

## D8.2– INTEGRATION PROCESS FOR WIDENING COUNTRY

**Lead Author:** Neslihan ÖZTÜRK  
**With contributions from:** Nuria Barros  
**Reviewer:** Alice Andalo´, Naoufal Elazzouzi

<b>Deliverable nature</b>	<b>Report (R)</b>
<b>Dissemination level</b>	Public (PU)
<b>Delivery date</b>	26-01-2026
<b>Version</b>	2.0
<b>Total number of pages</b>	20
<b>Keywords</b>	TRUMPET, Federated Learning, Healthcare Data Integration, Privacy, GDPR Compliance, Non-EU Countries, Digital Health

## EXECUTIVE SUMMARY

“D8.2– Integration Process For Widening Country” presents the transformation process undertaken to integrate the Ministry of Health of the Republic of Turkey (MoH), an expanding country partner of the TRUMPET platform, into its digital health infrastructure. Building on the regulatory analysis presented in D8.1- Legal Compliance for Non-EU Countries, this delivery translates GDPR compliance findings into concrete technical, organizational, and operational integration actions.

The document initially outlines the regulatory framework that directs the transformation process, providing a summary of the essential comparative findings between GDPR and KVKK that are pertinent to platform integration and pilot execution. It identifies the compliance requirements, regulatory dependencies, constraints and opportunities that directly influence the deployment of privacy-preserving federated learning technologies within a national, non-EU health system.

Based on this regulatory foundation, the deliverable defines the requirements for integrating TRUMPET into the MoH’s infrastructure. These include an overview of the MoH digital health ecosystem, functional requirements and stakeholder needs, prerequisites for data interoperability and semantic alignment, and the infrastructure and security conditions required to enable a safe, on-premise implementation.

The core of the deliverable documents the transformation process itself, covering technical, organisational and human aspects. This involves aligning data sharing and interoperability, implementing security and privacy measures in accordance with D8.1 guidelines, and supporting the integration process through close cooperation between the MoH, pilot hospitals, technical partners, and project stakeholders. The primary deviations that occurred during the integration process are also discussed, along with the associated risk management strategies.

Finally, the deliverable consolidates the lessons learned from the transformation process and provides recommendations for future privacy-enhancing technology installations. Overall, D8.2 demonstrates that the TRUMPET platform can be effectively integrated into a security-first, on-premise national health infrastructure, offering a scalable reference model for widening countries seeking to balance regulatory compliance, data sovereignty and AI-driven health research.

## DOCUMENT INFORMATION

<b>Grant agreement No.</b>	<b>101070038</b>	<b>Acronym</b>	<b>TRUMPET</b>
<b>Full title</b>	<b>TRUstworthy Multi-site Privacy Enhancing Technologies</b>		
<b>Call</b>	HORIZON-CL3-2021-CS-01-04		
<b>Project URL</b>	<a href="https://cordis.europa.eu/project/id/101070038">https://cordis.europa.eu/project/id/101070038</a>		
<b>EU project officer</b>	Ioannis ASKOXYLAKIS		

<b>Deliverable</b>	<b>Number</b>	<b>D8.2</b>	<b>Title</b>	<b>Integration Process for Widening Country</b>
<b>Work package</b>	Number	WP8	Title	TRUMPET Validation for Widening Activity
<b>Task</b>	Number	T8.2	Title	Connection to TRUMPET platform

<b>Date of delivery</b>	<b>Contractual</b>	<b>Mxx</b>	<b>Actual</b>	<b>Mxx</b>
<b>Status</b>	version 1.0	<input checked="" type="checkbox"/> Final version		
<b>Nature</b>	<input checked="" type="checkbox"/> R <input type="checkbox"/> DEM <input type="checkbox"/> DMP <input type="checkbox"/> DEC <input type="checkbox"/> ETHICS <input type="checkbox"/> OTHER			
<b>Dissemination level</b>	<input checked="" type="checkbox"/> Public <input type="checkbox"/> Sensitive			

<b>Authors (partners)</b>	MOH
<b>Responsible author</b>	Neslihan ÖZTÜRK neslihan.ozturk3@saglik.gov.tr

