make you trust a compliance AI tool?		
Answer	Number	Percentage
Transparency in how the AI makes decisions (SQ001)	27	84,38%
Auditability (ability to trace and review AI decisions) (SQ002)	22	68,75%
Human-in-the-loop (human oversight and intervention) (SQ003)	28	87,50%
Proven accuracy and reliability (SQ004)	19	59,38%
Certifications (e.g., ISO, GDPR compliance seals) (SQ005)	16	50,00%
Explainability of AI decisions (clear reasoning provided) (SQ006)	25	78,13%
Reduction of hallucinations	19	59,38%

and errors in AI outputs (SQ007)		
Structured and well-organized responses (SQ008)	15	46,88%
Anonymous and secure data processing (SQ009)	16	50,00%
Fast processing and response times (SQ010)	9	28,13%
Otheres	2	6,25%
ID	Answer	
4	nothing could make me trust a genAI compliance tool	
41	very low costs	
Summary for Q019		
Which questions did we forget? What else is important to you?		
Answer	16	100,00%
ID	Answer	
2	Nothing	
3	You have not omitted any essential questions.	
7	Pay me.	
11	Have you completed training in using AI tools - generative AI, AI chatbots, etc. Give example of risks that are particular to your domain and industry.	
23	None.	

38	none	
41	usability, ability of process customization which will be saved in templates or forms or checklist (we use no-code checklist generator) ability of design modifications which will become part of the data model and saves time in every audit process	
59	i'm sorry ,but i'm very pessimistic that an ai-based tool could reach the targets you describe. My experience over the last years is, that every effort to less bureaucracy achieves the opposite.	
62	Regulation und Förderungen von Entwicklung eigener künstlicher Intelligenz	
65	Bislang nichts weiter.	
66	AI must be hosted in EU	
68	May be mentioning CRA, NIS2, DORA	
72	...	
80	which tools of AI using programming languages i.e. Java , C++ , Rust or Python, JavaScript, Ruby could be preferred for improved then new protocol HTTP/3 industry	
84	I'm all for AI tools that help me locate and/or understand legal texts. It's also fine to have AI tools scan full-text sources and pre-fill forms. However, if I need to sign anything, I'd like to see the form inputs and understand, what I'm submitting there. Please do not build a tool that black-boxes me out of the decision loop.	
86	scalability to small company, integration of topics that are not prebuilt, or not EU-driven. e.g. ISO 27000 was not listed initially.	

Annex 3 - DPO Survey: Questionnaire

Section 1: Background & Context

- 1) What type of DPO are you?
(Dropdown: External DPO (consultant), Internal DPO (employee), Materialized DPO (designated within the organization), Other)
 - a) If internal DPOs: Do you have an internal compliance team?
(Yes/No/Partially)
 - b) If yes: How many people are dedicated to compliance?
(Dropdown: 1, 2-5, 6-10, 10+, I don't know, No Answer)
- 2) How important is it for your organization to communicate its compliance at each of the following levels?
Rate each level on a scale of 1 to 10, where 1 = Not important and 10 = Extremely important.
 - a) Company-wide — communicating overall organizational compliance
 - b) Product or service level — communicating compliance for specific offerings
- 3) In which country is your organisation (mainly) based?
(Dropdown: [EU-Countries])
- 4) Which sector does your organization primarily operate in?
(Dropdown)
 - a) Health & life sciences (e.g., MDR, IVDR),
 - b) Financial services & fintech (e.g., MiFID II, PSD2, DORA),
 - c) Insurance (e.g., Solvency II, IDD),
 - d) Energy & utilities
 - e) Transport & mobility,
 - f) Agriculture & food,
 - g) Media & content,
 - h) Other (please specify)

Section 2: Current Compliance Challenges

- 5) How would you rate the overall complexity of the current regulatory compliance environment for your organization?
Please rate on a scale of 1 to 10, where 1 = Very simple / manageable and 10 = Extremely complex / overwhelming.

- 6) How challenging is each of the following aspects of regulatory compliance for your organization?
Rate each challenge factor on a scale of 1 to 10, where 1 = No challenge and 10 = Major challenge.
- a) Expertise (lack of in-house regulatory/legal knowledge)
 - b) Costs (financial resources required for compliance)
 - c) Time (time burden of compliance activities)
 - d) Legal knowledge (interpreting complex legal texts)
 - e) Keeping up with regulatory changes (pace of new rules)
 - f) Implementation (translating requirements into practice)
 - g) Documentation & reporting (administrative burden)
 - h) Cross-border complexity (dealing with multiple jurisdictions)
 - i) Technology adaptation (updating systems to comply)
 - j) SME-specific guidance (lack of tailored resources for smaller organizations)
- 7) Are there any other regulations — not listed above — that are important for your organization to comply with or communicate compliance about? *Please list them below and briefly explain their relevance to your business.*
- 8) What are the most time-consuming compliance tasks for your team? *(Multi-select)*
- a) Monitoring regulatory updates
 - b) Understanding legal jargon and requirements
 - c) Risk analysis and assessment
 - d) Generating compliance reports (DPIA, TIA, FRIA, etc.)
 - e) Auditing and internal reviews
 - f) Ensuring data privacy and security
 - g) Other (please specify): _____
- 9) How important is it for your organization to comply with and communicate compliance to each of the following regulations?
Please rate each regulation on a scale of 1 to 10, where 1 = Not at all important and 10 = Extremely important.
- a) AI Act — Artificial Intelligence Act
 - b) DGA — Data Governance Act
 - c) GDPR — General Data Protection Regulation
 - d) Data Act – Regulation on harmonised rules on fair access to and use of data
 - e) NIS2 — Network and Information Security Directive
 - f) DORA — Digital Operational Resilience Act
 - g) CRA — Cyber Resilience Act
 - h) EHDS – European Health Data Space
 - i) eIDAS 2.0 — Electronic Identification & Trust Services

- 10) How important is it for your organisation to communicate compliance with regulations that are specific to your sector or domain?
Rate each sector/domain below according to its relevance to your organisation, where 1 = Not relevant / not important and 10 = Highly relevant and very important to communicate.
- a) Health & life sciences (e.g. MDR, IVDR, clinical data rules)
 - b) Financial services & fintech (e.g. MiFID II, PSD2, DORA)
 - c) Insurance (e.g. Solvency II, IDD)
 - d) Energy & utilities (e.g. Clean Energy Package, REMIT)
 - e) Transport & mobility (e.g. autonomous vehicles, drones)
 - f) Agriculture & food (e.g. Farm-to-Fork, food safety standards)
 - g) Media & content (e.g. DSA content rules, copyright)
 - h) Other sector (please specify)
- 11) If your sector is not listed above, or if you would like to elaborate on sector specific regulations that are relevant to your organisation, please describe them here.
- 12) How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?
Rate each potential benefit on a scale of 1 to 10, where 1 = Not significant / not relevant and 10 = Extremely significant. Focus on the concrete outcomes your organisation has experienced or would expect from strong data governance compliance.
- a) Access to new business partnerships and data-sharing agreements
 - b) Easier participation in public tenders and procurement processes
 - c) Faster and smoother regulatory audits or inspections
 - d) Reduced internal compliance management effort and costs
 - e) Increased customer trust and confidence in your data practices
 - f) Improved data quality leading to better business decisions
 - g) Competitive differentiation and market positioning
 - h) Access to data spaces, platforms, or ecosystems
 - i) Simplified cross-border operations within the EU
 - j) Stronger investor or stakeholder confidence
 - k) Ability to demonstrate accountability in case of incidents or disputes
 - l) Increased employee confidence in internal data handling
- 13) Are there other benefits or added values — not listed above — that your organisation has experienced or would expect from showcased compliance?
Please describe them.

Section 3: AI & Automation Readiness

14) How comfortable are you with using AI for compliance tasks?

Please rate on a scale of 1 to 5, where 1 = Not comfortable and 5 = Very comfortable.

15) Would you trust an AI tool to handle compliance tasks without human oversight?

- a) Yes, for all tasks
- b) Only for specific tasks
- c) No

16) What concerns do you have about using AI for compliance?

(Multi-select)

- a) Hallucinations (false or missing sources)
- b) Data privacy and security risks
- c) Reliability and consistency of outputs
- d) Lack of transparency in AI decision-making
- e) Accuracy and liability risks
- f) Other (please specify): _____

Annex 4 - DPO Survey: Results

Number of records in this query:	118	
Total number of data points in this survey:	118	
Percentage:	100,00%	
Summary for Q00		
Which category best describes your current role?		
Answer	Number	Percentage
External DPO (consultant) (A001)	26	32,50%
Internal DPO (employee) (A002)	38	47,50%
Materialized DPO (designated within the organization) (A003)	4	5,00%
Member of a certification authority (A005)	0	0,00%
Other (A004)	12	15,00%
Summary for Q002		
Do you have an internal compliance team?		
Answer	Number	Percentage
Yes (A001)	27	50,94%

No (A002)	15	28,30%
Partially (A003)	10	18,87%
Does not apply (A004)	1	1,89%
Summary for Q003		
How many people are dedicated to compliance?		
Answer	Number	Percentage
1 (A001)	13	26,00%
2-5 (A002)	30	60,00%
6-10 (A003)	2	4,00%
10+ (A004)	5	10,00%
I don't know (A005)	0	0,00%
Summary for Q001		
In which country is your organisation (mainly) based?		
Answer	Number	Percentage
Austria (A001)	0	0,00%
Belgium (A002)	2	2,44%
Bulgaria (A003)	0	0,00%
Croatia (A004)	0	0,00%
Cyprus (A005)	0	0,00%
Czech Republic (A006)	0	0,00%
Denmark (A007)	0	0,00%

