

PURPOSE LIMITATION · DATA MINIMISATION · ACCOUNTABILITY

Governed by purpose. Enabled by technology.

Principles for responsible data processing in government and mission-critical software.

DOCUMENT ID	VERSION	CLASSIFICATION	DOCUMENT OWNER	REVIEW CYCLE	PUBLISHED
ITO-TRUST-PRV-001	1.0	PUBLIC	Privacy & Information Annual Security		October 2026

Responsible data governance by design

ITO develops digital platforms used by government institutions, public safety organisations and other organisations operating complex and mission-critical processes.

These systems may process personal, operational or otherwise sensitive information. Responsible data governance must therefore be considered throughout system design, implementation, operation and maintenance.

This document describes the principles used by ITO when designing technology that processes or provides access to institutional data.

ITO APPROACHES PRIVACY AND DATA GOVERNANCE THROUGH SIX PRINCIPLES

01

Purpose limitation
Processing for defined and legitimate purposes.

02

Data minimisation
No unnecessary collection or duplication.

03

Controlled access
Access for authorised users and systems only.

04

Accountability
Relevant activities recorded where required.

05

Security
Protection throughout the information lifecycle.

06

Transparency
Clear roles and documented governance.



This document does not replace the legal, regulatory or governance responsibilities of the institution operating the system.

CONTENTS

01	Purpose	02
02	Institution-controlled governance	03
03	Privacy by design	04
04	Minimisation & authoritative sources	05
05	Access & accountability	06
06	Data lifecycle	06
07	Data sharing & integrations	07
08	Privacy roles & responsibilities	08
09	Privacy & security	09
10	Standards & regulatory context	09
11	Privacy assurance	10
12	Our principle	10

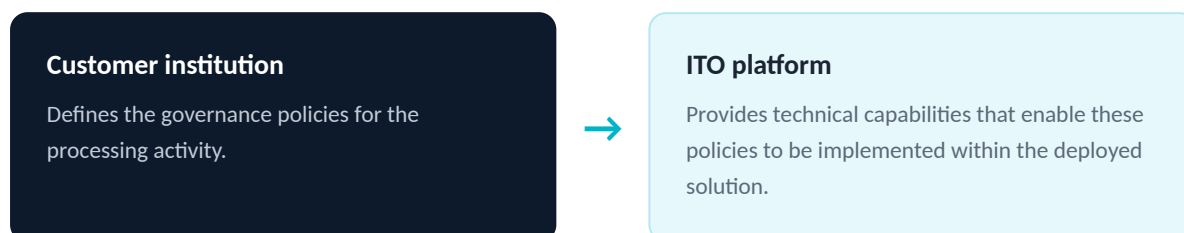
DOCUMENT CONTROL

DOCUMENT ID	ITO-TRUST-PRV-001
VERSION	1.0
CLASSIFICATION	PUBLIC
OWNER	Privacy & Information Security
REVIEW CYCLE	Annual
PUBLISHED	October 2026

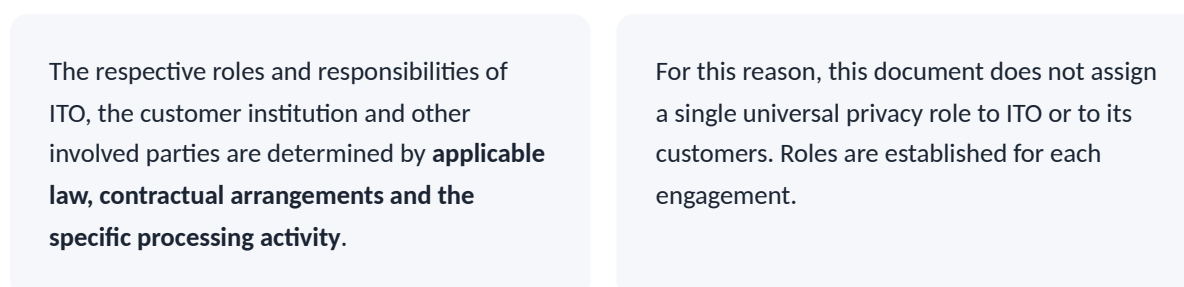
Technology enables governance. Institutions define it.

ITO platforms are designed to operate within governance frameworks defined by the organisations using them.