<b>Summary (for dissemination)</b>	This deliverable offer important insights into the execution of data processing and adaptation activities within a technical and operational framework, aligning with the regulatory requirements of Turkish data protection legislation (KVKK) and the EU General Data Protection Regulation (GDPR), during the transformation process of integrating the TRUMPET platform into the Ministry of Health infrastructure, and will also serve as valuable information for future integration systems.
<b>Keywords</b>	<i>TRUMPET, Federated Learning, Healthcare Data Integration, Privacy, GDPR Compliance, Non-EU Countries, Digital Health</i>

VERSION LONG			
Issue Date	Rev. No.	Author	Change
17/12/2025	1.0	Neslihan ÖZTÜRK (MOH)	First Draft
26/01/2026	2.0	Neslihan ÖZTÜRK (MOH)	Final Draft

## TABLE OF CONTENTS

### Contenido

<b>1. Introduction.....</b>	<b>6</b>
1.3 Structure of the Document.....	7
<b>2. Regulatory Baseline for the Transformation Process.....</b>	<b>9</b>
2.1 Summary of GDPR–KVKK Comparative Findings Relevant to Integration .....	9
2.2 Key Compliance Requirements Affecting Technical Transformation.....	9
2.3 Regulatory Dependencies for National Deployment.....	10
<b>3. Requirements for Integrating TRUMPET into Ministry of Health’s Infrastructure .....</b>	<b>12</b>
3.1 Overview of the Ministry of Health’s Digital Health Ecosystem .....	12
3.2 Stakeholder Needs and Functional Requirements .....	12
3.3 Data Interoperability and Semantic Alignment Requirements .....	13
3.4 Infrastructure and Security Prerequisites for Integration.....	13
<b>4. Transformation Process: Technical, Organisational and Human Aspects .....</b>	<b>15</b>
4.1 Interoperability and Data Exchange Alignment .....	15
4.2 Security and Privacy-Preserving Implementations .....	15
4.3 Integration Workflow and Stakeholder Collaboration .....	16
4.4 Main Deviations and Risk Management.....	17
<b>5. Conclusions .....</b>	<b>19</b>
5.1 Lessons Learned from the Transformation Process.....	19
5.2 Recommendations for Future Privacy-Enhancing Technology Deployments .....	20

## ABBREVIATIONS AND ACRONYMS

DPA - Data Protection Authority

EU - European Union

FL- Federated Learning

GDPR - General Data Protection Regulation

KVKK - Kişisel Verilerin Korunması Kanunu (Turkish Data Protection Law)

SCCs- Standard Contractual Clauses

TRUMPET - TRUStworthy Multi-site Privacy Enhancing Technologies

PET - Privacy-Enhancing Technologies

## 1. Introduction

### 1.1 Purpose and Scope of D8.2

The Ministry of Health of the Republic of Türkiye (MoH), as the national authority responsible for the planning, implementation, regulation and supervision of health services in Türkiye, carries out policy formulation, strategy development and implementation processes with a holistic approach in order to protect and improve public health. The MoH undertakes key responsibilities such as ensuring the sustainability of the health system, improving the quality of health services, supporting digital transformation in healthcare, implementing programmes for disease prevention and control, coordinating healthcare facilities, strengthening human resources, and managing international collaborations. In addition, in priority public health areas such as cancer, the MoH establishes effective national control mechanisms by developing screening, early diagnosis, treatment and registry systems, and contributes to the continuous improvement of healthcare services by supporting scientific research, data management and technological innovation.

Through its participation in the TRUMPET Project, the MoH aimed to integrate the TRUMPET platform into the national digital health infrastructure in order to address strategic, scientific and regulatory priorities related to artificial intelligence technologies, data privacy and security, and cancer research. Throughout the project, the MoH carried out the necessary technical, operational and regulatory transformation processes required for the integration of the platform into the national digital health ecosystem.

The platform developed within the scope of the TRUMPET Project enables the collaborative development of artificial intelligence models across institutions holding sensitive health data, without the need for raw data sharing, by leveraging FL methods reinforced with advanced PETs. This approach is strongly aligned with Türkiye's national commitments to data sovereignty and the protection of sensitive health information under the Personal Data Protection Law (KVKK), while also supporting the MoH's participation in international AI-driven research initiatives.

The integration process led by the MoH was structured around Türkiye's role as a Data Owner within the TRUMPET framework. A local TRUMPET learning node established within the MoH infrastructure operates in an on-premise environment in full compliance with GDPR and KVKK requirements that prohibit the transfer of personal data outside Türkiye. This local node enables the privacy-preserving processing of clinical data, their protection through PET methods, and the sharing of only secure model updates within the federated learning environment.

