

Russia — Federal Law No. 152-FZ (Personal Data)

Regional cybersecurity and data protection requirements for EMEA and Russia define legal obligations for protecting personal and critical data.



What it is

EMEA Russia — Regional Cybersecurity and Data Protection Requirements is a regional regulatory framework that helps organizations operating in Russia address cybersecurity risks, ensure data protection, and comply with national information security laws. The framework establishes key requirements for safeguarding personal and sensitive data, as well as securing IT infrastructure against cyber threats.

Published and enforced by various Russian regulatory bodies, including Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Media) and the FSB (Federal Security Service), these regulations are mandatory for organizations collecting, processing, or storing data of Russian citizens. The requirements cover areas such as data localization, mandatory breach notification, encryption standards, and internal cybersecurity controls.

At a glance

PUBLISHER Unknown	TYPE Regulation	VERSION 2019
EFFECTIVE July 1, 2025	DOMAIN Cybersecurity	FAMILY Global Privacy Regulations
REGION Russia	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: <https://priemnaya.duma.gov.ru/ru/info/inf/fz/>

Why it matters

- Enhance regulatory alignment** Support compliance with Russian legal mandates and sector-specific regulations to avoid penalties and ensure ongoing business operations.
- Strengthen data protection practices** Enable more robust safeguarding of sensitive personal data in accordance with stringent Russian privacy requirements.
- Improve security risk oversight** Enhance identification, assessment, and mitigation of cybersecurity threats specific to the Russian regulatory and threat landscape.
- Promote operational resilience** Support uninterrupted critical services and enable recovery readiness in response to cyber incidents or data breaches.

How SmartSuite supports 152-FZ

Personal Data Localization Tracking Track systems and data stores to ensure personal data is processed and stored within Russia as required.	Processing Records for Regulatory Transparency Maintain records of personal data categories, purposes, and processing activities for regulatory transparency.	Security Controls and Certification Alignment Map controls to Russian security standards (e.g., FSTEC/FSB) and track implementation and evidence.
Access Governance and Cryptographic Controls Manage user access, authentication, and encryption requirements aligned to national security expectations.	Incident Response and Breach Notification Track incidents and manage reporting obligations to Russian authorities and affected individuals.	Data Localization and Regulatory Inspection Readiness Provide dashboards showing localization status, control coverage, and readiness for regulatory inspections.

Common framework mappings

- CIS Controls v8.1
- COBIT 2019
- GDPR
- ISO 27001:2022
- ISO 27002:2022
- ISO 27701
- NIST CSF 2.0
- NIST 800-53 Rev.5
- PCI DSS 4.0.1
- SOC 2

Official resources

EU General Data Protection Regulation (GDPR) Official EU regulation outlining comprehensive data protection and privacy requirements for organizations. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679	EU Data Protection Authorities' Guidelines Provides guidance from EU Data Authorities on implementing GDPR requirements. edpb.europa.eu/our-work-tools/general-guidance_en
Russian Federal Law on Personal Data Describes Russia's legal requirements for processing and protecting personal data. pravo.gov.ru/proxy/ips/?docbody=&nd=102108098	BRICS Joint Declaration on Cybersecurity Outlines cybersecurity cooperation and principles among BRICS nations. static.kremlin.ru

Frequently asked questions

- What are the EMEA Russia regional cybersecurity and data protection requirements used for?**
These requirements establish a framework for protecting personal data and critical information infrastructure within the Russian Federation and EMEA jurisdictions. They aim to ensure organizations comply with local laws, such as Russia’s Federal Law No. 152-FZ (Personal Data Law), by defining how data must be collected, processed, stored, and transferred.
- Are the EMEA Russia cybersecurity and data protection requirements mandatory?**
Yes, these requirements are mandated by Russian federal laws and governmental regulators for organizations handling personal data or operating critical information infrastructure in Russia. Non-compliance can result in administrative penalties, fines, or operational restrictions as enforced by watchdog agencies like Roskomnadzor.
- What is the scope of the EMEA Russia data protection requirements?**
The scope includes any entity processing personal data of Russian citizens, operating within Russia, or managing networks and information systems deemed critical to national security. Cross-border data transfers, data localization, and the security of digital infrastructure are also addressed within this scope.

What key controls and documentation are required by the Russian data protection framework?

Key requirements include data localization, consent collection and management, mandatory notification of data breaches, designation of data protection officers, maintenance of processing registers, and security controls for critical infrastructure. Organizations must document their data processing activities and implement technical and organizational measures to ensure compliance.

How should organizations implement the EMEA Russia cybersecurity and data protection requirements?

Implementation involves conducting initial data inventories and risk assessments, establishing and documenting technical and organizational security measures, ensuring all personal data is stored within Russian territory, and regularly training staff. Regular audits and assessments are recommended to ensure ongoing compliance.

How do Russia's data protection requirements align with other international frameworks like GDPR?

While sharing similarities with the GDPR, such as data subject rights and consent requirements, Russian regulations require stricter data localization and cross-border processing controls. Organizations operating in both Russian and EU jurisdictions should address the nuanced differences and overlapping compliance obligations.

What are the ongoing compliance obligations under the EMEA Russia framework?

Ongoing obligations include regular internal audits, vulnerability assessments, timely breach notification to authorities, continuous monitoring of critical systems, and updates to processing documentation. Data protection impact assessments and staff awareness training are also required to maintain compliance.

How would SmartSuite support EMEA Russia — Regional Cybersecurity and Data Protection Requirements?

SmartSuite helps organizations manage these requirements by providing modules for risk tracking, control implementation, and evidence collection aligned to Russian regulations. The platform enables centralized management of data processing registers, audit readiness workflows, and real-time compliance reporting, supporting seamless demonstration of adherence to regulators.

License included / downloadable: Yes Official Russian federal laws and EMEA national/regional data protection regulations are published by governments and supervisory authorities and are publicly available on their official websites. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/emea-russia-regional-cybersecurity-and-data-protection-requirements-152-fz