Estonia (A008)	0	0,00%
Finland (A009)	0	0,00%
France (A010)	37	45,12%
Germany (A011)	11	13,41%
Greece (A012)	0	0,00%
Hungary (A013)	0	0,00%
Ireland (A014)	3	3,66%
Italy (A015)	0	0,00%
Latvia (A016)	0	0,00%
Lithuania (A017)	0	0,00%
Luxembourg (A018)	0	0,00%
Malta (A019)	0	0,00%
Netherlands (A020)	0	0,00%
Poland (A021)	0	0,00%
Portugal (A022)	0	0,00%
Romania (A023)	0	0,00%
Slovakia (A024)	0	0,00%
Slovenia (A025)	0	0,00%
Spain (A026)	24	29,27%
Sweden (A027)	1	1,22%
Other (A028)	4	4,88%

Summary for Q020		
Which sector does your organization primarily operate in?		
Answer	Number	Percentage
IT (A001)	14	17,72%
Health & life sciences (e.g., MDR, IVDR) (A002)	11	13,92%
Financial services & fintech (e.g., MiFID II, PSD2, DORA) (A003)	6	7,59%
Insurance (e.g., Solvency II, IDD) (A004)	2	2,53%
Energy & utilities (A005)	7	8,86%
Transport & mobility (A006)	0	0,00%
Agriculture & food (A007)	2	2,53%
Media & content (A008)	7	8,86%
Otheres	30	37,97%
ID	Answer	
4	Legal services and consultancy in data protection, digital law and compliance	
5	European Social Funds_ Training Programmes	
21	Engineering, manufacturing and specialized services	
25	health and social care	

27	Higher Education	
28	public organisation	
35	Editeur de logiciel B2B	
39	medical and social sector	
43	social housing	
44	Business services	
46	services aux entreprises	
47	retail	
51	Consultoría	
61	various sectors	
63	AI development + Social Media	
70	All of these	
78	Salud	
81	social housing	
83	Pymes	
85	CONSULTORIA	
91	SANTE : sanitaire et EMS	
93	industry	
101	Housing	
106	Education	
107	Legal counsel	
111	Telecommunications	
116	Industry and Trade	
Summary for Q021		
How would you rate the overall complexity of the current regulatory compliance environment for your organization?		
Answer	Number	Percentage
1 (1)	0	0,00%

2 (2)	3	2,54%
3 (3)	10	8,47%
4 (4)	24	20,34%
5 (5)	6	5,08%
Total (Answers)	43	100,00%
Number of cases	0	0,00%
Arithmetic mean	3,77	
Standard deviation	0,78	
Summary for Q022(SQ001)[Expertise (lack of in-house regulatory/legal knowledge)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	3	6,52%
2 (A002)	11	23,91%
3 (A003)	18	39,13%
4 (A004)	11	23,91%
5 (A005)	3	6,52%
Summary for Q022(SQ002)[Costs (financial resources required for compliance)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	14	31,11%
3 (A003)	12	26,67%
4 (A004)	13	28,89%

5 (A005)	6	13,33%
Summary for Q022(SQ003)[Time (time burden of compliance activities)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	1	2,27%
2 (A002)	4	9,09%
3 (A003)	7	15,91%
4 (A004)	20	45,45%
5 (A005)	12	27,27%
Summary for Q022(SQ004)[Legal knowledge (interpreting complex legal texts)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	3	6,52%
2 (A002)	8	17,39%
3 (A003)	17	36,96%
4 (A004)	13	28,26%
5 (A005)	5	10,87%
Summary for Q022(SQ005)[Keeping up with regulatory changes (pace of new rules)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	2	4,35%
2 (A002)	3	6,52%
3 (A003)	8	17,39%
4 (A004)	23	50,00%

5 (A005)	10	21,74%
Summary for Q022(SQ006)[Implementation (translating requirements into practice)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	1	2,17%
2 (A002)	4	8,70%
3 (A003)	9	19,57%
4 (A004)	20	43,48%
5 (A005)	12	26,09%
Summary for Q022(SQ007)[Documentation & reporting (administrative burden)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	1	2,17%
2 (A002)	8	17,39%
3 (A003)	10	21,74%
4 (A004)	17	36,96%
5 (A005)	10	21,74%
Summary for Q022(SQ008)[Cross-border complexity (dealing with multiple jurisdictions)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	7	17,50%
2 (A002)	3	7,50%
3 (A003)	5	12,50%
4 (A004)	11	27,50%

5 (A005)	14	35,00%
Summary for Q022(SQ009)[Technology adaptation (updating systems to comply)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	4	8,89%
3 (A003)	13	28,89%
4 (A004)	22	48,89%
5 (A005)	6	13,33%
Summary for Q022(SQ010)[SME-specific guidance (lack of tailored resources for smaller organizations)]		
How challenging is each of the following aspects of regulatory compliance for your organization?		
Answer	Number	Percentage
1 (A001)	1	3,03%
2 (A002)	4	12,12%
3 (A003)	7	21,21%
4 (A004)	9	27,27%
5 (A005)	12	36,36%
Summary for Q023		
Are there any other regulations — not listed above — that are important for your organization to comply with or communicate compliance about?		
Answer	18	100,00%
ID	Answer	

4	Spanish Organic Law 3/2018 on Data Protection and Digital Rights (LOPDGDD), Law 34/2002 on Information Society Services and E-Commerce (LSSI-CE), and Law 2/2023 on whistleblower protection. These regulations are relevant to our privacy, digital law and compliance advisory services, including online-service obligations, internal reporting channels and governance controls.	
18	GDPR	
21	ePrivacy	
24	AI Act Data Act Anticorruption regulation	
27	Listed above? I can't go back in the survey and have not seen it... Of course, GDPR, AI ACT, possibly NIS II if education gets in the scope, India's New Data Law, to consider for communication and marketing data processing (recruitment of students)...	
46	Devoir de vigilance - Sapin 2 et autres dispositifs anticorruption	
65	Content management & Online Safety	
75	NIS2, eIDAS, RGD, RIA	
76	gdpr	
78	ENS	
80	Intern audit, is a very important step.	
92	media and communications law	
93	CPRA-PIPL-Loi 09-08-PIPEDA-UK GDPR-Digital PDP	
96	NIS 2	
104	NIS2, BSI IT-Grundschutz	
106	AI ACT / GDPR	
108	AI matters wrt Privacy & GDPR	
111	Many regulations and sets of rules—which have not been harmonized by the legislature—result in duplicative work and the need to distinguish between them, as well as the need for consistent documentation and uniform evidence of their implementation.	
Summary for Q025		
What are the most time-consuming compliance tasks for your team?		
Answer	Number	Percentage

Monitoring regulatory updates (SQ001)	14	31,11%
Understanding legal jargon and requirements (SQ002)	12	26,67%
Risk analysis and assessment (SQ003)	37	82,22%
Generating compliance reports (DPIA, TIA, FRIA, etc.) (SQ004)	31	68,89%
Auditing and internal reviews (SQ005)	26	57,78%
Ensuring data privacy and security (SQ006)	22	48,89%
Otheres	9	20,00%
ID	Answer	
4	Reviewing contracts, data processing agreements and third-party/vendor compliance documentation.	
16	Ensuring that product and business teams understand compliance priorities	
18	Convincing other departments to comply and to draft documentation	
21	(a) adapting compliance frameworks (b) monitoring implementation of remediation plans (c) building, training, animating the compliance ecosystem	
44	Documentation & reporting (administrative burden)	

65	Engaging with regulators	
92	Check third party compliance	
101	Responding to customer requests	
111	* Delegating complexity to the functional departments. * Fostering understanding and awareness within the functional departments regarding the necessity of the many, many regulations and rules.	
Summary for Q024(SQ001)[AI Act — Artificial Intelligence Act]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	1	2,22%
3 (A003)	9	20,00%
4 (A004)	4	8,89%
5 (A005)	31	68,89%
Summary for Q024(SQ002)[DGA — Data Governance Act]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage
1 (A001)	7	17,95%
2 (A002)	9	23,08%
3 (A003)	14	35,90%
4 (A004)	4	10,26%
5 (A005)	5	12,82%
Summary for Q024(SQ003)[GDPR — General Data Protection Regulation]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage

1 (A001)	0	0,00%
2 (A002)	0	0,00%
3 (A003)	2	4,44%
4 (A004)	6	13,33%
5 (A005)	37	82,22%
Summary for Q024(SQ004)[Data Act – Regulation on harmonised rules on fair access to and use of data]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage
1 (A001)	4	9,76%
2 (A002)	4	9,76%
3 (A003)	17	41,46%
4 (A004)	7	17,07%
5 (A005)	9	21,95%
Summary for Q024(SQ005)[NIS2 — Network and Information Security Directive]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage
1 (A001)	7	17,07%
2 (A002)	1	2,44%
3 (A003)	1	2,44%
4 (A004)	14	34,15%
5 (A005)	18	43,90%
Summary for Q024(SQ006)[DORA — Digital Operational Resilience Act]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage

1 (A001)	13	35,14%
2 (A002)	4	10,81%
3 (A003)	6	16,22%
4 (A004)	6	16,22%
5 (A005)	8	21,62%
Summary for Q024(SQ007)[CRA — Cyber Resilience Act]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage
1 (A001)	8	21,05%
2 (A002)	4	10,53%
3 (A003)	6	15,79%
4 (A004)	10	26,32%
5 (A005)	10	26,32%
Summary for Q024(SQ008)[EHDS – European Health Data Space]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage
1 (A001)	16	44,44%
2 (A002)	8	22,22%
3 (A003)	2	5,56%
4 (A004)	6	16,67%
5 (A005)	4	11,11%
Summary for Q024(SQ009)[eIDAS 2.0 — Electronic Identification & Trust Services]		
How important is it for your organization to comply with and communicate compliance to each of the following regulations?		
Answer	Number	Percentage