The technical scope of the integration was validated through two clinical use cases implemented at two major radiation oncology centres in Ankara (Use Case 2: Head and Neck Cancer – HNC, and Use Case 3: Stereotactic Body Radiotherapy – SBRT). Within this scope, data obtained from hospital information management systems, clinical reports, epicrisis documents, and outputs from Tomotherapy and LINAC devices were meticulously collected, anonymised, cleaned and transformed into standardised, research-ready datasets. This workflow was conducted in line with the requirements of the TRUMPET Data Owner Node, and all processes were designed in full compliance with KVKK and GDPR principles.

Within the project, the MoH fulfilled all integration-related responsibilities in accordance with the tasks defined under Work Package 8. The completion of legal checks (Task 8.1), adaptation of pilot

requirements (Task 8.2), collection of use case data (Task 8.3), and establishment of connectivity with the TRUMPET platform (Task 8.4) constituted the methodological backbone of the integration process. Türkiye's integration with the TRUMPET platform as a non-EU country necessitated additional regulatory alignment mechanisms, technical modifications and extended testing activities, and this deliverable has been prepared to comprehensively document the resulting transformation process.

## 1.2 Relation to Prior Deliverable D8.1

D8.1- Legal Compliance for Non-EU Countries provided the foundational regulatory analysis required to enable the integration of the TRUMPET platform in Türkiye, with a specific focus on the comparative assessment of the EU GDPR and the KVKK. This prior deliverable identified the key similarities, differences and compliance dependencies related to federated learning workflows, privacy-enhancing technologies, patient data processing, and cross-border data restrictions.

Building directly on the findings of D8.1, Deliverable D8.2:

- Translates the GDPR–KVKK comparative analysis into practical integration requirements for the MoH's infrastructure.
- Ensures that all technical adaptations, anonymisation workflows, PET-enhanced model operations, and TRUMPET Data Owner Node processes remain fully compliant with Turkish legislation and EU-aligned data protection principles.
- Addresses regulatory considerations related to ethical committee approvals, data processing agreements and privacy risk mitigation mechanisms required under Task 8.1 and Task 8.2.
- Demonstrates how federated learning can be implemented within Türkiye in full compliance with KVKK restrictions, ensuring that personal data remain within national borders.

Accordingly, while D8.1 established the legal and regulatory foundation, D8.2 operationalises this framework through concrete implementation pathways, technical validation steps and stakeholder-driven integration mechanisms.

## 1.3 Structure of the Document

This deliverable is structured to provide a comprehensive and sequential overview of the transformation process required to integrate the TRUMPET platform into the MoH digital health ecosystem. The document is organised as follows:

### Section 2 – Regulatory Baseline for the Transformation Process

This section consolidates the core regulatory findings of D8.1 and summarises how GDPR–KVKK similarities and differences shape the technical and organisational integration requirements. It highlights the legal and ethical constraints that must be addressed during the deployment of TRUMPET in Türkiye, including data minimisation, anonymisation, on-site data processing and cross-border data restrictions. The section also identifies regulatory dependencies and opportunities influencing national deployment strategies.

### Section 3 – Requirements for Integrating TRUMPET into Ministry of Health's Infrastructure

This section provides an in-depth overview of the MoH's digital health ecosystem and defines the functional, operational and stakeholder-driven requirements for TRUMPET integration. It covers interoperability needs, semantic alignment of datasets, data flow considerations, infrastructure prerequisites and security-by-design principles necessary to support federated learning activities in a KVKK-compliant environment.

#### Section 4 – Transformation Process: Technical, Organisational and Human Aspects

This section describes the concrete transformation pathways applied to adapt TRUMPET to the MoH's on-premise infrastructure and explains how the identified requirements were implemented in practice. It covers interoperability and data exchange alignment, security and privacy-preserving implementations, and the integration workflow supported by stakeholder collaboration. The section also addresses the tasks executed under Work Package 8, including legal checks (T8.1), pilot requirements (T8.2), data preparation (T8.3) and technical connectivity with TRUMPET (T8.4, as well as the main deviations encountered during the integration process and the corresponding risk management measures applied.