DEPENDING ON THE APPLICABLE LEGAL AND CONTRACTUAL MODEL, THE CUSTOMER INSTITUTION DETERMINES MATTERS SUCH AS



ROLES AND RESPONSIBILITIES



Privacy begins at the design stage

Privacy considerations should begin during system design rather than being introduced only after deployment.

Depending on the nature of the solution, relevant design considerations may include:

Purpose limitation

01

Information should be processed for defined and legitimate operational purposes.

Data minimisation

02

Systems should avoid unnecessary collection or duplication of information.

Access limitation

03

Information should be accessible only to appropriately authorised users and systems.

Traceability

04

Relevant activities should be recorded where required to support accountability.

Retention

05

Information should not be retained longer than required by applicable rules and operational requirements.

Security

06

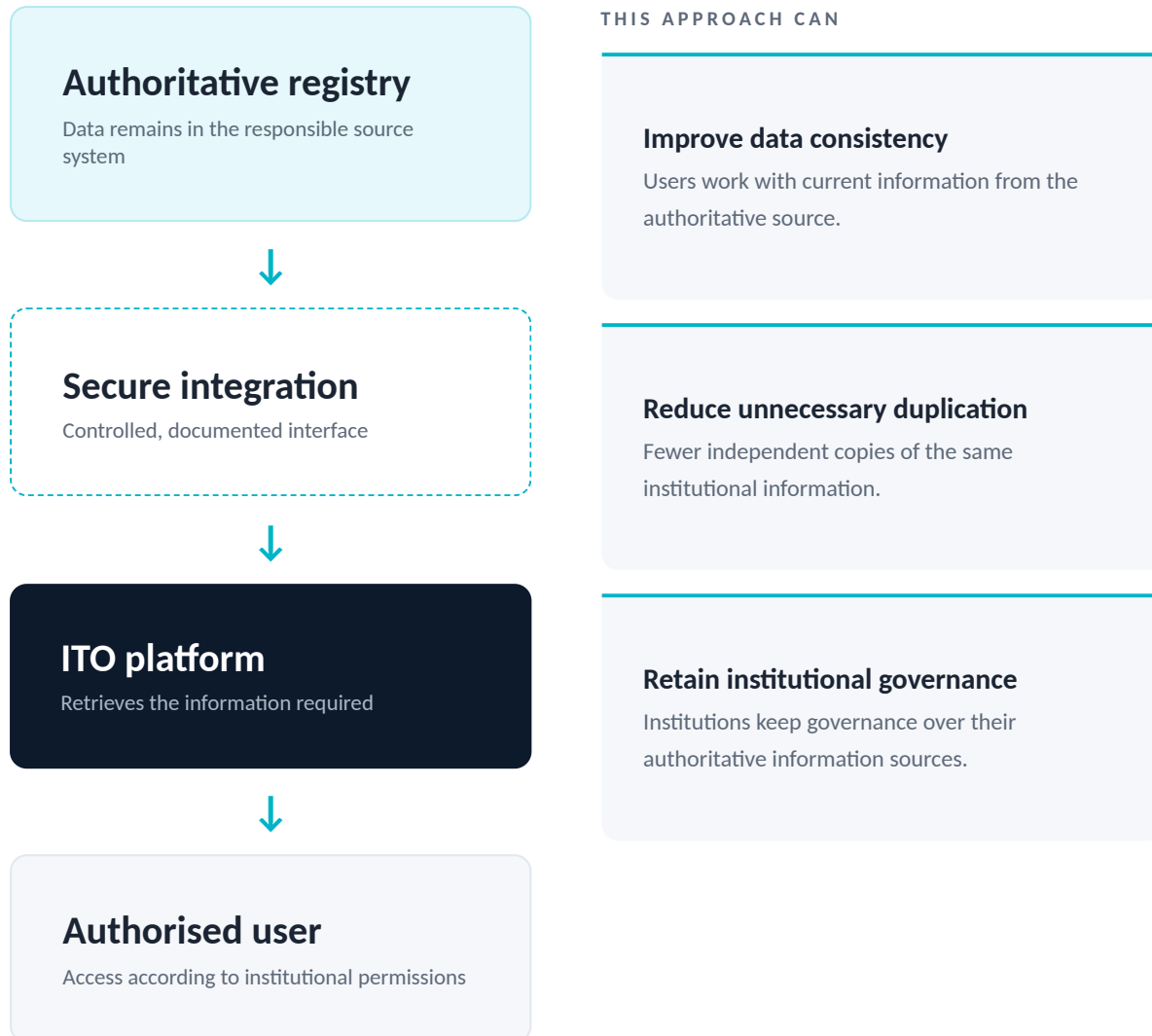
Appropriate technical and organisational measures should protect information throughout its lifecycle.

