#001 ? Compliance Summary ? AI Compliance System vs gdpr-info.eu ? November 09, 2025

This Compliance Summary (the "Agreement") is entered into as of November 09, 2025 between AI Compliance System and gdpr-info.eu. The Parties agree as follows:

1. Scope of Services:

General Data Protection Regulation (GDPR) ? Legal Text
Search for: General Data Protection Regulation (GDPR) Final text of the GDPR including recitals. Menu and widgets DSGVO GDPR Recitals Key Issues AI Act Data Act Skip to content Search for: GDPR Recitals Key Issues AI Act Data Act GDPR Chapter 1 (Art. 1 ? 4)General provisions Art. 1Subject-matter and objectives Art. 2Material scope Art. 3Territorial scope Art. 4Definitions Chapter 2 (Art. 5 ? 11)Principles Art. 5Principles relating to processing of personal data Art. 6Lawfulness of processing Art. 7Conditions for consent Art. 8Conditions applicable to child?s consent in relation to information society services Art. 9Processing of special categories of personal data Art. 10Processing of personal data relating to criminal convictions and offences Art. 11Processing which does not require identification Chapter 3 (Art. 12 ? 23)Rights of the data subject Art. 12Transparent information, communication and modalities for the exercise of the rights of the data subject Art. 13Information to be provided where personal data are collected from the data subject Art. 14Information to be provided where personal data have not been obtained from the data subject Art. 15Right of access by the data subject Art. 16Right to rectification Art. 17Right to erasure (?right to be forgotten?) Art. 18Right to restriction of processing Art. 19Notification obligation regarding rectification or erasure of personal data or restriction of processing Art. 20Right to data portability Art. 21Right to object Art. 22Automated individual decision-making, including profiling Art. 23Restrictions Chapter 4 (Art. 24 ? 43)Controller and processor Art. 24Responsibility of the controller Art. 25Data protection by design and by default Art. 26Joint controllers Art. 27Representatives of controllers or processors not established in the Union Art. 28Processor Art. 29Processing under the authority of the controller or processor Art. 30Records of processing activities Art. 31Cooperation with the supervisory authority Art. 32Security of processing Art. 33Notification of a personal data breach to the supervisory authority Art. 34Communication of a personal data breach to the data subject Art. 35Data protection impact assessment Art. 36Prior consultation Art. 37Designation of the data protection officer Art. 38Position of the data protection officer Art. 39Tasks of the data protection officer Art. 40Codes of conduct Art. 41Monitoring of approved codes of conduct Art. 42Certification Art. 43Certification bodies

Chapter 5 (Art. 44 ? 50)Transfers of personal data to third countries or international organisations Art. 44General principle for transfers Art. 45Transfers on the basis of an adequacy decision Art. 46Transfers subject to appropriate safeguards Art. 47Binding corporate rules Art. 48Transfers or disclosures not authorised by Union law Art. 49Derogations for specific situations Art. 50International cooperation for the protection of personal data   Chapter 6 (Art. 51 ? 59)Independent supervisory authorities Art. 51Supervisory authority Art. 52Independence Art. 53General conditions for the members of the supervisory authority Art. 54Rules on the establishment of the supervisory authority Art. 55Competence Art. 56Competence of the lead supervisory authority Art. 57Tasks Art. 58Powers Art. 59Activity reports   Chapter 7 (Art. 60 ? 76)Cooperation and consistency Art. 60Cooperation between the lead supervisory authority and the other supervisory authorities concerned Art. 61Mutual assistance Art. 62Joint operations of supervisory authorities Art. 63Consistency mechanism Art. 64Opinion of the Board Art. 65Dispute resolution by the Board Art. 66Urgency procedure Art. 67Exchange of information Art. 68European Data Protection Board Art. 69Independence Art. 70Tasks of the Board Art. 71Reports Art. 72Procedure Art. 73Chair Art

2. Confidentiality:

Each Party shall maintain the confidentiality of Confidential Information disclosed by the other Party and shall not disclose or use such information except as expressly permitted by this Agreement or required by law.

3. Data Protection:

The Parties shall process personal data in compliance with applicable data protection laws including GDPR, HIPAA, and AI Act as applicable.

4. Compliance and Audit:

The Parties shall comply with all applicable laws and industry standards related to the subject matter of this Agreement. Upon reasonable notice, the customer may audit the provider's relevant records to verify compliance.

5. Limitation of Liability:

Except for willful misconduct or gross negligence, neither Party's aggregate liability shall exceed the total fees paid under this Agreement in the twelve (12) months preceding the claim.

6. Termination:

Either Party may terminate this Agreement upon thirty (30) days' prior written notice if the other Party materially breaches any provision and fails to cure within the notice period. Obligations regarding confidentiality and data protection shall survive termination.

IN WITNESS WHEREOF, the Parties have executed this Agreement.