#### Section 5 – Conclusion

The conclusion synthesises the key findings of the transformation process, reflecting on the outcomes of the integration efforts and highlighting the significance of Türkiye's contribution as a widening country implementing a GDPR-aligned federated learning platform. It provides a structured and coherent account of Türkiye's integration journey, articulating both the regulatory rationale and the practical implementation pathway underlying the adaptation of TRUMPET to a non-EU national health system.

## 2. Regulatory Baseline for the Transformation Process

This section establishes the regulatory foundation guiding the integration of the TRUMPET platform into the infrastructure of the MoH. It builds directly on the legal and regulatory analysis presented in Deliverable D8.1, which examined the alignment and divergences between the GDPR and the KVKK. Within the context of the integration activities described in D8.2, this section focuses on the regulatory factors that influence the technical, organisational and operational transformation process.

The purpose of this section is to translate the regulatory findings of D8.1 into actionable integration requirements and to highlight how compliance considerations shape system architecture, data processing workflows, governance mechanisms and stakeholder coordination within a non-EU national health system.

### 2.1 Summary of GDPR–KVKK Comparative Findings Relevant to Integration

The comparative analysis conducted in D8.1 demonstrates that GDPR and KVKK share common foundational principles, including lawfulness, transparency, purpose limitation, data minimisation and security of processing. However, several structural and procedural differences are particularly relevant to the integration of TRUMPET into the infrastructure of the MoH.

The key differences considered throughout the integration process include:

- **Territorial scope:** GDPR has an extraterritorial scope, whereas KVKK is territorially anchored and closely aligned with national data sovereignty principles.
- **Consent requirements:** KVKK requires more explicit, purpose-specific disclosure and clarity in consent mechanisms compared to the broader but stringent consent framework under GDPR.
- **Cross-border data transfers:** While GDPR permits international transfers through safeguards such as Standard Contractual Clauses (SCCs), KVKK prioritises data localisation and requires explicit approval from the Turkish Data Protection Authority for cross-border transfers.
- **Data breach notification:** GDPR mandates notification within 72 hours, whereas KVKK provides greater procedural flexibility depending on guidance from the competent authority.
- **Data protection governance:** GDPR introduces formal roles such as the Data Protection Officer (DPO), while KVKK adopts a different institutional governance model.
- **Sensitivity of health data:** Both frameworks classify health data as sensitive; however, KVKK imposes particularly strict conditions on the processing and retention of health-related personal data.

These differences do not prevent integration; rather, they introduce specific design, governance and operational constraints that must be addressed through appropriate technical and organisational measures.

### 2.2 Key Compliance Requirements Affecting Technical Transformation

The regulatory differences outlined above were directly taken into account throughout the technical transformation process required for the integration of TRUMPET in Türkiye. In particular, KVKK's

strong emphasis on data localisation and strict control over sensitive health data necessitated an on-premise deployment model in which all personal data remain physically within environments under the control of the MoH.

The FL plays a central role in mitigating potential GDPR–KVKK tensions. By design, FL ensures that raw patient data never leave the premises of the Data Owner and that only encrypted or privacy-preserving model updates are exchanged across sites. Within the TRUMPET context, this approach is further strengthened through the application of advanced PETs, including Differential Privacy, Secure Multi-Party Computation and Homomorphic Encryption.

As a result, TRUMPET enables:

- Compliance with KVKK requirements on data localisation and purpose limitation.
- Alignment with GDPR-level privacy expectations without cross-border data transfer.
- Reduction of re-identification and inference risks associated with federated model updates.

These compliance-driven requirements shaped the selection of system architecture, security mechanisms, validation procedures and access control policies implemented by the MoH throughout the integration process.

### 2.3 Regulatory Dependencies for National Deployment

Beyond core data protection principles, the national deployment of TRUMPET in Türkiye is subject to additional regulatory and procedural dependencies. The preparatory steps undertaken prior to initiating retrospective clinical studies within the integration process included the following:

- Ethical committee approvals at the Ministry level were obtained for the retrospective oncology datasets used within the pilot studies.
- Legal checks were completed under Task 8.1 in alignment with D5.1 (Legal and Ethics Compliance Report) and D5.3 (Data Management Plan), and the necessary data processing agreements and confidentiality undertakings were executed.
- Formal assignment letters were issued for each clinical team member, and signed activity reports related to data processing activities within the scope of the clinical studies were systematically tracked.
- Institutional governance alignment was maintained throughout the project to ensure that data processing responsibilities, access rights and accountability structures were clearly defined within the MoH and the partner hospitals.

