

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CH-1	Chapter 1 — General Provisions	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 1	N/A	Scope of this Federal Law: This Federal Law regulates relations related to the processing of personal data carried out by federal government bodies, regional government bodies, local government bodies, legal entities, and individuals using automation tools, including in information and telecommunications networks, or without such tools where the processing corresponds to the nature of the actions performed using automation. The provisions of the Federal Law also apply to the processing of personal data of Russian citizens carried out by foreign legal entities or individuals on the basis of agreements to which Russian citizens are a party, or on the basis of the consent of a Russian citizen. The law does not apply to processing exclusively for personal or family needs, archival affairs, or processing of data constituting state secrets.	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 2	N/A	Purpose of this Federal Law: The purpose of this Federal Law is to ensure the protection of the rights and freedoms of persons and citizens when their personal data is processed, including protection of the right to privacy, personal and family secrets.	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 3	N/A	Basic Concepts Used in this Federal Law: This article defines the key terms used throughout the Federal Law, including: personal data (any information relating to a directly or indirectly identified or identifiable individual — the data subject); personal data permitted by the data subject for dissemination; operator (a state body, municipal body, legal entity, or individual that organizes and/or carries out personal data processing and determines the purposes, composition, and operations of processing); processing of personal data (any action or set of actions performed with personal data, including collection, recording, systematization, accumulation, storage, updating, extraction, use, transfer/dissemination/provision/access, anonymization, blocking, deletion, and destruction); automated processing; dissemination; provision; blocking; destruction; anonymization; personal data information system; and cross-border transfer of personal data.	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 4	N/A	Legislation of the Russian Federation in the Field of Personal Data: The legislation on personal data is based on the Constitution of the Russian Federation and international treaties and consists of this Federal Law and other federal laws governing specific cases and particulars of personal data processing. Government bodies, the Bank of Russia, and local authorities may issue subordinate regulatory acts on specific personal data processing matters, provided those acts do not restrict data subject rights or impose unauthorized obligations on operators. Such acts must be officially published. Regulatory acts that address cross-border transfers, special categories of personal data, biometric data, personal data of minors, or anonymized personal data must be coordinated with the authorized supervisory body within 30 days. Rules established in international treaties of the Russian Federation take precedence over this Federal Law. Decisions of intergovernmental bodies that contradict the Russian Constitution are not enforceable in the Russian Federation.	Functional	No Relationship	N/A	N/A	N/A	0	
CH-2	Chapter 2 — Principles and Conditions for Processing Personal Data	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 5	N/A	Principles of Personal Data Processing: Processing of personal data must be carried out on a lawful and fair basis. Processing must be limited to achieving specific, predetermined, and lawful purposes; processing incompatible with the purposes of collection is not permitted. Databases containing personal data whose processing purposes are incompatible may not be merged. Only personal data that meets the purposes of processing shall be processed, and the content and volume of processed data must correspond to the stated purposes (data minimization). Personal data must be accurate and, where necessary, up to date; the operator must take measures to remove or correct incomplete or inaccurate data. Personal data must be stored in a form that allows identification of the data subject no longer than required by the purposes of processing, unless a storage period is established by federal law or contract; upon achieving the processing purposes or when there is no further need, data must be destroyed or anonymized.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
Art. 6	N/A	Conditions for Personal Data Processing: Processing of personal data must comply with the principles and rules of this Federal Law. Processing is permitted in the following cases: with the consent of the data subject; where necessary to achieve purposes stipulated by international treaty or law; in connection with participation in judicial proceedings; to execute a court act; to perform functions of federal, regional, or municipal executive bodies and government services; to execute a contract to which the data subject is a party or beneficiary; to protect the vital interests of the data subject where consent is impossible; to exercise the rights and legitimate interests of the operator or third parties; for professional journalistic, literary, or scientific activities, provided data subject rights are not violated; for statistical or research purposes, provided data is anonymized; for anonymized data processed under the artificial intelligence experiment law (Federal Law No. 123-FZ); or where the data is subject to mandatory publication under a federal law. Special rules for processing special categories and biometric data are set out in Articles 10 and 11. The operator may delegate processing to another person by the data subject's consent under a contract; responsibility to the data subject remains with the operator, while the processing person is responsible to the operator. Where processing is delegated to a foreign person, both the operator and the processing person are jointly liable to the data subject.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