1 (A001)	8	22,86%
2 (A002)	5	14,29%
3 (A003)	8	22,86%
4 (A004)	10	28,57%
5 (A005)	4	11,43%
Summary for Q026(SQ001)[Health & life sciences (e.g. MDR, IVDR, clinical data rules)]		
How important is it for your organisation to communicate compliance with regulations that are specific to your sector or domain?		
Answer	Number	Percentage
1 (A001)	16	45,71%
2 (A002)	4	11,43%
3 (A003)	4	11,43%
4 (A004)	1	2,86%
5 (A005)	10	28,57%
Summary for Q026(SQ002)[Financial services & fintech (e.g. MiFID II, PSD2, DORA)]		
How important is it for your organisation to communicate compliance with regulations that are specific to your sector or domain?		
Answer	Number	Percentage
1 (A001)	12	34,29%
2 (A002)	7	20,00%
3 (A003)	5	14,29%
4 (A004)	5	14,29%
5 (A005)	6	17,14%
Summary for Q026(SQ003)[Insurance (e.g. Solvency II, IDD)]		
How important is it for your organisation to communicate compliance with regulations that are specific to your sector or domain?		
Answer	Number	Percentage

1 (A001)	17	51,52%
2 (A002)	5	15,15%
3 (A003)	3	9,09%
4 (A004)	3	9,09%
5 (A005)	5	15,15%
Summary for Q026(SQ004)[Energy & utilities (e.g. Clean Energy Package, REMIT)]		
How important is it for your organisation to communicate compliance with regulations that are specific to your sector or domain?		
Answer	Number	Percentage
1 (A001)	22	62,86%
2 (A002)	3	8,57%
3 (A003)	4	11,43%
4 (A004)	3	8,57%
5 (A005)	3	8,57%
Summary for Q026(SQ005)[Transport & mobility (e.g. autonomous vehicles, drones)]		
How important is it for your organisation to communicate compliance with regulations that are specific to your sector or domain?		
Answer	Number	Percentage
1 (A001)	18	54,55%
2 (A002)	6	18,18%
3 (A003)	5	15,15%
4 (A004)	3	9,09%
5 (A005)	1	3,03%
Summary for Q026(SQ006)[Agriculture & food (e.g. Farm-to-Fork, food safety standards)]		
How important is it for your organisation to communicate compliance with regulations that are specific to your sector or domain?		
Answer	Number	Percentage

1 (A001)	25	73,53%
2 (A002)	2	5,88%
3 (A003)	4	11,76%
4 (A004)	2	5,88%
5 (A005)	1	2,94%
Summary for Q026(SQ007)[Media & content (e.g. DSA content rules, copyright)]		
How important is it for your organisation to communicate compliance with regulations that are specific to your sector or domain?		
Answer	Number	Percentage
1 (A001)	14	36,84%
2 (A002)	1	2,63%
3 (A003)	7	18,42%
4 (A004)	7	18,42%
5 (A005)	9	23,68%
Summary for Q027		
If your sector is not listed above, or if you would like to elaborate on sector specific regulations that are relevant to your organisation, please describe them here.		
Answer	7	100,00%
ID	Answer	
4	Legal services and compliance consultancy, particularly in data protection, digital law and AI governance.	
28	French local authority, public service in the social sector	
46	vigilance , Sapin 2, CSRD	
101	Sector is not directly mentioned. Some new regs indirectly impact the housing area.	
104	Public Sector	
108	cross border data flows of PII	

111	All compliance requirements for the production and use of electronic communication devices (CRA, GDPR, AI Act, NIS2, Data Act, Repair Regulations, environmental regulations, carbon footprint, etc.)	
Summary for Q009(SQ002)[Reliability]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	1	2,38%
2 (A002)	0	0,00%
3 (A003)	0	0,00%
4 (A004)	11	26,19%
5 (A005)	30	71,43%
Summary for Q009(SQ003)[Integration with existing tools and workflows]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	3	7,32%
3 (A003)	6	14,63%
4 (A004)	18	43,90%
5 (A005)	14	34,15%
Summary for Q009(SQ004)[Customizable templates for reports and assessments]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	3	6,82%
2 (A002)	1	2,27%
3 (A003)	4	9,09%
4 (A004)	19	43,18%
5 (A005)	17	38,64%

Summary for Q009(SQ005)[Data privacy and confidentiality protection]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	0	0,00%
3 (A003)	2	4,76%
4 (A004)	7	16,67%
5 (A005)	33	78,57%
Summary for Q009(SQ006)[Cost-effectiveness and budget-friendly pricing]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	2	4,65%
2 (A002)	2	4,65%
3 (A003)	7	16,28%
4 (A004)	16	37,21%
5 (A005)	16	37,21%
Summary for Q009(SQ007)[User-friendly interface and ease of use]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	1	2,27%
2 (A002)	2	4,55%
3 (A003)	11	25,00%
4 (A004)	14	31,82%
5 (A005)	16	36,36%
Summary for Q009(SQ008)[Scalability to accommodate business growth]		

How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	1	2,38%
2 (A002)	5	11,90%
3 (A003)	11	26,19%
4 (A004)	11	26,19%
5 (A005)	14	33,33%
Summary for Q009(SQ009)[Training and support resources (e.g., tutorials, customer service)]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	1	2,33%
2 (A002)	8	18,60%
3 (A003)	9	20,93%
4 (A004)	15	34,88%
5 (A005)	10	23,26%
Summary for Q009(SQ010)[Ability to handle multiple regulations (e.g., GDPR, AI Act,...)]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	1	2,27%
3 (A003)	2	4,55%
4 (A004)	12	27,27%
5 (A005)	29	65,91%
Summary for Q009(SQ011)[Automated monitoring of compliance status]		
How important is each of the following features for a compliance tool?		

Answer	Number	Percentage
1 (A001)	1	2,27%
2 (A002)	4	9,09%
3 (A003)	4	9,09%
4 (A004)	16	36,36%
5 (A005)	19	43,18%
Summary for Q009(SQ012)[Collaboration features for teams and external partners]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	4	9,30%
3 (A003)	10	23,26%
4 (A004)	18	41,86%
5 (A005)	11	25,58%
Summary for Q009(SQ013)[Access to a centralized knowledge base or regulatory library]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	1	2,33%
2 (A002)	3	6,98%
3 (A003)	9	20,93%
4 (A004)	16	37,21%
5 (A005)	14	32,56%
Summary for Q009(SQ014)[Customizable dashboards for tracking compliance metrics]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%

2 (A002)	4	9,09%
3 (A003)	10	22,73%
4 (A004)	19	43,18%
5 (A005)	11	25,00%
Summary for Q009(SQ015)[Automated document completion (e.g., DPIA, TIA, FRIA templates)]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	2	4,65%
3 (A003)	4	9,30%
4 (A004)	17	39,53%
5 (A005)	20	46,51%
Summary for Q009(SQ016)[Proactive risk management and mitigation / traceability/auditability suggestions]		
How important is each of the following features for a compliance tool?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	1	2,27%
3 (A003)	1	2,27%
4 (A004)	21	47,73%
5 (A005)	21	47,73%
Summary for Q010		
Which of the following TRUST tools would be most valuable to your organization		
Answer	Number	Percentage
Real-time alerts for	21	46,67%

regulatory updates (RCA) (SQ001)		
Plain-language summaries of legal obligations (ROA) (SQ002)	14	31,11%
Risk scoring and legal data analysis (LRA) (SQ003)	30	66,67%
Automated report generation (RRA) (SQ004)	23	51,11%
Compliance gap analysis and scoring (RCE) (SQ005)	24	53,33%
Auditor collaboration tools (CPA) (SQ006)	17	37,78%
All of them (SQ007)	14	31,11%
None of them (SQ008)	2	4,44%
Otheres	1	2,22%
ID	Answer	
65	Cross regulatory analysis	
Summary for Q028(SQ001)[Access to new business partnerships and data-sharing agreements]		

How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	6	16,22%
2 (A002)	7	18,92%
3 (A003)	12	32,43%
4 (A004)	7	18,92%
5 (A005)	5	13,51%
Summary for Q028(SQ002)[Easier participation in public tenders and procurement processes]		
How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	6	15,00%
2 (A002)	6	15,00%
3 (A003)	15	37,50%
4 (A004)	9	22,50%
5 (A005)	4	10,00%
Summary for Q028(SQ003)[Faster and smoother regulatory audits or inspections]		
How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	4	9,76%
3 (A003)	10	24,39%
4 (A004)	13	31,71%
5 (A005)	14	34,15%
Summary for Q028(SQ004)[Reduced internal compliance management effort and costs]		

How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	2	4,88%
3 (A003)	6	14,63%
4 (A004)	14	34,15%
5 (A005)	19	46,34%
Summary for Q028(SQ005)[Increased customer trust and confidence in your data practices]		
How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	1	2,44%
2 (A002)	7	17,07%
3 (A003)	7	17,07%
4 (A004)	10	24,39%
5 (A005)	16	39,02%
Summary for Q028(SQ006)[Improved data quality leading to better business decisions]		
How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	2	5,00%
2 (A002)	4	10,00%
3 (A003)	10	25,00%
4 (A004)	14	35,00%
5 (A005)	10	25,00%
Summary for Q028(SQ007)[Competitive differentiation and market positioning]		