These dependencies required close coordination among technical teams, legal units, ethics committees and clinical stakeholders. Addressing them at an early stage of the integration process proved critical for enabling the activation of Tasks 8.2 and 8.3, particularly with respect to pilot data access and the execution of the defined use cases.

### 2.4 Constraints and Opportunities Identified in D8.1

D8.1 identified both constraints and opportunities that informed the transformation strategy adopted throughout Work Package 8. On the constraint side, KVKK's approach to data localisation, consent specificity and regulatory oversight limits the applicability of certain GDPR-based data transfer

mechanisms. These constraints required the MoH to adopt a cautious, compliance-first integration strategy.

At the same time, the deliverable highlighted significant opportunities. FL, combined with PETs-reinforced safeguards, emerged as a natural compliance bridge between GDPR and KVKK. Within this context, the TRUMPET integration process fulfilled the following roles:

- Acting as an active compliance-enabling platform that embeds regulatory requirements directly into its technical design and governance model.
- Serving as a reference implementation demonstrating how privacy-preserving AI infrastructures can be deployed across national contexts without compromising domestic legal frameworks.

By operationalising the regulatory insights of D8.1, the integration carried out by the MoH has positioned Türkiye as a reference model for GDPR-aligned federated learning deployments in non-EU settings, while offering valuable lessons for future national and cross-border health data initiatives.

### 3. Requirements for Integrating TRUMPET into Ministry of Health's Infrastructure

This section defines the technical, functional and infrastructural requirements that enabled the integration of the TRUMPET platform into the digital health infrastructure of the MoH in Türkiye. The requirements described herein reflect the characteristics of a non-EU, security-first national health system and are directly shaped by the operational constraints, regulatory considerations and pilot implementation needs identified during the integration process.

#### 3.1 Overview of the Ministry of Health's Digital Health Ecosystem

The MoH's digital health ecosystem is designed around a secure, on-premise infrastructure model aligned with KVKK requirements for data localisation and the protection of sensitive health data. Accordingly, the TRUMPET integration was carried out within a controlled environment that prioritises security, isolation and operational resilience.

Key characteristics of the MoH's ecosystem relevant to the TRUMPET integration include:

- **On-premise server infrastructure**, ensuring that all personal and sensitive health data remain physically within environments under the control of the MoH.
- **Container-based deployment using Docker**, enabling modular installation, service isolation and controlled lifecycle management of platform components.
- **Service exposure behind a load balancer**, supporting scalability, controlled access and resilience while preventing direct exposure of internal services.
- **Enforcement of TLS 1.2 / TLS 1.3 and HTTPS-only communication**, ensuring encrypted data transmission at all stages of interaction.
- **IP whitelisting and bidirectional network permissions**, allowing only explicitly authorised endpoints to communicate with the MoH environment.

This ecosystem provided a stable and secure foundation for deploying the TRUMPET's Data Owner Node and for supporting federated learning workflows without compromising national data sovereignty principles.

#### 3.2 Stakeholder Needs and Functional Requirements

The integration process involved multiple stakeholders, each with distinct functional and operational requirements that needed to be addressed in a coordinated manner.

The main stakeholders included:

- **MoH's IT and DevOps teams**, responsible for infrastructure provisioning, deployment, configuration management and operational continuity.
- **Network and cybersecurity teams**, responsible for secure connectivity, access control, traffic monitoring and compliance with national security policies.
- **Radiation Oncology clinics**, acting as data providers and clinical validation environments for the Head and Neck Cancer and SBRT use cases.
- **TRUMPET technical partners**, responsible for platform-side configuration, federated learning orchestration and compatibility with the MoH deployment.

- **IRST and CHU**, acting as project pilot partners responsible for clinical studies, with whom communication was maintained during the alignment of technical and operational requirements.

Across these stakeholders, the functional requirements were framed to ensure:

- **Secure connectivity** between the MoH's infrastructure, the TRUMPET platform and the hospital partners.
- **Controlled data ingestion**, guaranteeing that only authorised, anonymised and research-ready datasets are processed within the Data Owner Node.
- **Auditability and monitoring**, enabling traceability of system actions, access events and operational status.
- **Operational continuity during platform updates**, allowing integration activities to continue despite iterative changes on the TRUMPET platform side.