Art. 6	N/A	Conditions for Personal Data Processing: Processing of personal data must comply with the principles and rules of this Federal Law. Processing is permitted in the following cases: with the consent of the data subject; where necessary to achieve purposes stipulated by international treaty or law; in connection with participation in judicial proceedings; to execute a court act; to perform functions of federal, regional, or municipal executive bodies and government services; to execute a contract to which the data subject is a party or beneficiary; to protect the vital interests of the data subject where consent is impossible; to exercise the rights and legitimate interests of the operator or third parties; for professional journalistic, literary, or scientific activities, provided data subject rights are not violated; for statistical or research purposes, provided data is anonymized; for anonymized data processed under the artificial intelligence experiment law (Federal Law No. 123-FZ); or where the data is subject to mandatory publication under a federal law. Special rules for processing special categories and biometric data are set out in Articles 10 and 11. The operator may delegate processing to another person by the data subject's consent under a contract; responsibility to the data subject remains with the operator, while the processing person is responsible to the operator. Where processing is delegated to a foreign person, both the operator and the processing person are jointly liable to the data subject.	Functional	Intersects With	Data Subject Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with: (1) Plain language explaining the potential data privacy risks of the authorization; (2) A means to decline the authorization; and (3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Art. 7	N/A	Confidentiality of Personal Data: Operators and other persons who have gained access to personal data are obliged not to disclose to third parties or distribute personal data without the consent of the data subject, unless otherwise provided by federal law.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
Art. 8	N/A	Publicly Available Sources of Personal Data: For information purposes, publicly available sources of personal data (such as directories and address books) may be created. With the written consent of the data subject, publicly available sources may include the data subject's name, year and place of birth, address, telephone number, professional information, and other personal data communicated by the data subject. Information about a data subject must be excluded from publicly available sources at any time upon demand of the data subject or by court or other authorized government body decision.	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 9	N/A	Consent of the Data Subject to the Processing of His/Her Personal Data: The data subject freely, of their own will and in their own interest, decides to provide personal data and gives consent to its processing. Consent must be specific, informed, conscious, and unambiguous, and must be formalized separately from other information or documents signed by the data subject. Consent may be given in any form that allows confirmation of its receipt, unless a federal law requires written form. Written consent in electronic form signed with an electronic signature is equivalent to written consent on paper. Where required by federal law, written consent must include: the data subject's name and identity document details; the operator's name and address; the purpose of processing; the list of personal data and list of processing actions; the validity period of consent and the procedure for its withdrawal; and the data subject's signature. Consent may be withdrawn; if withdrawn, the operator may continue processing only on other lawful grounds. The operator bears the burden of proving that consent was obtained or that another lawful ground exists. In the case of the data subject's incapacity, consent is given by a legal representative; in case of death, consent is given by the data subject's heirs, unless consent was given during the data subject's lifetime. Personal data may be obtained from a third party only where that third party can confirm a lawful processing ground.	Functional	Intersects With	Data Subject Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with: (1) Plain language explaining the potential data privacy risks of the authorization; (2) A means to decline the authorization; and (3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Art. 10	N/A	Special Categories of Personal Data: Processing of special categories of personal data relating to racial or ethnic origin, political views, religious or philosophical beliefs, health status, or intimate life is prohibited, except in the cases provided by this article. Processing of special categories is permitted where: the data subject has given written consent; processing is permitted by the personal data dissemination rules of Article 10.1; processing is required by international readmission treaties; processing is carried out under the population census law; processing is required under social assistance, labor, or pension legislation; processing is necessary to protect the vital interests of the data subject or others and consent is impossible; processing concerns members of a public or religious organization in the course of its lawful activities without distribution to third parties without written consent; processing is necessary for the exercise of rights or in connection with the administration of justice; processing is carried out under defense, security, counter-terrorism, transport security, anti-corruption, operational search, enforcement, criminal procedure, or criminal enforcement legislation; processing is by prosecution authorities in connection with prosecutorial oversight; processing is under mandatory insurance or insurance legislation; processing is by state or municipal bodies for foster care placement of children; or processing is under citizenship legislation. Processing of health related data obtained through anonymization is permitted for improving public administration under Article 13.1 conditions. Processing of criminal record data may be performed by state and municipal bodies within their statutory powers, or by other persons as specifically provided by federal law. Special category processing must immediately cease when the grounds for such processing are eliminated, unless federal law provides otherwise.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