AI Compliance System

By: ______________________

Name: Automated Generator

Title: Compliance Engine

gdpr-info.eu

By: ______________________

Name: Website Source

Title: Public Information Provider

#002 ? Compliance Summary ? AI Compliance System vs www.oecd.org ? November 09, 2025

This Compliance Summary (the "Agreement") is entered into as of November 09, 2025 between AI Compliance System and www.oecd.org. The Parties agree as follows:

1. Scope of Services:

Just a moment...Enable JavaScript and cookies to continue

2. Confidentiality:

Each Party shall maintain the confidentiality of Confidential Information disclosed by the other Party and shall not disclose or use such information except as expressly permitted by this Agreement or required by law.

3. Data Protection:

The Parties shall process personal data in compliance with applicable data protection laws including GDPR, HIPAA, and AI Act as applicable.

4. Compliance and Audit:

The Parties shall comply with all applicable laws and industry standards related to the subject matter of this Agreement. Upon reasonable notice, the customer may audit the provider's relevant records to verify compliance.

5. Limitation of Liability:

Except for willful misconduct or gross negligence, neither Party's aggregate liability shall exceed the total fees paid under this Agreement in the twelve (12) months preceding the claim.

6. Termination:

Either Party may terminate this Agreement upon thirty (30) days' prior written notice if the other Party materially breaches any provision and fails to cure within the notice period. Obligations regarding confidentiality and data protection shall survive termination.

IN WITNESS WHEREOF, the Parties have executed this Agreement.

AI Compliance System

By: ______________________

Name: Automated Generator

Title: Compliance Engine

www.oecd.org

By: ______________________

Name: Website Source

Title: Public Information Provider

#003 ? Compliance Summary ? AI Compliance System vs digital-strategy.ec.europa.eu ? November 09, 2025

This Compliance Summary (the "Agreement") is entered into as of November 09, 2025 between AI Compliance System and digital-strategy.ec.europa.eu. The Parties agree as follows:

1. Scope of Services:

AI Act | Shaping Europe?s digital future Skip to main content enenSelect your languageClosebg?????????esespañolcs?e?tinadadanskdeDeutscheteestiel????????enEnglishfrfrançaisgaGaeilgehrhrvatskiititalianolvlatvie?ultlietuvi?humagyarmtMaltinlNederlandsplpolskiptportuguêsroromân?sksloven?inaslsloven??inafisuomisvsvenska SearchSearch Shaping Europe?s digital future MenuCloseMenuBackPrevious itemsNext itemsHomePoliciesActivitiesNewsLibraryFundingCalendarConsultationsAI Office Home?PoliciesArtificial IntelligenceEuropean approach to artificial intelligenceAI ActAI Act Page ContentsPage ContentsWhy do we need rules on AI?A risk-based approachHow does it all work in practice for providers of high-risk AI systems?A solution for the trustworthy use of large AI modelsSupporting complianceGovernance and implementationApplication timeline The AI Act is the first-ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally. The AI Act (Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence) is the first-ever comprehensive legal framework on AI worldwide. The aim of the rules is to foster trustworthy AI in Europe. For any questions on the AI Act, check out the AI Act Single Information platform. The?AI Act sets out a clear set of risk-based rules for AI developers and deployers regarding specific uses of AI. The AI Act is part of a wider package of policy measures to support the development of trustworthy AI, which also includes the?AI Innovation Package and the launch of AI Factories. Together, these measures guarantee safety, fundamental rights and human-centric AI, and strengthen uptake, investment and innovation in AI across the EU. To facilitate the transition to the new regulatory framework, the Commission has launched the?AI Pact, a voluntary initiative that seeks to support the future implementation, engage with stakeholders and invite AI providers and deployers from Europe and beyond to comply with the key obligations of the AI Act ahead of time. In parallel, the AI Act Service Desk is also providing information and support for a smooth and effective implementation of the AI Act across the EU. Why do we need rules on AI? The AI Act ensures that Europeans can trust what AI has to offer. While most AI systems pose limited to no risk and can contribute to solving many societal challenges, certain AI systems create risks that we must address to avoid undesirable outcomes. For example, it is often not possible to find out why an AI system has made a decision or prediction and taken a particular action. So, it may become difficult to assess whether someone has been unfairly disadvantaged, such as in a hiring decision or in an application for a public benefit scheme. Although existing legislation provides some protection, it is insufficient to address the specific challenges AI systems may bring. A risk-based approach The AI Act defines 4 levels of risk for AI systems: Unacceptable risk All AI systems considered a clear threat to the safety, livelihoods and rights of people are banned. The AI Act prohibits eight practices, namely: harmful AI-based manipulation and deception harmful AI-based exploitation of vulnerabilities social scoring Individual criminal offence risk assessment or prediction untargeted scraping of the internet or CCTV material to create or expand facial recognition databases emotion recognition in workplaces and education institutions biometric categorisation to deduce certain protected characteristics real-time remote biometric identification for law enforcement purposes in publicly accessible spaces High risk AI use cases that can pose serious risks to health, safety or fundamental rights are classified as high-risk. These high-risk use-cases include: AI safety components in critical infrastructures (e.g. transport), the failure of which could put the life and health

2. Confidentiality:

Each Party shall maintain the confidentiality of Confidential Information disclosed by the other Party and shall not disclose or use such information except as expressly permitted by this Agreement or required by law.

3. Data Protection:

The Parties shall process personal data in compliance with applicable data protection laws including GDPR, HIPAA, and AI Act as applicable.