How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	7	17,95%
2 (A002)	3	7,69%
3 (A003)	13	33,33%
4 (A004)	11	28,21%
5 (A005)	5	12,82%
Summary for Q028(SQ008)[Access to data spaces, platforms, or ecosystems]		
How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	3	7,89%
2 (A002)	11	28,95%
3 (A003)	9	23,68%
4 (A004)	11	28,95%
5 (A005)	4	10,53%
Summary for Q028(SQ009)[Simplified cross-border operations within the EU]		
How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	7	17,50%
2 (A002)	7	17,50%
3 (A003)	8	20,00%
4 (A004)	9	22,50%
5 (A005)	9	22,50%
Summary for Q028(SQ010)[Stronger investor or stakeholder confidence]		

How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	5	12,50%
2 (A002)	8	20,00%
3 (A003)	11	27,50%
4 (A004)	11	27,50%
5 (A005)	5	12,50%
Summary for Q028(SQ011)[Ability to demonstrate accountability incase of incidents or disputes]		
How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	0	0,00%
2 (A002)	1	2,50%
3 (A003)	6	15,00%
4 (A004)	12	30,00%
5 (A005)	21	52,50%
Summary for Q028(SQ012)[Increased employee confidence in internal data handling]		
How significant are the following potential benefits or added values that your organisation could gain from complying with data governance frameworks?		
Answer	Number	Percentage
1 (A001)	2	5,13%
2 (A002)	6	15,38%
3 (A003)	10	25,64%
4 (A004)	13	33,33%
5 (A005)	8	20,51%

Summary for Q029		
Are there other benefits or added values — not listed above — that your organisation has experienced or would expect from showcased compliance?		
Answer	3	100,00%
ID	Answer	
4	Showcased compliance would strengthen the organisation's credibility as a legal and privacy advisory provider, support client due diligence, improve the traceability of professional decisions, and reduce reputational and liability risks.	
46	gain de temps	
57	Positive reputational opinion from Global Compliance Director and in the Global Group	
Summary for Q011		
How comfortable are you with using AI for compliance tasks?		
Answer	Number	Percentage
1 (1)	0	0,00%
2 (2)	4	3,39%
3 (3)	12	10,17%
4 (4)	11	9,32%
5 (5)	10	8,47%
Total (Answers)	37	100,00%
Number of cases	0	0,00%
Arithmetic mean	3,73	
Standard deviation	0,99	

Summary for Q017		
What concerns do you have about using AI for compliance?		
Answer	Number	Percentage
Hallucinations / invented results (SQ001)	38	82,61%
Data privacy (SQ002)	39	84,78%
Reliability (SQ003)	28	60,87%
Lack of transparency (SQ004)	23	50,00%
Cost (SQ005)	11	23,91%
Otheres	7	15,22%
ID	Answer	
4	Outdated or incomplete legal sources, insufficient traceability of conclusions, lack of meaningful human oversight, and uncertainty about responsibility for incorrect compliance recommendations.	
21	Lack of imagination, little value (too often this is 'what we did yesterday, quicker, less reliable, much much more expensive'). Environmental sustainability. Building new dependencies on a very or non existent fragile business model.	
28	Data control, no SaaS	
40	Negative impact on nature, loosing the autonomy to work/think without AI	
101	have AI make the rules which it then checks seems like a win-win	
104	No Human in the Loop	
111	Manipulation of LLMs and Datasets by Providers	
Summary for Q019		

Which questions did we forget? What else is important to you?		
Answer	7	100,00%
ID	Answer	
4	The survey could further address how the tools will ensure legal-source accuracy, version control and traceability of every recommendation. It would also be important to clarify the role of human review, allocation of responsibility for incorrect outputs, data retention and confidentiality, security and incident management, interoperability and data portability, and safeguards against vendor lock-in. For DPOs and legal professionals, the ability to evidence why a conclusion was reached, which sources were used and who validated the result is essential.	
16	EU digital data sovereignty and the threats of global fragmentation and data weaponisation	
21	Open. Agnostic. Portable. We don't start from scratch, we don't need yet another interface, a new separate platform. This needs open, documented APIs to feed and be consumable in tools and processes that exist or others will develop.	
27	What would be helpful and time saving is a shared compliance analysis of digital tools and softwares. All DPO analyse legal documentation, make same comments, request same modifications...	
57	Template for on line basic course for employee or graphic material to help them understand privacy compliance	
65	AI agent that could assist tracking internal discussions/decisions across regulatory domains and flag areas that require priority	
101	Is there too much focus on non-risky compliance topics? the risks are industry specific.	

Annex 5 – SME Focus Group Interview Guidelines

Introduction (15 min)

- Welcome & Icebreaker (10 min):
 - Moderator introduces the purpose:
"We're co-designing AI tools to simplify EU compliance for SMEs. Your insights will shape tools like the Regulatory Compliance Assistant and the Regulatory Report Assistant."
 - Participants introduce themselves:
Name, role, institution, and one compliance challenge they face
- Ground Rules (5 min):
 - Confidentiality, no wrong answers, encourage open discussion.
 - Explain recording, get consent

Pain Points & Challenges (45 min)

- Opening Question:
"In a nutshell: How is your current compliance process structured? What works? What doesn't?"
(10 min, open discussion)
- Follow-ups:
 - *"What EU regulations are most burdensome for your business? Why?"*
(Multi-select if online + 10 min discussion)
 - *"How do you currently stay updated on regulatory changes? What do you find most effective or frustrating about this process?"*
(5 min, open discussion)
 - *"How do you currently ensure your services/products are EU-compliant?"*
(word cloud if online + 10 min discussion)

Where is help needed? (20 min)

- Guided Discussion: (10 min each)
 - *"If you could change one thing about your current compliance process, what would it be and why?"*
 - *"What compliance tasks do you wish you could offload to a junior colleague or AI? Why?"*

Envisioning the Solution (30 min)

- Tool-Specific Breakouts:
(20 min, divide into 2 groups, each group discusses 3 tools for 10 min, then switch)
 - Group 1:
 - RCA: *"How should a Regulatory Compliance Assistant alert you to new regulations? What format (email, dashboard, etc.) would be most useful?"*
 - ROA: *"What would make a Regulatory Obligations Analyzer actionable for your team? (e.g., checklists, plain-language summaries)"*
 - LRA: *"What features would help you analyse regulatory risks proactively? (e.g., risk scoring, historical data analysis)"*
 - Group 2:
 - RRA: *"What would streamline report generation for you? (e.g., templates, automated data collection, integration with existing tools)"*
 - RCE: *"How should a Regulatory Compliance Evaluator present compliance gaps and scoring? (e.g., dashboards, detailed reports)"*
 - CPA: *"What features would facilitate certification processes for you? (e.g., document automation, auditor collaboration tools)"*
 - Group Prioritization & Feedback: (10 min)
 - *"Which of these tools do you think would have the biggest impact on your work? Why?"* (Open discussion)
- "For each tool, what is the ONE feature you need most?"*
(word cloud if online + 10 min discussion)

Trust & Adoption (10 min)

- Key Questions:
- *"What would make you trust an AI tool for compliance?"* (Open discussion)
- *"What reservations or concerns do you have about using AI for compliance tasks?"*

Wrap-Up & Next Steps (5 min)

- Recap: Moderator summarizes key themes.
- Q&A: *"What questions or concerns do you have about the TRUST project?"*
- Closing: Thank participants, share next steps (e.g., survey follow-up, co-design opportunities).

Annex 6 - SME Focus Group - Workshop 1

Key Pain Points & Insights

Overwhelming Complexity and Volume of Regulations

- Multiple extensive laws and directives need to be connected into single algorithms or workflows to shortcut the time required for specific tasks.
- Cross-sector knowledge is continuously required to handle compliance, data, metadata, and coding, which involves coordinating many people across different domains.
- Navigating very long regulatory lists and documents, such as those required for GDPR compliance, is highly tedious and time-consuming.

Tracking and Identifying Regulatory Updates

- Finding out when regulations change and determining if those changes actually affect a specific business is incredibly difficult.
- Keeping up with changes is often a matter of "luck" rather than a reliable, systematic process.
- Traditional search methods like manually searching Google are inefficient and unreliable for timely updates.

Vague and Inconsistent Legal Requirements

- Regulations, especially around data protection, are often perceived as vague or "blurry" regarding what data can be stored and when consent must be requested.
- This ambiguity leads to overly cautious defaults, such as blocking data use entirely, which hinders business operations.
- Even minor B2B consulting tasks involving customer data analysis require tedious, disproportionate efforts to obtain additional client consents due to strict data processing rules.

Inefficient, Person-Dependent Processes

- In smaller firms, compliance is often managed by a single individual (such as the managing director) who must manually sift through documents to determine what is relevant, diverting time from core business activities.

Current Workarounds

Manual Search and Tracking

- Relying on casual news reading, luck, or periodic Google searches to discover regulatory updates.
- Monitoring specialized IT news portals, though this is not done consistently every day.

In-House AI Tools and Custom Assistants

- Building custom GPT models (using ChatGPT) and feeding them company data to track compliance. However, this is flagged as unreliable because the AI can produce excessive, irrelevant details and might not cover all regulatory gaps.
- Developing completely custom in-house products, as done by Speaker 1 to aggregate complex post-marketing system regulations into a single block.

Basic Internal Document and Task Management

- Assigning compliance tasks to a single person who manually manages and distributes compliance documents.
- Adding and expanding acceptance criteria within ticket systems or project management tools whenever new rules are identified.
- Getting condensed case-by-case training or support from specialized corporate offices in larger company settings.