Art. 10	N/A	Special Categories of Personal Data: Processing of special categories of personal data relating to racial or ethnic origin, political views, religious or philosophical beliefs, health status, or intimate life is prohibited, except in the cases provided by this article. Processing of special categories is permitted where: the data subject has given written consent; processing is permitted by the personal data dissemination rules of Article 10.1; processing is required by international readmission treaties; processing is carried out under the population census law; processing is required under social assistance, labor, or pension legislation; processing is necessary to protect the vital interests of the data subject or others and consent is impossible; processing concerns members of a public or religious organization in the course of its lawful activities without distribution to third parties without written consent; processing is necessary for the exercise of rights or in connection with the administration of justice; processing is carried out under defense, security, counter-terrorism, transport security, anti-corruption, operational search, enforcement, criminal procedure, or criminal enforcement legislation; processing is by prosecution authorities in connection with prosecutorial oversight; processing is under mandatory insurance or insurance legislation; processing is by state or municipal bodies for foster care placement of children; or processing is under citizenship legislation. Processing of health related data obtained through anonymization is permitted for improving public administration under Article 13.1 conditions. Processing of criminal record data may be performed by state and municipal bodies within their statutory powers, or by other persons as specifically provided by federal law. Special category processing must immediately cease when the grounds for such processing are eliminated, unless federal law provides otherwise.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5	
Art. 10.1	N/A	Specifics of Processing Personal Data Permitted by the Data Subject for Dissemination: Consent to the processing of personal data permitted by the data subject for dissemination must be formalized separately from other consents. The operator must enable the data subject to specify, for each category of personal data listed in the consent, the particular data items consented to. Where the data subject directly discloses personal data to an unlimited circle of persons without providing consent under this article, the burden of proving the lawfulness of subsequent dissemination or other processing lies with each person who carries out such dissemination or processing. The same burden applies where data was disclosed due to an offense, crime, or force majeure. Where consent does not clearly indicate agreement to dissemination, the data may be processed by the operator to whom it was provided but may not be disseminated. The data subject may, in the consent, establish prohibitions and conditions on processing by an unlimited circle of persons; the operator must publish information about such conditions within 3 working days of receiving the consent. Established prohibitions do not apply to processing for state, public, or other public interests as defined by Russian law. Processing that is not permitted or is not in accordance with this article must cease within 3 working days of the data subject's demand, and in cases of court order, within 3 working days of the court ruling taking effect.	Functional	Intersects With	Data Subject Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with: (1) Plain language explaining the potential data privacy risks of the authorization; (2) A means to decline the authorization; and (3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
Art. 11	N/A	Biometric Personal Data: Information characterizing the physiological and biological characteristics of a person on the basis of which the person's identity can be established (biometric personal data), used by the operator for identification purposes, may only be processed with the written consent of the data subject, except in the cases provided in this article. Biometric personal data may be processed without consent in connection with international readmission treaties, the administration of justice, mandatory state fingerprinting or genomic registration, and in cases provided for by legislation on defense, security, counter-terrorism, transport security, anti-corruption, operational search, public service, criminal procedure, criminal enforcement, entry/exit and citizenship, the legal status of foreign nationals, migration registration, and notarial activities. Providing biometric personal data may not be made mandatory except in the cases referred to in the preceding provision; an operator may not refuse to provide services if the data subject declines to provide biometric data or consent to processing, where obtaining consent is not mandatory under federal law.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
Art. 11	N/A	Biometric Personal Data: Information characterizing the physiological and biological characteristics of a person on the basis of which the person's identity can be established (biometric personal data), used by the operator for identification purposes, may only be processed with the written consent of the data subject, except in the cases provided in this article. Biometric personal data may be processed without consent in connection with international readmission treaties, the administration of justice, mandatory state fingerprinting or genomic registration, and in cases provided for by legislation on defense, security, counter-terrorism, transport security, anti-corruption, operational search, public service, criminal procedure, criminal enforcement, entry/exit and citizenship, the legal status of foreign nationals, migration registration, and notarial activities. Providing biometric personal data may not be made mandatory except in the cases referred to in the preceding provision; an operator may not refuse to provide services if the data subject declines to provide biometric data or consent to processing, where obtaining consent is not mandatory under federal law.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