These requirements shaped both the architectural decisions and the operational workflows adopted during the integration process.

### 3.3 Data Interoperability and Semantic Alignment Requirements

Interoperability and semantic alignment were critical requirements for enabling effective federated learning across heterogeneous clinical data sources. To address this, the integration adopted HL7 FHIR-compliant data structures as a common representation framework.

The key interoperability requirements included:

- Use of FHIR-compliant resource structures to standardise the representation of clinical data.
- Explicit utilisation of FHIR Questionnaire and QuestionnaireResponse resources to support structured data capture and ensure variable consistency across datasets.
- Semantic alignment using standard terminologies, including ICD-10 for diagnoses and, where applicable, LOINC and SNOMED CT for clinical variables.
- Normalisation of complex oncology-specific data, including Dose–Volume Histogram (DVH) parameters and radiotherapy-related metrics, to ensure compatibility with federated model training processes.

These alignment activities enabled datasets originating from different hospital systems and devices to be processed uniformly within the TRUMPET Data Owner Node. This section also provides a conceptual bridge to Section 4.1, where interoperability and data exchange alignment are addressed as part of the transformation process.

### 3.4 Infrastructure and Security Prerequisites for Integration

To support the requirements outlined above, a set of explicit infrastructure and security prerequisites were defined and implemented prior to and during the integration process:

- Allocation of a dedicated virtual server within the MoH's on-premise environment for the deployment of TRUMPET.

- Docker-based isolated deployment, separating TRUMPET components from other MoH's services and reducing attack surfaces.
- A Load Balancer with SSL offloading, supporting secure access and traffic management.
- Bidirectional IP whitelisting, ensuring that only approved external and internal endpoints can establish connections.
- OAuth or token-based API access mechanisms, enabling controlled and auditable interaction with platform services.
- Logging, retry and error-handling mechanisms, supporting operational stability, troubleshooting and resilience during integration and pilot execution.

Together, these prerequisites established a secure and robust operational environment capable of supporting privacy-preserving federated learning workflows in alignment with both national and EU-aligned regulatory expectations.

## 4. Transformation Process: Technical, Organisational and Human Aspects

The transformation process undertaken to integrate the TRUMPET platform into the MoH's infrastructure was implemented based on the requirements defined in Section 3, addressing technical interoperability, security and privacy-preserving implementations, as well as organisational coordination and stakeholder collaboration. Given Türkiye's status as a non-EU country operating a security-first, on-premise health data environment, the transformation required tailored architectural adaptations and close coordination among multiple technical and institutional actors.

### 4.1 Interoperability and Data Exchange Alignment

The interoperability transformation focused on enabling seamless and secure data exchange between the MoH's on-premise systems and the TRUMPET platform, while maintaining strict control over data access and localisation. Clinical datasets originating from hospital information systems, radiotherapy devices and departmental clinical records were transformed into standardised, research-ready formats compatible with the TRUMPET Data Owner Node.

This process included:

- Alignment of heterogeneous clinical data structures to HL7 FHIR-compliant representations, ensuring consistency across data sources.
- Use of FHIR Questionnaire and QuestionnaireResponse resources to support structured variable definitions and consistent data capture.
- Semantic normalisation using ICD-10 and other relevant medical terminologies, enabling meaningful aggregation and analysis across multiple centres.
- Normalisation of complex oncology-specific data, including Dose–Volume Histogram (DVH) metrics and radiotherapy parameters, to support federated learning workflows.

From an infrastructure perspective, interoperability was achieved through controlled, IP-based communication channels. Secure, bidirectional network configurations enabled MoH's systems to communicate with the TRUMPET platform while preventing unauthorised data flows. Data ingestion and validation processes were designed to support iterative testing, ensuring that data quality, consistency and model compatibility were preserved throughout the pilot phase.

### 4.2 Security and Privacy-Preserving Implementations

Security and privacy-preserving implementations constituted a core pillar of the TRUMPET integration process within the MoH's infrastructure. All technical and organisational measures adopted during integration were explicitly aligned with the regulatory principles, risk assessments and mitigation strategies defined in D8.1, ensuring that the operational deployment remained compliant with both KVKK and GDPR-aligned expectations.