What Success Looks Like

Automated and Centralized Integration

- Having all regulatory updates centralized, updated automatically, and tailored specifically to the company's products, services, and business model.
- Complete integration of updates directly into existing workflows—such as receiving actionable summaries automatically in an existing ticket system (e.g., Teams or Slack) rather than having to log into a separate compliance application.

Actionable and Simplified Guidance

- Having complex legal language translated into plain, understandable, and structured language.
- Receiving clear, practical examples of how specific paragraphs apply to a business to improve comprehension.

- Knowing exactly what needs to be changed and when (e.g., receiving a direct notification that a specific paragraph must be added to a website's privacy policy by a certain deadline).

Product Feedback & Next Steps

Regulatory Compliance Assistant (RCA)

- General Reaction: Participants found the tool highly necessary to avoid relying on luck for updates.
- Notification Preferences:
 - Standard email notifications are generally disliked due to cluttered inboxes and spam risks.
 - Speaker 1 and Speaker 3 highly prefer integrations with existing communication tools like Slack or Microsoft Teams.
 - Speaker 1 suggested utilizing RSS feeds for a more sustainable, lightweight infrastructure that easily integrates into other company systems.
 - Speaker 1 emphasized that output formats must be highly customizable (e.g., CSV files) to fit different organizational structures.
 - Speaker 3 requested that notifications allow user-level configuration regarding detail depth, focusing on differences/changes rather than sending full-length documents.
 - Speaker 2 expressed a need for complex, structured timing updates integrated directly into custom AI models, categorized by degrees of importance (high, medium, low).

Regulatory Obligations Analyzer

- General Reaction: Accepted as a valuable translation tool from "legal speak" to "normal speak."
- Feature Requests:
 - Speaker 1 requested a quick-toggle button (similar to "easy language" buttons on news websites) to easily switch between the official legal text and the simplified version.
 - Speaker 3 requested that the tool generate concrete, practical, and individualized examples based on the company's profile to make the translated paragraphs easier to comprehend.

Legal Risk Analyzer

- General Reaction: Positive reception regarding proactive risk management.
- Feature Request:
Speaker 1 recommended a simple, three-stage traffic light system (green, yellow, red) to clearly visualize where the highest penalties or compliance risks lie.

Report Generation Tool

- General Reaction: Divided opinions on how much control should be handed over to the AI.
- Feature Requests:
 - Speaker 1 prefers a fully automated, hands-off approach where the tool completely generates reports (such as GDPR reports) with a single click.
 - Speaker 3 prefers keeping control over the final document, wanting the tool to provide quick, one-sentence summaries, relevant tags, and references to changes, while leaving the actual drafting to the user.
 - Speaker 2 noted that the reporting interface should accommodate the entire lifecycle and various phases of reporting, prioritizing a clear mindset and comfort zone for the user.

Regulatory Compliance Evaluator

- General Reaction: Highly valued, especially if it can utilize actual company data.
- Feature Request:
Speaker 1 requested that this tool actively propose concrete text modifications. For example, if it has access to a Git repository, it should identify missing paragraphs in the website's privacy policy and draft the exact text to be inserted.

Compliance Partner Assistant (CPA)

- General Reaction: Seen as a helpful bridge for communication with auditors and authorities.
- Feature Requests:
 - Speaker 1 emphasized that a "human-in-the-loop" is absolutely mandatory because the ultimate liability remains with the human compliance manager.
 - Users highlighted the need for real-time evidence, continuous monitoring, and automated checklist tracking to simplify the certification process.

Priority & Feature Ranking

- **Most Important Tool:**
The Regulatory Compliance Assistant (RCA) for tracking and alerting on regulatory changes was ranked as the absolute highest priority. Speaker 1 noted that if a company does not know a regulation exists, none of the other analytical or translation tools can help.
- **Key Focus Area:**
Risk scoring and document management were ranked as the top focus areas for development over automated report generation.

Trust, Credibility, & AI Concerns

- **The Transparency & Source Requirement:**
Providing direct links to original legal sources and documentation is essential for users to trust the AI's output.
- **Liability and Error Disclaimer:**
It is understood that the tool cannot assume legal liability. Clear disclaimers indicating the text is AI-generated are required.
- **Trust Score Concept:**
Speaker 1 proposed implementing a "Trust Score" (e.g., from 0 to 100) generated by a secondary, independent AI model that evaluates the reliability and accuracy of the primary AI's compliance answers.

Annex 7 - SME Focus Group - Workshop 2

Company Backgrounds and Problems

- Participating companies in general
- These are organizations and consultants who must comply with EU regulations.
- Structures are often fragmented, with unclear responsibility for compliance issues (e.g., tasks often land with IT or a single Compliance Officer).
- Many companies struggle with sector-specific regulations (e.g., chemical sector, customs databases like TARIC/ECICS) and the lack of integration between legislative databases.
- Goals and problems to be solved
 - Resource minimization: Compliance efforts should be reduced to a maximum of two hours per month.
 - Responsibility and knowledge management: Need for targeted information distribution to avoid knowledge loss during staff turnover (e.g., retirement of long-standing Compliance Officers).
 - Regulatory mapping: Identifying which laws (e.g., AI Act, GDPR, CLP Regulation) apply to their company or products and which exemptions exist.
 - Companies seek plain-language guidance and simple checklists to streamline compliance processes.
 - Data protection and security-by-design are critical concerns, especially for sensitive sectors like chemicals.

Key Pain Points & Insights

Most Important Problems and Challenges

- Information overload and lack of relevance in notifications
- Standard newsletters or updates are often ignored due to lack of time or relevance.
- Information is frequently sent to department heads instead of the actual executors.
- Participants emphasized the need for filtering mechanisms to avoid irrelevant information (e.g., compliance alerts for child protection when unrelated to the business).

Internal responsibilities and knowledge loss

- Compliance responsibility is often passed between departments (IT, data protection, management), leading to inefficiencies.
- High risk of knowledge loss during staff turnover (e.g., retirement of Compliance Officers).

- Companies lack continuous processes or permanent access to historical compliance decisions

Complexity of legal texts and lack of data linking

- Legal texts are written in complex legalese and require translation into plain language for operational use.
- Lack of direct links between legislation and databases (e.g., CAS numbers missing in CLP Regulation despite their availability in customs databases).
- Better integration of EU databases (e.g., TARIC/ECICS) was highlighted as a critical need

Classification challenges:

- Determining whether a company/product falls under a regulation (e.g., AI Act) or qualifies for exemptions is highly complex.
- Participants requested simple checklists with yes/no options, legal sources, and plain-language explanations.

Misinterpretations and trust risks in AI systems

- Concerns about hallucinations, incorrect legal sources, or misinterpretations by AI during compliance analyses.
- Inconsistent quality due to statistical nature of LLMs and variability in prompting.
- Liability risks: Companies may adopt AI suggestions without verification, leading to legal consequences.
- Participants emphasized the need for traceable decisions with correct citations and human validation ("Human leads, AI supports") [1].
- No "learning" of the LLM model was demanded to prevent corruption of the system.

Current Workarounds

- Manual research and information procurement: Use of newsletters, authority websites, or network posts (e.g., LinkedIn).
- Self-programmed aids and proprietary nomenclatures
 - Use of local AI assistants (e.g., speaker 1's self-programmed tools)
 - Some participants use AI tools like ChatGPT or Claude for research, but this is not systematic.
 - Some companies rely on weekly dossiers compiled by AI agents to stay updated
- Manual maintenance of proprietary data structures (e.g., number-based labeling systems for external data sources).
- Privacy-by-design and security-by-design are prioritized, especially for sensitive data.

Definition of Success (What success means to users)

Targeted filtering instead of information overload

- Information should be filtered, bite-sized, and targeted to avoid manual processing.
- Participants want a system that prepares information so they "don't have to chew for themselves".

Simple language and clear instructions for action

- Legal texts should be translated into plain language.
- Checklists with yes/no options, legal sources, and explanations for exclusions ("Why does this not apply to me?").
- Risk scoring and alerts were identified as valuable features for proactive compliance management.

Human control as the standard ("Human leads, AI supports")

- AI should be a tool (like a pencil or hammer) to facilitate work, but final validation and responsibility must remain with humans.
- Participants stressed that AI must not replace human decision-making in compliance matters.

Product Feedback & Next Steps

Reactions to the TRUST Project and Feedback on Components

- General feedback on the AI agent system
- The detailed planning of agents was positively highlighted.
- Concerns about complexity: Speaker 1 warned that English terminology and system complexity might deter medium-sized customers.
- Human validation is mandatory: AI is seen as a support tool, not a replacement for human decision-making.

Feedback on specific agents and functions

- Regulatory Compliance Assistant (Notifications on new/changed EU regulations):
 - Prioritized as the most useful tool by participants.
 - Notifications should be sent via email to the Compliance Officer but with an opt-in filter to avoid spam.
 - Permanent storage (e.g., knowledge base, wiki, or Slack) was suggested to prevent loss during absences.
 - Some participants preferred no emails but instead a dedicated platform for compliance updates.

- **Obligations Analyzer** (Translation of regulation into understandable language):
 - Desired: A combined approach of a reference encyclopedia and a chatbot for non-binding questions.
 - Annual review workshops were suggested to ensure continuity during staff changes.
- **Legal Risk Analyzer** (Assessment of penalties and risks):
 - Useful for proactive risk management, with a suggested quarterly rhythm for notifications.
 - Data protection is critical: Company data must remain local and protected from access by investigative authorities.
- **Report Assistant** (Creation of compliance reports):
 - Creation via a guided questionnaire filled out by the data protection officer, followed by AI-generated sample reports.
 - No independent interpretation by AI: Final control must remain with humans.
- **Compliance Evaluator** (Summary of gaps):
 - Desired: A short summary with legal sources and action outlines in the user's native language.
- **Certification Assistant** (Facilitating certification processes):
 - Desired: A simple checklist of requirements to tick off.