Art. 12	N/A	Cross-Border Transfer of Personal Data: Cross-border transfer of personal data is carried out in accordance with this Federal Law and international treaties of the Russian Federation. The authorized supervisory body approves a list of foreign states that ensure adequate protection of the rights of personal data subjects, including all parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and other states meeting comparable standards of confidentiality and security. Before beginning cross-border transfer, the operator must notify the authorized supervisory body of its intent, providing details including: the operator's name and address; the legal basis and purpose of transfer; categories of data and data subjects; list of destination countries; and the date of the operator's assessment of the receiving party's confidentiality and security practices. Prior to submitting the notification, the operator must obtain from the receiving foreign authority or entity information on its data protection measures and conditions of processing cessation, on the legal regulation of the destination country (where the country is not a party to the Council of Europe Convention and not on the adequate protection list), and identifying contact information of the recipient. The transfer may be prohibited or restricted to protect the foundations of the Russian constitutional order, morality, health, citizens' rights, national defense and security, economic and financial interests, or Russia's sovereignty and international standing. Decisions on prohibition or restriction are made by the authorized supervisory body within 10 working days of receiving the notification. An operator may begin cross-border transfer to countries on the adequate protection list after submitting the notification, pending the supervisory body's decision.	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
Art. 13	N/A	Specifics of Processing Personal Data in State or Municipal Information Systems: State and municipal bodies may, within their statutory powers, create state or municipal personal data information systems. Federal laws may establish special rules for recording personal data in such systems, including the use of different methods of identifying specific data subjects. Rights and freedoms of citizens may not be restricted on the basis of the method of identification used, and methods that are offensive or degrading to human dignity are prohibited. A state population register may be established by federal law to ensure the rights of data subjects in connection with processing by state or municipal systems.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
Art. 13.1	N/A	Specifics of Processing Personal Data Obtained from Anonymization: The federal executive body responsible for IT policy (the authorized IT regulatory body) may, in cases determined by the Russian Government, form datasets from anonymized personal data grouped by a defined criterion, provided subsequent processing cannot identify specific data subjects. Formation of such datasets from special categories (Article 10) or biometric data (Article 11) is prohibited, with limited exceptions under Article 10 Part 2.1. Operators receiving a formal requirement must anonymize the relevant personal data in accordance with Government-approved standards and submit it to the authorized IT regulatory body's state information system. Access to datasets is restricted: within the first year, only state bodies and subordinate organizations may access data sourced from non-governmental operators; Russian legal entities and citizens meeting strict eligibility criteria may access after one year. Processing is permitted only within the designated state system — extraction, transfer, or export of datasets is prohibited. Results of processing that could harm defense or state security may be banned, and providing results to foreign entities is prohibited except under an international treaty, federal law, or Presidential decision.	Functional	Intersects With	De-identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
Art. 13.1	N/A	Specifics of Processing Personal Data Obtained from Anonymization: The federal executive body responsible for IT policy (the authorized IT regulatory body) may, in cases determined by the Russian Government, form datasets from anonymized personal data grouped by a defined criterion, provided subsequent processing cannot identify specific data subjects. Formation of such datasets from special categories (Article 10) or biometric data (Article 11) is prohibited, with limited exceptions under Article 10 Part 2.1. Operators receiving a formal requirement must anonymize the relevant personal data in accordance with Government-approved standards and submit it to the authorized IT regulatory body's state information system. Access to datasets is restricted: within the first year, only state bodies and subordinate organizations may access data sourced from non-governmental operators; Russian legal entities and citizens meeting strict eligibility criteria may access after one year. Processing is permitted only within the designated state system — extraction, transfer, or export of datasets is prohibited. Results of processing that could harm defense or state security may be banned, and providing results to foreign entities is prohibited except under an international treaty, federal law, or Presidential decision.	Functional	Intersects With	Data Anonymization	PRI-05.3	Mechanisms exist to mask sensitive and/or regulated data through data anonymization, pseudonymization, redaction and/or de-identification.	5	
CH-3	Chapter 3 — Rights of Personal Data Subjects	N/A	Functional	No Relationship	N/A	N/A	N/A	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