These considerations are applied in proportion to the nature of each solution, the information it processes and the governance framework defined by the institution.

Integrate without duplicating

One of ITO's core architectural principles is to avoid unnecessary duplication of institutional information.

Where technically and operationally appropriate, ITO platforms can integrate with authoritative information sources rather than creating additional independent copies of the same information.



Access reflects responsibility

Access to information should reflect organisational responsibility and operational need.

DEPENDING ON THE SOLUTION, ITO PLATFORMS MAY SUPPORT

Authenticated identities

Role-based access control

Organisational hierarchy

Restricted administrative functions

Audit logging

Where supported by the solution, audit information can provide authorised personnel with visibility into relevant system and user activities.

THE INSTITUTION DECIDES

The institution determines who should have access to specific information and functionality according to its applicable governance model.

Governance across the information lifecycle

Data governance extends throughout the lifecycle of information.



ITO PLATFORMS

May provide technical mechanisms supporting lifecycle policies.

LAW, INSTITUTIONAL PROCEDURES AND CONTRACTS

Determine the applicable retention, archival and deletion requirements.

Controlled exchange between systems

Information exchange between systems should occur through controlled and documented integration mechanisms.

DEPENDING ON THE ARCHITECTURE, INTEGRATIONS MAY INCLUDE



Access to external information sources remains subject to the authority, policies and technical controls of the responsible organisations.