Objections, Concerns, and Technical Worries

Error tolerance and quality assurance:

- Low tolerance for hallucinations or incorrect legal references.
- Traceability is essential: AI decisions must include correct citations.
- Consistent quality is a concern due to the statistical nature of LLMs.

Further development and data security ("No learning"):

- Uncontrolled model training with unstructured user data could corrupt the system.
- Clear separation required: Either the model is maintained by a controlled external body with verified data, or a secure error-reporting mechanism must be established.

Liability and misinformation:

- High concern about legal consequences from AI misinterpretations.
- Disclaimer of liability and explicit human verification are necessary.

Open Questions from Participants

Technical details and licensing:

- Under which open-source license will the tool be released?

- Implementation and testing phase: How does local installation work, and when will the first models be available for testing?

Long-term financing:

- How will the tool be maintained and developed after the three-year EU-funded project period if it remains free?

Additional Questions:

- How can users "stay in the loop" regarding the TRUST project's progress?
- What are the next steps for co-design and testing sessions?

Annex 8 – DPO Focus Group Interview Guidelines

1. Welcome & Setting the Stage (15 min)

- Opening & Icebreaker (10 min)
 - Moderator introduces the purpose: "As DPOs and compliance experts, you're on the front lines of navigating complex, fast-evolving regulations—from GDPR and the AI Act to sector-specific laws. Today, we're co-designing AI tools to simplify your workflow, not replace your expertise. Your insights will directly shape tools like the Regulatory Compliance Assistant (RCA) ensuring they address your pain points, from obligation registers to risk scoring and audit-ready reporting."
 - Participants introduce themselves:
Name, role, institution, and one compliance challenge they face
- Ground Rules (5 min)
 - Confidentiality, no wrong answers, encourage open discussion.
 - Explain recording, get consent

2. The Compliance Landscape: Your Realities (45 min)

- Opening Discussion (10 min): "In a nutshell: How is your current compliance process structured? What works? What doesn't?"
- Targeted Follow-Ups:
 - Regulatory Overload (10 min): "Which EU or national/sector-specific regulations (e.g., GDPR + AI Act) consume the most time? Why?" (Multi-select if online + 10 min discussion)
 - Staying Updated (5 min): "How do you track regulatory changes now? What's the most effective—or frustrating—part of this process?" (5 min, open discussion)
 - Compliance Assurance (10 min): "How do you prove compliance today? What tools or methods do you use?" (word cloud if online + 10 min discussion)

3. Pain Points & Wish Lists (20 min)

- Guided Discussion (10 min each): "If you could change one thing about your current compliance process, what would it be and why?"
- "What compliance tasks would you trust a junior colleague or AI to handle? What would you never delegate?"

4. Co-Designing Your Ideal Tools (30 min)

- Breakout Groups (20 min):
- Divide into two groups; each discusses three tools for 10 minutes, then switch.
- Group 1: Proactive Compliance

- RCA (Regulatory Compliance Assistant): "How should this tool alert you to new or updated regulations? Email? Dashboard? And how should it prioritize them?"
- ROA (Regulatory Obligations Analyzer): "What would make this tool truly actionable? For example: Automated obligation registers? Mapping across GDPR, AI Act, and national laws?"
- LRA (Legal Risk Analyzer): "What features would help you proactively analyze risks? Think: Objective risk scoring? Benchmarking by sector/company size? Narrative summaries for auditors?"
- Group 2: Efficiency & Certification
 - RRA (Regulatory Report Assistant): "What would streamline report generation for you? Templates? Automated data collection? Integration with tools like DataGuard or OneTrust?"
 - RCE (Regulatory Compliance Evaluator): "How should compliance gaps and scores be presented? Dashboards? Detailed reports? And how should it handle regional variations?"
 - CPA (Certification Process Assistant): "What would make certification processes faster and cheaper? Document automation? Auditor collaboration tools? Pre-mapped criteria for schemes like Europrivacy?"
- Group Prioritization (10 min):
 - "Which of these tools would have the biggest impact on your work? Why?"
 - "For each tool, what's the ONE non-negotiable feature you need?"
 - (Word cloud if online)

5. Trust, Adoption & Digital Sovereignty (10 min)

- Key Questions: "What would make you trust an AI tool for compliance? Think: Transparency? Human oversight? Proven accuracy?"
- Digital Sovereignty Check: "How important is it that the tool is 100% EU-hosted with no data transfers outside the EEA? Would you use a tool that wasn't?"

6. Wrap-Up & Next Steps (5 min)

- Recap: Moderator summarizes top pain points and tool priorities
- Q&A: "What questions or concerns remain about the TRUST project?"
- Closing: Thank participants for their expertise—"Your input will directly shape tools designed by DPOs, for DPOs."
- Next Steps:
 - Invite participants to join upcoming co-design sessions (focus groups before summer; report deadline: September 2026).
 - Highlight outreach plans

Annex 9 - DPO Focus Group - Workshop 3

The Problem They Are Trying to Solve

- The participants are looking to streamline compliance with overlapping EU and regional legislations (such as GDPR and the AI Act) while minimizing manual effort.
- Specifically, Speaker 1 is currently undertaking a massive data mapping exercise to produce records of processing activities (ROPA) under data protection laws, operating without an independent data management department.
- The overall cohort is seeking a way to manage compliance proactively, translate complex regulatory updates into actionable tasks, and establish reliable internal training and reporting mechanisms.
- Several participants highlighted that data inventory / ROPA is among the most challenging recurring tasks.
- Participants also noted the difficulty of keeping final legal assessments with qualified experts while offloading repetitive tasks such as document tracking, first drafts, checklists, and regulatory monitoring to AI.

Key Pain Points & Insights

Regulatory Complexity and Framework Overlap

- Inconsistent and Overlapping Regulations: DPOs and compliance teams struggle to coordinate multiple complex frameworks simultaneously.
- Specific overlapping regulations causing friction include the AI Act (most burdensome, cited by 6 respondents), NIS2 (cited by 3), GDPR, DORA (Digital Operational Resilience Act), the Data Act, the Cyber Act, the Cyber Resilience Act (CRA), and sector-specific rules like Health Data regulations.
- There is a major challenge in navigating the inconsistencies between various EU laws, which are written separately but heavily influence one another. Cross-mapping between GDPR, the AI Act, and national laws was highlighted as a critical unmet need.
- Contractual Compliance Layer: Beyond public legal regulations, there is a burdensome second layer of ensuring compliance on a contractual level, which often requires extensive internal legal discussions to verify if the organization is on safe ground.
- Regional and International Inconsistencies: Managing international corporate groups introduces severe coordination hurdles due to different regional requirements.
- Compliance standards and the strictness of legal consequences vary highly by country. For example, German and Austrian regions face much tighter local requirements (such as the Strafgesetzbuch) than other

European countries, meaning CEOs could face jail time for non-compliance.

- Global corporate IT compliance policies frequently clash with localized laws. For instance, a global policy cannot simply "rule over" local operations if local regulations (like India's data protection rules) contradict them.
- Centralized compliance roles coming from a third country often do not match local requirements in international matrix organizations.
- Clarity on local national requirements or derogations as they interact with EU law was identified as a critical missing piece.

Operational and Resource Constraints

- Severe Resource and Time Deficits: Compliance teams — especially in smaller entities and SMEs — face a lack of physical time, budget, and dedicated personnel to stay on top of rapid compliance changes.
- Many organizations rely on a single person to handle all compliance processes, in constant struggle to communicate regulations to relevant persons while staying up to date.
- SMEs in particular often do not have compliance at the top of their priorities and only act when obliged, typically without large budgets.
- Organizations working with EU funds face additional constraints: any compliance service must follow procurement rules and be justified, proportionate, and auditable.
- Internal Communication and Executive Buy-in: DPOs find it difficult to get CEOs to listen, obtain corporate appreciation for their work, and successfully train general team members to understand compliance requirements.
- In matrix organizations, it is particularly hard to secure sponsorship for compliance investment.
- Late-Stage Integration: Compliance is rarely integrated into project designs from the start, leaving teams to scramble to address privacy and cybersecurity issues late in the development cycle.
- Embedding compliance at the start of every project — not at the end — would reduce risks, save time, and make privacy, cybersecurity, and AI governance easier for teams.
- Pace of Technological and Legal Change: The rapid speed of AI development makes it highly difficult to keep up with daily updates, new decisions, and changing guidelines.
- A key structural issue is that the speed at which new technologies (especially AI tools) are adopted often outpaces the time needed to assess risks, update documentation, and train users properly.
- Local Hub Networks and Departmental Champions: Large organizations build localized hubs where people in the same region coordinate, or

establish internal "data protection champions" in every department to cascade a data protection culture downward.

Current Workarounds

- **Fragmented Information Gathering:** Teams stay updated through a time-consuming combination of newsletters, LinkedIn experts, community forums, academic research, podcasts, and directly following European Commission or national data protection authority updates.
- Specific sources mentioned include: EDPB, EDPS, AEPD, ENISA, GDD membership, public affairs teams, social media, and following other DPAs and expert communities (e.g., CEDPO).
- **Custom AI Tools with Reliability Issues:** Some teams have programmed their own custom AI agents to summarize updates. A key workaround is ensuring these custom tools provide sources immediately following each paragraph so humans can manually verify the text to catch AI hallucinations.
- Participants noted that AI-provided citations to court decisions are often of poor quality, and that AI is fundamentally statistical — a fact that must be made transparent to users.