Art. 14	N/A	Right of the Data Subject to Access His/Her Personal Data: A data subject has the right to obtain information about the processing of his or her personal data and to demand from the operator that inaccurate, incomplete, outdated, unlawfully obtained, or unnecessary personal data be corrected, blocked, or destroyed. The operator must provide the requested information within 10 working days of receiving the request, extendable by up to 5 working days with a reasoned notice to the data subject. The data subject may submit a repeat request no earlier than 30 days after the initial request, unless a shorter period is established by law or contract; a repeat request within that window is permitted only if the first response was incomplete. The information provided must include: confirmation of processing and its legal grounds and purposes; categories of data processed and their source; storage periods; details of persons with access; information on cross-border transfers; and the procedure for exercising data subject rights. Access may be restricted under federal law in cases involving national security, counter-intelligence, criminal proceedings, anti-money laundering, or transport security purposes.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
Art. 15	N/A	Rights of Data Subjects When Personal Data is Processed for Direct Marketing or Political Campaigning: Processing of personal data for the purpose of promoting goods, works, or services through direct contact with potential consumers via communication means, or for political campaigning, is permitted only with the prior consent of the data subject. The burden of proving that consent was obtained lies with the operator. The operator is required to immediately cease such processing upon the data subject's demand.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
Art. 16	N/A	Rights of Data Subjects When Decisions Are Made Solely on the Basis of Automated Processing: Decisions producing legal consequences for a data subject or otherwise affecting the data subject's rights and legitimate interests, made solely on the basis of automated processing of personal data, are prohibited except where the data subject has given written consent or where permitted by federal laws that also establish data subject rights safeguards. The operator is obliged to explain to the data subject the procedure for making such a decision, the possible legal consequences, and the procedure for protecting the data subject's rights. The operator must review any objection raised by the data subject within 30 days of receipt and notify the data subject of the outcome.	Functional	Intersects With	Automated Decision-Making Technology (ADMT) For Data Subject Actions	PRI-19	Mechanisms exist to ensure data subject actions utilizing Automated Decision-Making Technology (ADMT) where computation replaces, or substantially replaces, human decisionmaking, conforms with all applicable statutory, regulatory and/or contractual obligations.	5	
Art. 16	N/A	Rights of Data Subjects When Decisions Are Made Solely on the Basis of Automated Processing: Decisions producing legal consequences for a data subject or otherwise affecting the data subject's rights and legitimate interests, made solely on the basis of automated processing of personal data, are prohibited except where the data subject has given written consent or where permitted by federal laws that also establish data subject rights safeguards. The operator is obliged to explain to the data subject the procedure for making such a decision, the possible legal consequences, and the procedure for protecting the data subject's rights. The operator must review any objection raised by the data subject within 30 days of receipt and notify the data subject of the outcome.	Functional	Intersects With	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how data subjects can opt-out of Automated Decision-Making Technology (ADMT).	3	
Art. 16	N/A	Rights of Data Subjects When Decisions Are Made Solely on the Basis of Automated Processing: Decisions producing legal consequences for a data subject or otherwise affecting the data subject's rights and legitimate interests, made solely on the basis of automated processing of personal data, are prohibited except where the data subject has given written consent or where permitted by federal laws that also establish data subject rights safeguards. The operator is obliged to explain to the data subject the procedure for making such a decision, the possible legal consequences, and the procedure for protecting the data subject's rights. The operator must review any objection raised by the data subject within 30 days of receipt and notify the data subject of the outcome.	Functional	Intersects With	Automated Decision-Making Technology (ADMT) Transparency	PRI-19.3	Mechanisms exist to provide data subjects with sufficient details of the logic and parameters used by Automated Decision-Making Technology (ADMT) to process the Personal Data (PD) to generate an output with respect to the data subject.	3	
Art. 17	N/A	Right to Appeal Actions or Inactions of the Operator: If a data subject believes that an operator is processing his or her personal data in violation of this Federal Law or is otherwise violating the data subject's rights and freedoms, the data subject may appeal the operator's actions or inactions to the authorized body for the protection of the rights of personal data subjects or to a court. The data subject has the right to protection of his or her rights and legitimate interests, including the right to claim damages and/or compensation for moral harm through court proceedings.	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	
