GDPR, ISO/IEC 27001:2022, and ISO/IEC 27701:2019 Comparison

Aspect	GDPR	ISO/IEC 27001:2022	ISO/IEC 27701:2019
Primary Focus	Protecting the personal data of EU citizens and ensuring privacy rights.	Establishing an Information Security Management System (ISMS) to protect all types of information assets.	Extending ISO 27001 to include Privacy Information Management System (PIMS) for managing personal data.
Purpose	Compliance with legal and regulatory requirements for data protection and privacy.	Mitigating information security risks and protecting the confidentiality, integrity, and availability of information.	Ensuring compliance with privacy laws (e.g., GDPR) by implementing privacy-focused controls.
Scope	Organizations processing personal data of EU citizens, regardless of location.	Broad scope for all organizational information assets, not limited to personal data.	Specific to managing Personally Identifiable Information (PII), building on ISO 27001.
Applicability	All organizations that collect, process, or store personal data of EU citizens.	Any organization managing sensitive information, regardless of industry or location.	Organizations acting as PII controllers or processors, particularly those needing compliance with GDPR or other privacy laws.
Legal Requirement	Mandatory for compliance in the EU and for businesses interacting with EU citizens.	Voluntary, but often required by industry standards, clients, or stakeholders.	Voluntary, but supports compliance with privacy regulations like GDPR.
Key Principles	Lawfulness, fairness, transparency, data minimization, purpose limitation, accountability, security, and privacy by design/default.	Risk-based approach to managing information security, including identifying and mitigating risks to information assets.	Adds privacy-specific principles like PII processing, lawful basis for processing, consent, and data subject rights.
Certification	No official GDPR certification exists but compliance can be demonstrated through certifications like ISO 27701.	ISO 27001 certification verifies an organization's ISMS.	ISO 27701 certification extends ISO 27001 to include privacy and data protection, supporting GDPR compliance.

Compliance Requirements	Mandatory compliance with GDPR articles and principles, enforced by penalties and fines.	Compliance with ISO 27001 is voluntary but demonstrates a commitment to securing information assets.	Compliance with ISO 27701 is voluntary but demonstrates alignment with GDPR and similar privacy laws.
Alignment with GDPR	The regulation itself.	Provides a framework for securing personal data, but not specifically aligned with GDPR.	Explicitly designed to address GDPR requirements and extend ISO 27001 with privacy-specific controls.
Control Categories	No formal control categories but focuses on accountability, data subject rights, and technical/organizational measures.	93 controls grouped under 4 themes: organizational, people, physical, and technological.	Extends ISO 27001 with privacy-specific controls like consent, data subject rights, and PII processing activities.
Auditability	Organizations can be audited to demonstrate GDPR compliance but no formal certification exists.	Certification involves audits of the ISMS against ISO 27001 requirements.	Certification involves auditing privacy controls as part of the ISMS, ensuring PII management and GDPR compliance.
Examples of Requirements/Controls	Data subject rights, breach notification, consent, DPIAs, privacy by design/default, record of processing activities.	Access control, encryption, incident response, risk assessment, secure software development, and business continuity.	Privacy-specific controls, including consent management, lawful basis for processing, PII processing agreements, and privacy impact assessments.
Implementation Framework	GDPR compliance requires implementing policies, technical/organizational measures, and training staff.	ISO 27001 requires a risk management approach with documented policies, objectives, and continual improvement.	ISO 27701 integrates with ISO 27001, focusing on PII controllers/processors and privacy risks.
Penalties for Non-Compliance	Fines of up to €20 million or 4% of annual global turnover, whichever is higher.	No penalties, but failure to implement ISO 27001 could result in security incidents and reputational damage.	No penalties, but certification improves privacy compliance and reduces the risk of GDPR fines.

List of Documents Required for ISO 27701 (Extension ISO 27001)

Category	ISO/IEC 27701 Clause	Policy	Procedure	Formats/Records
PII Processing	7.2.1, 8.2.1	PII Processing Policy	PII Processing Procedure	- **PII Inventory**: List of all PII processed, including its purpose. - **Data Flow Maps**: Visual representation of PII flows.
Risk Management	6.2.1	Privacy Risk Management Policy	Privacy Risk Assessment Procedure	- **Risk Assessment Report**: Summary of identified privacy risks. - **Privacy Risk Register**: Ongoing log of risks and mitigation.
Impact Assessments	7.4.1, 8.4.1	Privacy by Design and Default Policy	Privacy Impact Assessment (PIA/DPIA)	- **PIA Templates**: Standardized forms for conducting assessments. - **Completed PIA Reports**: Detailed reports of privacy impacts.
Data Subject Rights	7.3.1, 8.3.1	Data Subject Rights Management Policy	Data Subject Rights Procedure	- **Request Log**: Tracks all data subject requests. - **Handling Templates**: Predefined templates for request responses.
Consent Management	7.3.1	Consent Management Policy	Consent Management Procedure	- **Consent Forms**: Documentation of individual consent. - **Consent Logs**: Records of granted and withdrawn consent.
Third-Party Management	7.2.6, 8.2.6	Third-Party Management Policy	Third-Party PII Processor Management	- **Vendor Agreements**: Contracts with privacy clauses. - **Assessment Forms**: Vendor evaluation forms.
Privacy by Design	7.4.1	Privacy by Design and Default Policy	Privacy by Design and Default Procedure	- **Development Checklists**: Privacy-focused system design checklist. - **Assessment Reports**: Reports confirming compliance.

Incident Management	7.5.1, 8.5.1	Incident Response and Breach Notification Policy	Incident Response Procedure	- **Incident Reporting Templates**: Forms for documenting incidents. - **Incident Logs**: Records of breach details and resolutions.
Retention and Disposal	7.2.4, 8.2.4	Retention and Disposal Policy	Retention and Disposal of PII Procedure	- **Retention Schedules**: Timeframes for retaining PII. - **Disposal Records**: Logs of securely deleted PII.
Cross-Border Transfers	7.6.1, 8.6.1	Cross-Border Data Transfer Policy	Cross-Border Data Transfer Procedure	- **Transfer Agreements**: Legal agreements for PII transfers. - **Data Flow Logs**: Records of cross-border data flows.
Training	6.3.1	Training and Awareness Policy	Privacy Training Procedure	- **Training Records**: Attendance and completion logs. - **Training Materials**: Privacy-specific content for employees.
Audits	6.5.1	Monitoring and Audit Policy	Privacy Auditing Procedure	- **Audit Checklists**: Privacy-focused audit criteria. - **Audit Reports**: Findings from internal or external audits.
Monitoring and Reporting	6.4.1	Reporting and Communication Policy	Reporting and Communication Procedure	- **Compliance Reports**: Periodic reports on privacy compliance. - **Communication Plans**: Strategy for privacy-related communications.
PII Handling	7.2.1, 8.2.1	Data Classification and Handling Policy	Data Classification and Handling Procedure	- **Classification Records**: Categories of PII handled. - **Access Logs**: Records of who accessed PII and when.