What Success Looks Like

- **The "One-Pager" and Structured Checklists:** A simplified, highly visual compliance process consolidated onto a single page or PowerPoint.
- Success is having a clear, step-by-step checklist (spanning IT, marketing, and legal) so employees immediately know the exact process to follow and whom to contact without spending days searching for information on a global scale.
- Pre-made forms and checklists handed out proactively (ideally by the legislator or tool) before laws enter into effect were cited as an ideal outcome.
- **Early-Stage Compliance Integration:** Embedding privacy, compliance, and cybersecurity natively into the initial design phase of every project rather than treating it as an afterthought.
- **Actionable Risk Quantifying:** Receiving proactive, localized early warning alerts and risk scoring.
- This includes calculating the financial impact of risks (such as the potential cost of data breaches like credit card monitoring, which can far exceed regulatory fines) to help justify compliance budgets to board members.
- Risk prioritization should consider legal impact, deadlines, risk level, sector relevance, and whether action is required.
- **Automated Documentation and Templates:** Shifting repetitive manual labor — like gathering evidence, tracking documents, updating registers, and drafting reports — to automated systems that can pre-fill templates and export compliant outputs.

- Tasks participants would most like to offload to an AI include: document tracking, first drafts, checklists, regulatory monitoring, DPIA creation, data inventory / processing registry updates, KPI follow-up, policy and procedure drafting, newsletters on new rules, contract evaluation, data gathering for systems and processes, and identifying all relevant laws, sections, and case law.
- Final legal assessment must remain with a qualified expert.

Product Feedback & Next Steps

Regulatory Compliance Assistant (RCA)

- Preferred Notification Methods: A strong preference emerged for a centralized dashboard as the primary interface, supplemented by direct emails specifically for high-priority or urgent regulatory changes.
- Participants favored: dashboard with export interface, email notifications prioritized by impact on the company (low / high / severe), and the option to set individual parameters for prioritization.
- Push notifications via platform were suggested as an additional delivery channel.
- Prioritization Logic: Regulatory change alerts should be prioritized based on legal impact, deadlines, risk level, sector relevance, and whether action is required.
- Scope: The RCA should include cross-mapping of GDPR, AI Act, NIS2, and national laws, with automated obligation registers and clear deadlines.

Regulatory Obligations Analyser (ROA)

- Actionable Features: Participants requested that this assistant automatically generate obligation registers, set clear deadlines, establish risk scoring, assign task owners, and provide checklists.
- Automated obligation registers with cross-mapping between GDPR, AI Act, and national laws, with clear deadlines, risk scoring, assigned owners, evidence templates, and practical action checklists were explicitly requested.
- Integration: The tool should integrate smoothly with existing team platforms like Notion, provide "one-click" analysis of existing documentation, and assist in maintaining a data inventory register for DPIAs and tracking data breaches.
- Top requested single feature: "Check compliance dataflow," "data inventory," and "check compliance document."

Legal Risk Analyser (LRA)

- Risk Assessment and Alerts: The assistant should provide proactive alerts, horizon scanning, and a visual risk heat map spanning global and local levels.
- Deadline reminders were explicitly highlighted as essential.

- Risk assessment should be informed by current regulatory decisions, and include a compilation of decisions, guidelines, opinions, and news.
- Financial Risk Quantifying: Features should include risk scoring based on both impact and urgency. This includes calculating the realistic costs of data breaches (e.g., credit card monitoring) which often exceed actual regulatory fines, helping present worst-case scenarios to executives.
- Information on how often fines are issued and how high they are for specific failures was specifically requested.
- Contextual Data Visualizations: The tool should synthesize regulatory decisions, opinions, and news while mapping data transfers and visualizing complex data flows across departments.
- Participants requested the ability to analyze different data categories and get a better overview of data transfers and associated risks — with data flows visualized directly.
- Supplier data breach lists were also requested as a contextual input.
- "One-Pager" Generation Request: Speaker 2 requested a feature where the AI automatically aggregates data from various systems and departments to generate a unified, draft "one-pager" process overview categorized by driver (IT, financial, process, health data) to serve as an instant, cross-departmental starting point.
- Top requested single feature: "Heat map (global/local)" and "deadline reminders."

Regulatory Report Assistant (RRA)

- Audience and Format Customization: The tool must allow users to select their target audience (e.g., supervisory authorities vs. corporate stakeholders) and automatically reorganize the content and tone accordingly.
- The same content should be reorganizable for different audiences as a core feature.
- Templates and Evidence Integration: Users requested automated, pre-filled evidence templates, specific bullet-point summaries, and exportable formats (Word or PDF) that comply directly with official guidelines, datasheets, and checklists (with RAG red/amber/green status).
- Version control, audit trails, obligation mapping, and clear summaries showing risks, actions, owners, and deadlines were also requested.
- Sourcing and Languages: Reports should feature interactive links to allow further interrogation of source information and must support multi-language generation to assist with regional localization.
- Configurability: Reports should be configurable based on Key Risk Indicators (KRIs), with the ability to select the input, focus, and addressed group.
- The tool should suggest reports that have been proven helpful in similar contexts.
- Top requested single feature: "Documentation" and "automated templates."

Regulatory Compliance Evaluator / RCE (Compliance Gaps)

- Visual Gaps and Actionable Steps: The interface should use a simple, visual traffic-light or heat-map system paired with a Capability Maturity Model (e.g., Level 1 = ad hoc, Level X = optimized).
- Traffic light reports combined with explanation of possible risks and way out (remediation path) were explicitly requested.
- Reports must be readable with narrative, visuals, and actionable steps suitable for sharing with non-compliance personnel.
- Plain-Language Explanations: Gaps must be presented with clear, plain-language explanations, assigned risk scores, and step-by-step actionable instructions designed so they can be easily understood by non-compliance personnel.
- Each gap should include: a short explanation, a score, the risk level, and the actions needed to fix it.
- Top requested single feature: "Traffic-light gap scoring."

Certification Process Assistant (CPA)

- Process Simplification: Key feature requests include clear certification checklists, required evidence templates, automated document tracking, deadline reminders, visual progress updates, and the capability to scrape prep documents using AI.
- Wizards, interpretation detail checklists, and maturity assessments tailored to the specific certification being targeted were requested.
- A maturity check that adapts based on which certification the organization is aiming for was highlighted.
- Feedback Loop: DPOs want the assistant to evaluate submitted applications and provide clear feedback on why an application might be rejected so they can learn from the audit.
- Specifically, the accreditation process for DPOs is noted as time-consuming; automating the initial assessment of submitted applications (accepted/not accepted) would save significant effort.
- The Credibility of the Seal: Participants, including Paul and Speaker 3, emphasized that the certification must have broad, market-leader recognition (similar to how Allianz adopted the Euro Privacy seal) to motivate SMEs to pursue it.
- The tool should target an "80% satisfaction standard" to establish a highly accessible, trusted, and unified pan-European baseline that prevents weak links in supply chains.

- A pan-European certification process recognised by public authorities and regulatory agencies was explicitly called for.
- Organizations are generally willing to invest in voluntary certification only when tangible benefits are expected — e.g., strengthening competitive position or winning public tenders.
- Top motivations for compliance certification (word cloud results): Trust (4 mentions), Transparency (3), Competitive Advantage, Building Trust, Customer Reassurance, Customer Requirement, ESG Rating, Winning Contracts, Reputational Enhancement, and "Being on the Safe Side."

Overall Preferences and Ranking of Assistants

- Risk Scoring and Alerts: ~30 points (average)
- Document / Evidence Management: ~30 points (average)
- Automated Monitoring of Changes: ~19 points (average)
- Reporting Support: ~12 points (average)
- Plain-Language Guidance: ~6 points (average)
- Most-Requested Single Tool Feature (word cloud from survey): "Automation" and "check compliance" ranked highest, followed by "compliance monitoring," "data inventory," "documentation," "open source," "native API," and "user friendly tool."
- Core Product Expectations: The final product must feature an open architecture, be community-driven, offer native APIs, and maintain an open-source format

General AI Skepticism, Objections, and Trust Requirements

- Human-in-the-Loop Requirement: All participants agreed that AI tools must not replace DPOs. A human reviewer is mandatory before acting on any recommendations.
- Speaker 5 emphasized that user interfaces must be designed in accordance with Article 14 of the AI Act to facilitate human review, ensuring the AI's logic is easily interpretable, structured for human thinking, and simple to interrogate.
- The tool must be built to help the DPO in their job — not to replace them ("Don't sell a car to be an airplane").
- The Hallucination Challenge: Speaker 5 and Speaker 3 noted that simply showing sources is insufficient because LLMs are prone to hallucinating the legal sources themselves.
- The AI must be designed to avoid "sycophancy" (flattering the user) and instead match a DPO's naturally skeptical mindset.
- AI-provided citations to court decisions are often of poor quality. AI is fundamentally statistical in nature — this must be made transparent and communicated clearly to users.

- Recommended trust features: good court decision interpretation, proven sources, percentage probability of a hit, transparent citations, up-to-date databases, and human-in-the-loop design.
- Data Privacy and Retention Boundaries: Trust relies on absolute GDPR compliance, zero data retention policies, local database hosting options, and strict guarantees that no user input or confidential corporate data is used to train the underlying models without explicit consent.
- Participants explicitly stated: "No sharing of my inputs. No transfer to LLM learning."
- The tool must itself comply with the AI Act first.