4. Compliance and Audit:

The Parties shall comply with all applicable laws and industry standards related to the subject matter of this Agreement. Upon reasonable notice, the customer may audit the provider's relevant records to verify compliance.

5. Limitation of Liability:

Except for willful misconduct or gross negligence, neither Party's aggregate liability shall exceed the total fees paid under this Agreement in the twelve (12) months preceding the claim.

6. Termination:

Either Party may terminate this Agreement upon thirty (30) days' prior written notice if the other Party materially breaches any provision and fails to cure within the notice period. Obligations regarding confidentiality and data protection shall survive termination.

IN WITNESS WHEREOF, the Parties have executed this Agreement.

AI Compliance System

By: ______________________

Name: Automated Generator

Title: Compliance Engine

digital-strategy.ec.europa.eu

By: ______________________

Name: Website Source

Title: Public Information Provider

#004 ? Compliance Summary ? AI Compliance System vs www.nist.gov ? November 09, 2025

This Compliance Summary (the "Agreement") is entered into as of November 09, 2025 between AI Compliance System and www.nist.gov. The Parties agree as follows:

1. Scope of Services:

AI Risk Management Framework | NIST Skip to main content NOTICE: Due to a lapse in annual appropriations, most of this website is not being updated. Learn more. Form submissions will still be accepted but will not receive responses at this time. Sections of this site for programs using non-appropriated funds (such as NVLAP) or those that are excepted from the shutdown (such as CHIPS and NVD) will continue to be updated. An official website of the United States government Here?s how you know Here?s how you know Official websites use .gov A .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPS A lock (Lock A locked padlock) or https:// means you?ve safely connected to the .gov website. Share sensitive information only on official, secure websites. https://www.nist.gov/itl/ai-risk-management-framework Search NIST Menu Close Publications What We Do All Topics Advanced communications Artificial intelligence Bioscience Buildings and construction Chemistry Cybersecurity and Privacy Electronics Energy Environment Fire Forensic science Health Information technology Infrastructure Manufacturing Materials Mathematics and statistics Metrology Nanotechnology Neutron research Performance excellence Physics Public safety Quantum information science Resilience Standards Transportation Labs & Major Programs Assoc Director of Laboratory Programs Laboratories Communications Technology Laboratory Engineering Laboratory Information Technology Laboratory Material Measurement Laboratory Physical Measurement Laboratory User Facilities NIST Center for Neutron Research CNST NanoFab Research Test Beds Research Projects Tools & Instruments Major Programs Baldrige Performance Excellence Program CHIPS for America Initiative Manufacturing Extension Partnership (MEP) Office of Advanced Manufacturing Special Programs Office Technology Partnerships Office Services & Resources Measurements and Standards Calibration Services Laboratory Accreditation (NVLAP) Quality System Standard Reference Materials (SRMs) Standard Reference Instruments (SRIs) Standards.gov Time Services Office of Weights and Measures Software Data Chemistry WebBook National Vulnerability Database Physical Reference Data Standard Reference Data (SRD) Storefront License & Patents

Computer Security Resource Center (CSRC) NIST Research Library News & Events News Events Blogs Feature Stories Awards Video Gallery Image Gallery Media Contacts About NIST About Us Leadership Organization Structure Budget & Planning Contact Us Visit Careers Student programs Work with NIST History NIST Digital Archives NIST Museum NIST and the Nobel Educational Resources Information Technology Laboratory AI Risk Management Framework AI RMF Development NIST AI RMF Playbook Engage Resources Perspectives FAQs AI @ NIST Quick Links Download the AI RMF 1.0 View the AI RMF Playbook Visit the AI Resource CenterOverview of the AI RMF In collaboration with the private and public sectors, NIST has developed a framework to better manage risks to individuals, organizations, and society associated with artificial intelligence (AI). The NIST AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.Released on January 26, 2023, the Framework was developed through a consensus-driven, open, transparent, and collaborative process that included a Request for I

2. Confidentiality:

Each Party shall maintain the confidentiality of Confidential Information disclosed by the other Party and shall not disclose or use such information except as expressly permitted by this Agreement or required by law.

3. Data Protection:

The Parties shall process personal data in compliance with applicable data protection laws including GDPR, HIPAA, and AI Act as applicable.

4. Compliance and Audit:

The Parties shall comply with all applicable laws and industry standards related to the subject matter of this Agreement. Upon reasonable notice, the customer may audit the provider's relevant records to verify compliance.

5. Limitation of Liability:

Except for willful misconduct or gross negligence, neither Party's aggregate liability shall exceed the total fees paid under this Agreement in the twelve (12) months preceding the claim.

6. Termination:

Either Party may terminate this Agreement upon thirty (30) days' prior written notice if the other Party materially breaches any provision and fails to cure within the notice period. Obligations regarding confidentiality and data protection shall survive termination.

IN WITNESS WHEREOF, the Parties have executed this Agreement.

AI Compliance System

By: _______________________

Name: Automated Generator

Title: Compliance Engine

www.nist.gov

By: _______________________

Name: Website Source

Title: Public Information Provider