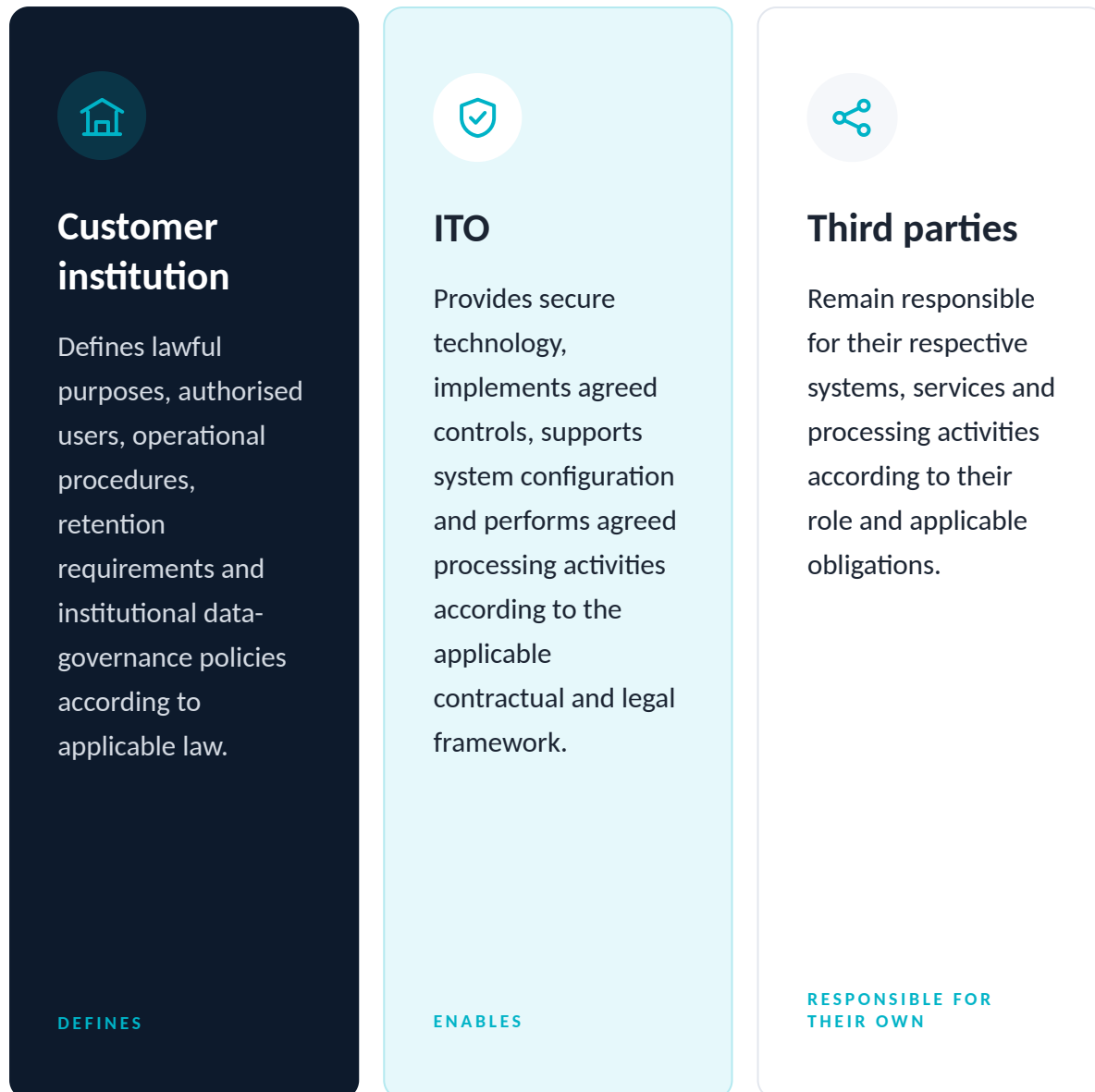
OUR POSITION

Integration does not create authority to access data.

Authority must exist **independently** of the technology enabling the integration.

Clear roles for every party

Each party is responsible for its own part of the processing, according to applicable law and contractual arrangements.



The precise allocation of roles is determined by applicable law, contractual arrangements and the specific processing activity.

Privacy cannot exist without security

ITO's privacy approach is therefore supported by security principles including:



For additional information

ITO Security Whitepaper

ITO-TRUST-SEC-001 · ito.dev/en/trust-center

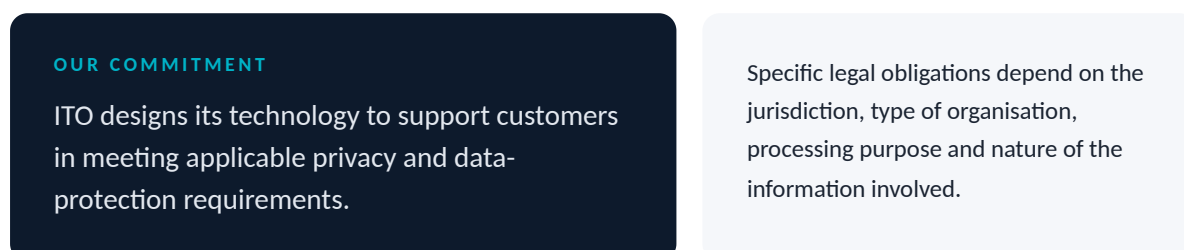
[Related document →](#)

Designed to support applicable requirements

ITO designs its privacy-management approach with reference to applicable data-protection requirements and recognised privacy-management principles.



ITO's management systems are supported by ISO/IEC 27701 and ISO/IEC 27001 certifications within their certified scope.



Information for due diligence

Customers and partners requiring additional information may request appropriate privacy and data-governance documentation as part of procurement, implementation or supplier-assurance activities.

DEPENDING ON THE ENGAGEMENT, THIS MAY INCLUDE INFORMATION CONCERNING

01 Data flows	02 Processing architecture	03 Security controls	04 Access management
05 Retention capabilities	06 Integrations	07 Relevant certifications	08 Contractual data-protection arrangements

Sensitive information may be provided subject to appropriate confidentiality requirements.

REQUEST DOCUMENTATION

Contact ITO through the Trust Center or the designated security channel.

security@ito.dev
ito.dev/en/trust-center

Data should be processed because there is a **legitimate institutional purpose** — not simply because technology makes processing possible.

ITO designs technology to enable institutions to use data effectively while maintaining appropriate governance, security, accountability and control.



ITO TRUST DOCUMENTS

Engineering Digital Trust.

RELATED DOCUMENTS

ITO-TRUST-SEC-001

ITO Security Whitepaper

TRUST DOCUMENT

ITO Responsible AI Principles

TRUST DOCUMENT

ITO Secure Development Overview

DOCUMENT

ITO Privacy & Data Governance

ID · VERSION · CLASSIFICATION

ITO-TRUST-PRV-001 · 1.0 · PUBLIC

OWNER · REVIEW

Privacy & Information Security · Annual · October 2026

CONTACT

security@ito.dev · ito.dev/en/trust-center

COMPANY

IT Odjel Mostar d.o.o., Mostar, Bosnia and Herzegovina