European Hosting Debated:

- Speaker 3 argued that 100% EU-hosting is not a black-and-white constraint. Since compliance guidance rarely involves personal data, organizations might prefer utilizing superior, US-hosted models (like Claude via Amazon Bedrock) to ensure they have the most advanced and competitive technology, provided the overall package is persuasive and priced correctly.
- However, another pointed out that geopolitics and US administration rules can "weaponize" access, sometimes preventing European professionals from using certain US models.
- Workshop participants noted a strong preference for a EU-based AI system, while acknowledging dependency on US tech for most tools and apps.
- For sensitive compliance work involving personal data, confidential documents, or compliance evidence, EU hosting was described as "almost a requirement" and a major trust factor. If a non-EU-hosted tool is used, strong GDPR safeguards, contractual guarantees, transparency on subprocessors, encryption, data residency options, and a documented Transfer Impact Assessment would all be required
- Data localization and access management were highlighted as top concerns for next steps and rollout.

Project Management and Development Objections

- Call for Agile Methodology: Speaker 3 raised concerns about the project's long timeline, advising the 19-partner consortium to adopt a strict Scrum/agile approach.
- He urged the project owners to make painful decisions, prioritize the vital 20% of requirements that satisfy 80% of user expectations (Pareto principle), and deliver a visible, working product within three months rather than waiting the full three years.
- Workshop participants echoed the need for transparency about next steps and a time plan for rollout.

Annex 10 - DPO Focus Group - Workshop 4

Key Pain Points & Insights

Evolving and Fragmented Regulatory Landscape

- Keeping up with a high volume of complex, intersecting EU regulations is highly burdensome.
- Specific regulations causing significant strain include:
 - General Data Protection Regulation (GDPR)
 - Artificial Intelligence Act (AI Act)
 - Corporate Sustainability Reporting Directive (CSRD)
 - Cyber Resilience Act (CRA)
 - European Health Data Space (EHDS)
 - Data Act
 - EU Omnibus
 - NIS2
 - Various ISO standards (such as ISO 27001)
- Disconnects frequently occur between localized compliance teams and centralized corporate headquarters in international or multinational organizations.
- Compliance professionals struggle to bridge the gap between European Union frameworks and non-EU international frameworks, such as Chinese and African regulations.

Operational and Communication Inefficiencies

- Early-stage product integration is a major challenge, specifically getting involved at the very beginning of decision-making to support products with "privacy by design" before implementation begins.
- Conducting comprehensive data mapping and compliance inventory processes is difficult due to the challenge of knowing everything that is happening across all departmental areas.
- Compliance teams are bogged down by repetitive, manual, and busy-work tasks, including:
 - Managing simple Data Subject Access Requests (DSARs).
 - Executing manual data deletions.
 - Constantly updating Records of Processing Activities (ROPA).
 - Drafting standard transparency templates, guidance, and policy documents from scratch.
 - First-level AI use-case reviews by department or area.
 - Finding contradictions and inconsistencies across extensive regulatory or corporate documentation is labor-intensive and prone to human oversight.

Current Workarounds

Regulatory Updates and Tracking:

- Organizations use third-party subscription databases, specifically OneTrust's DataGuidance tool, to retrieve materials on legislation and updates.
- Some participants use dedicated compliance monitoring tools — notably the CMS tracker, described as one of the best trackers and widely used by DPOs.
- Teams rely on newsletters, professional networks, webinars, LinkedIn, and dedicated public affairs solutions.
- Some participants conduct direct website research and review laws independently, including re-reading regulations multiple times.
- Some larger organizations maintain dedicated internal teams to conduct manual regulatory research, while others are developing their own internal AI-powered research and compliance monitoring tools.
- One participant specifically referenced the GDPR Enforcement Tracker / Fines Database as a key resource for tracking regulatory sanctions.

Internal Intake Coordination:

- Speaker 1's organization utilizes a single entry-point triage system where requests are routed to specific pillars (DPO, Legal Data, or AI) depending on the core focus of the project, though other pillars are looped in as needed.

What Success Looks Like

- Automated Data Mapping and Monitoring:
 - Establishing automated mapping and inventory tracking to ensure no compliance elements are missed.
 - Implementing automated, customizable, and high-frequency monitoring of legislative updates.

Actionable and Simplified Guidance:

- Translating complex legal jargon into clear, visual, and short action lists that explain exactly why a regulation applies and what remediation actions are required.

Sovereign and Open-Source Infrastructure:

- Utilizing sovereign compliance solutions that guarantee absolute protection of company data, ideally through open-source tools that are vendor-agnostic and seamlessly connect with existing data sources.
- The solution should be open (not tied to a vendor) and capable of connecting with downstream data sources and audit tools.

Strategic Value and TRUST:

- Leveraging compliance certifications (such as ISO or sustainability statements) to build market TRUST, protect reputation, secure internal buy-in, and maintain accountability.
- Participants highlighted accountability, competitive advantage, and market trust as the primary motivators for pursuing compliance certifications.

Product Feedback & Next Steps

General Prioritization and Preference

- High demand for automated legislative updates and risk analysis over other features.
- In a point-allocation exercise participants ranked capabilities as follows:
 - Automated monitoring of changes: ~32 points (highest priority)
 - Risk scoring and alerts: ~26 points
 - Plain-language guidance: ~16 points
 - Document / evidence management: ~16 points
 - Reporting support: ~6 points
- The single feature participants identified as most needed was automated DPIA completion, followed closely by report summary generation.

Regulatory Compliance Assistant (RCA):

- The RCA monitors current and forthcoming EU regulations, informs users about their status, and sends timely notifications and updates on regulatory changes.
- Participants want a flexible, customizable notification system.
- Preferences include a centralized dashboard for tracking, direct email alerts prioritized by topic, and the ability to opt-in to updates for specific selected laws and geographic jurisdictions (such as national-level legislation).
- Technical users requested open integration options, including an RSS feed, to build custom notification flows.

Regulatory Obligations Analyzer (ROA):

- The ROA translates complex EU regulatory requirements into clear, actionable assessment criteria, enabling SMEs to assess their compliance status and prepare for regulatory changes.
- Strong support for translating complex legal texts into clear, visual, and short action lists.
- Key requirements include integrating concrete examples and use cases, as well as providing clear explanations of why specific regulations apply and what actions are needed.

- Infographic or other visual items were suggested to describe and prioritize obligations.

Legal Risk Analyzer (LRA):

- The LRA analyses compliance risks by evaluating data from complaints lodged with supervisory authorities and administrative sanctions, enabling proactive risk management.
- Highly desired features include a comprehensive fines tracker covering all relevant EU data regulations — equivalent to the GDPR Enforcement Tracker but expanded to all EU data regulations.
- Participants requested risk-scoring models directly mapped to specific AI use cases and compliance management system (CMS) tracking.

Regulatory Compliance Evaluator (RCE):

- The RCE enables the systematic assessment and documentation of compliance using the criteria generated by the ROA, providing a comprehensive compliance assessment and gap analysis.
- Clear preference for highly visual presentation of compliance gaps to facilitate easy communication.
- Suggestions include a dashboard displaying compliance percentages and a high-visual color-coded traffic light scoring system that maps directly to remedial actions.

Regulatory Reports Assistant (RRA):

- The RRA streamlines the preparation of EU reports, including DPIAs, TIAs, FRIAs, and sector-specific reports.
- Participants prefer AI to assist rather than replace human judgment.
- The desired workflow is a system that can generate a "one-click" executive summary report with built-in evidence and recommendations.
- It should surface best practice knowledge, highlight inconsistencies, and serve as a reliable backup draft rather than writing final reports autonomously.
- For TIAs, participants requested analysis of multiple external regulations; for FRIAs, a per-country analysis of what each fundamental right means and its legal basis.

Certification Process Assistant (CPA):

- The CPA streamlines certification processes, including those for the European Data Protection Seal under Article 42 of the GDPR, and helps both applicants and auditors obtain compliance certification in accordance with ISO standards.
- Key feature requests include automated gap analyses that display completion rates alongside clear explanations of missing items.

- Participants also requested a "certification readiness score" supported by auto-generated evidence portfolios.
- Participants noted they are prioritizing certifications such as ISO/IEC 42001 and ISO/IEC 27001, with some focusing on sustainability statements.

Objections, Concerns, and Technical Requirements

Data Hosting and Sovereignty

- Mixed requirements regarding geographic data hosting:
 - Some participants strictly require the tool to be 100% hosted in the EU with zero external data transfers.
 - Others, particularly those from multinational setups, are comfortable with multi-geographic setups and data transfers, as long as data transfers are minimized as much as possible.
 - The tool should ideally run LLM-agnostically, allowing organizations to run it using their own self-hosted or preferred language models to maintain data privacy.
- A specific concern was raised about whether the tool can implement automation without transferring data to conventional large language models (LLMs).

Human-in-the-Loop and Accuracy

- Strong consensus that AI must have clearly defined boundaries and capabilities, avoiding pretending to perform tasks it cannot complete.
- To build TRUST, the tool must feature:
- Verifiable evidence and source citation with validation links.
- Accurate timestamps indicating when legislation was last reviewed or updated.
- A clearly visible "human-in-the-loop" review process at all times.
- Acknowledgement that AI-generated information may not always be complete or fully accurate.

International Framework Gap Analysis

- A prominent concern for multinational organizations is the scope limit of the project. While the Trust project focuses on EU regulations, global organizations need tools that can map compliance gaps between EU laws and non-EU frameworks, such as Chinese and African regulations.

Liability and Output Verification

- A critical concern was raised by Speaker 2 and supported by Speaker 1 regarding legal liability.

- Under frameworks like the AI Act, organizations cannot easily deflect liability by simply stating the content is "AI-generated."



TR**ST**