In line with the findings of D8.1, particular emphasis was placed on data localisation, purpose limitation, access control and the minimisation of privacy risks associated with federated learning model updates. As required by KVKK, all personal and sensitive health data remained within on-premise environments under the control of the MoH throughout the integration and pilot execution

phases. No raw clinical data were transferred beyond national borders, and no cross-border exchange of identifiable information took place.

The TRUMPET's Data Owner Node was deployed on a dedicated virtual server within the MoH's infrastructure and isolated through Docker-based containerisation, reducing attack surfaces and limiting the potential impact of security incidents. Network-level security controls—including bidirectional IP whitelisting, restricted port access and segmented network zones—were implemented to ensure that only explicitly authorised endpoints could communicate with platform components. All communications were encrypted using TLS 1.2 / TLS 1.3, with HTTPS enforced across all interfaces, in accordance with the security-by-design recommendations highlighted in D8.1.

From an application and access control perspective, token-based authentication mechanisms were employed to regulate interactions with TRUMPET platform services. In line with D8.1's emphasis on accountability and transparency in data processing operations, comprehensive logging, monitoring and audit mechanisms were activated to support traceability, incident detection and post-event analysis.

At the data processing level, privacy protection was further strengthened through the use of privacy-preserving federated learning workflows, which ensured that only encrypted or privacy-protected model updates were exchanged during training and analysis. The application of PETs, including Differential Privacy, Secure Multi-Party Computation and Homomorphic Encryption, directly addressed the residual privacy risks of federated learning identified in D8.1, such as inference and re-identification attacks on model updates.

In addition, operational procedures were established to ensure that ethical committee approvals, data processing agreements and, where applicable for retrospective studies, consent-related requirements were respected throughout the lifecycle of the pilots. These procedures ensured that security and privacy considerations were treated not as one-off technical controls, but as continuous governance elements embedded within the integration workflow.

### 4.3 Integration Workflow and Stakeholder Collaboration

The integration workflow was executed through close collaboration among technical, clinical and organisational stakeholders. The MoH coordinated the transformation activities across WP8 tasks, ensuring alignment between legal compliance (Task 8.1), pilot preparation (Task 8.2), data readiness (Task 8.3) and platform connectivity (Task 8.4).

Key contributions included:

- MoH's IT, DevOps and network teams, responsible for infrastructure provisioning, deployment, network configuration and operational monitoring.
- Pilot hospitals and Radiation Oncology departments, providing clinical expertise, validating datasets and supporting use case execution for HNC and SBRT.
- TRUMPET technical partners, ensuring compatibility between the MoH deployment and the platform's federated learning orchestration layer.
- Project pilot partners (IRST and CHU), contributing to harmonisation and alignment efforts based on pilot experiences.

Throughout the integration process, structured communication and coordination mechanisms were maintained. Technical alignment discussions, validation cycles and update synchronisation ensured that integration activities progressed in parallel with WP4 pilot execution, despite ongoing platform updates and iterative testing requirements.

This collaborative workflow enabled Türkiye to successfully implement TRUMPET as a widening country partner, demonstrating that complex privacy-preserving AI platforms can be integrated into national health infrastructures through coordinated technical adaptation and sustained stakeholder engagement.

#### 4.4 Main Deviations and Risk Management

Despite careful planning and alignment with regulatory and technical requirements, several deviations from the initially envisaged integration timeline and workflow were encountered during the transformation process. These deviations primarily stemmed from the complexity of integrating a cloud-based federated learning platform into a security-first, on-premise national health infrastructure.

##### *Main Deviations*

One of the primary deviations related to data preparation and formatting. Clinical datasets originating from hospital systems required additional transformation to meet the specific schema and structural requirements of the TRUMPET platform. This formatting and standardisation process, including quality control and validation steps, took longer than initially anticipated.

A second deviation arose from the hybrid nature of the integration architecture. While the MoH operates fully on-premise systems, the TRUMPET platform includes cloud-based coordination and federated model management components. Establishing secure, bidirectional communication between these environments required additional network configuration, testing and validation cycles, extending the integration timeline.

A third deviation was associated with extended validation and interoperability testing. Multiple test iterations were necessary to ensure that data exchange, security controls and federated learning workflows operated reliably under real-world conditions.

Finally, ongoing updates and enhancements to the TRUMPET platform during the integration period necessitated repeated technical adjustments on the MoH side. Each platform update required compatibility checks and, in some cases, configuration changes to maintain stable operation.

##### *Risk Identification and Mitigation Measures*

In response to these deviations, a structured risk management approach was adopted:

- Risk: Data incompatibility or delayed readiness
- Mitigation: A structured preprocessing and validation pipeline was established, enabling incremental data ingestion and reducing dependency on full dataset readiness.

- Risk: Network connectivity or security configuration issues
- Mitigation: Dedicated IP whitelisting, staged connectivity testing and close coordination between MoH's network teams and TRUMPET technical partners were implemented.
- Risk: Platform updates disrupting integration stability
- Mitigation: Version tracking, controlled update windows and rollback procedures were introduced to minimise operational disruption.
- Risk: Human resource constraints due to repeated technical adjustments
- Mitigation: Knowledge transfer sessions, shared technical documentation and closer DevOps collaboration reduced dependency on individual team members.

Overall, while these deviations led to extensions in the integration timeline, they significantly strengthened the robustness, adaptability and scalability of the final integration model. The risk management measures implemented throughout the process provide valuable guidance for future deployments of privacy-preserving federated learning platforms in Türkiye and other widening countries.

## 5. Conclusions

The integration of the TRUMPET platform into the MoH infrastructure demonstrates that privacy-preserving federated learning technologies can be successfully implemented within a non-EU, security-first national health system. Building upon the regulatory foundations established in D8.1, this deliverable has documented the technical, organisational and human transformation processes required to operationalise TRUMPET in compliance with the KVKK, while maintaining alignment with GDPR-level privacy expectations.

Through the execution of the WP8 tasks, Türkiye has validated a scalable integration model that enables advanced AI-driven research on sensitive health data without compromising data sovereignty, ethical standards or regulatory compliance. The experience gained throughout this process provides valuable insights for both national-level deployments and future cross-country implementations.

### 5.1 Lessons Learned from the Transformation Process

Several key lessons emerged from the integration and pilot implementation phases.

First, regulatory compliance must be embedded from the earliest stages of system design. The analyses conducted under D8.1 proved critical in shaping architectural decisions, data processing workflows and governance mechanisms, and in mitigating compliance risks during implementation.

Second, federated learning combined with advanced PETs effectively mitigates many of the inherent tensions between GDPR and KVKK, particularly with respect to data localisation and cross-border data transfer restrictions. Nevertheless, residual privacy risks, such as inference attacks on model updates, require continuous monitoring, validation and technical safeguards.

Third, the integration highlighted the importance of robust interoperability and data standardisation practices. Preparing heterogeneous clinical datasets for federated learning required substantial effort in data cleaning, semantic alignment and validation. These activities should be planned as core components of any similar deployment.

Fourth, hybrid architectures involving local national systems and externally coordinated platforms introduce additional complexity, particularly in terms of network configuration, validation cycles and update management. Close collaboration between DevOps, network and cybersecurity teams is therefore essential.

Finally, the process demonstrated that human and organisational readiness is as critical as technical capability. Continuous knowledge transfer, clear role definitions and cross-disciplinary collaboration were vital to sustaining integration activities in the face of platform updates and evolving requirements.

## 5.2 Recommendations for Future Privacy-Enhancing Technology Deployments

The integration experience within the TRUMPET Project has informed several recommendations for future deployments of privacy-enhancing AI platforms in Türkiye and other widening countries.

First, future deployments should further embrace on-premise or hybrid federated architectures that respect national data sovereignty while enabling participation in international research ecosystems. Federated learning platforms should natively support PETs and provide transparent privacy-risk measurement mechanisms.

Second, data interoperability and semantic alignment should be addressed systematically, including the adoption of standard terminologies, structured data models and validation processes tailored to the target use cases.

Third, operational planning must explicitly account for platform evolution and update cycles, incorporating version management, rollback strategies and controlled update windows to preserve system stability.

Finally, future initiatives should invest in capacity building and governance frameworks, ensuring that technical teams, clinical stakeholders and regulatory bodies are jointly engaged throughout the deployment lifecycle.

In conclusion, the TRUMPET integration experience positions Türkiye as a reference model for the responsible adoption of privacy-preserving federated learning technologies within national health systems and provides a practical pathway for countries seeking to balance innovation, collaboration and data protection.