CH-4	Chapter 4 — Obligations of the Operator	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 18	N/A	Obligations of the Operator When Collecting Personal Data: At the time of collection, the operator must, upon request by the data subject, provide information about the processing as specified in Article 14. Where federal law makes the provision of personal data or consent mandatory, the operator must explain the legal consequences of refusing. Where personal data is collected not from the data subject, the operator must — before processing begins — notify the data subject of the operator's identity, the purposes and legal grounds for processing, the intended users, the data subject's rights, and the source of the data; exemptions apply where the data subject was already informed, data was obtained under a federal law or contract, or notification would harm third-party rights. Personal data of Russian citizens may only be recorded, updated, accumulated, stored, refined, or extracted using databases located on Russian territory, except in limited cases under Article 6 Part 1 (items 2, 3, 4, and 8 — treaty obligations, judicial proceedings, executive function, and journalistic activity).	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
Art. 18.1	N/A	Measures Aimed at Ensuring the Operator's Fulfillment of Obligations: The operator is required to take measures necessary and sufficient to ensure compliance with this Federal Law and must independently determine the composition and list of such measures unless otherwise required by law. Required measures include: appointing a person responsible for organizing personal data processing (for legal entities); issuing a personal data processing policy and internal acts specifying, for each processing purpose, the categories of data, subjects, methods, storage periods, and destruction procedures; applying legal, organizational, and technical security measures per Article 19; conducting internal control and/or audits of compliance; conducting a harm assessment to data subjects in case of violations; and training employees who directly process personal data. Operators collecting data via the internet must publish their privacy policy and security measure information on their website. The Government establishes a list of mandatory measures for state and municipal body operators. Operators must, upon request by the authorized supervisory body, produce documentation demonstrating that these measures have been taken.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
Art. 18.1	N/A	Measures Aimed at Ensuring the Operator's Fulfillment of Obligations: The operator is required to take measures necessary and sufficient to ensure compliance with this Federal Law and must independently determine the composition and list of such measures unless otherwise required by law. Required measures include: appointing a person responsible for organizing personal data processing (for legal entities); issuing a personal data processing policy and internal acts specifying, for each processing purpose, the categories of data, subjects, methods, storage periods, and destruction procedures; applying legal, organizational, and technical security measures per Article 19; conducting internal control and/or audits of compliance; conducting a harm assessment to data subjects in case of violations; and training employees who directly process personal data. Operators collecting data via the internet must publish their privacy policy and security measure information on their website. The Government establishes a list of mandatory measures for state and municipal body operators. Operators must, upon request by the authorized supervisory body, produce documentation demonstrating that these measures have been taken.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
Art. 19	N/A	Measures to Ensure the Security of Personal Data During Processing: The operator must take necessary legal, organizational, and technical measures to protect personal data against unlawful or accidental access, destruction, alteration, blocking, copying, disclosure, distribution, and other unlawful actions. Security is achieved through: identifying threats to personal data in information systems; applying organizational and technical measures to meet Government-established security levels; using certified information protection tools (including certified tools with a data destruction function); evaluating effectiveness before systems enter operation; tracking data storage media; detecting and responding to unauthorized access and cyber incidents; recovery of modified or destroyed data; establishing access rules and logging all actions on personal data; and ongoing security monitoring. The Government establishes security levels and corresponding requirements. Technical and organizational requirements for each security level are set by the FSB and FSTEC. The operator must interact with the national GosSOPKA system, including reporting computer incidents involving unlawful transfer of personal data. Special handling rules apply to personal data of FSB personnel, foreign intelligence officers, protected witnesses, and police officers.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
Art. 20	N/A	Obligations of the Operator When Addressed by the Data Subject, His/Her Representative, or the Authorized Supervisory Body: Upon a data subject's request, the operator must inform the data subject of the existence of personal data relating to that subject and provide access within 10 working days (extendable by up to 5 working days with reasoned notice). If the operator refuses to provide information, it must give a written reasoned response citing the specific legal basis within 10 working days (extendable). The operator must provide free-of-charge access to the data and, where data is shown to be incomplete, inaccurate, or outdated, make necessary corrections within 7 working days of receiving supporting evidence. Where data was unlawfully obtained or is unnecessary for the stated purpose, the operator must destroy it within 7 working days. Requests from the authorized supervisory body must be responded to within 10 working days (extendable by up to 5 working days).	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
Art. 21	N/A	Obligations of the Operator to Remedy Violations, and to Correct, Block, and Destroy Personal Data: Upon identifying unlawfully processed or inaccurate personal data — whether on its own initiative, through a data subject's request, or via the supervisory authority — the operator must immediately block the relevant data for the duration of the verification period. If inaccuracy is confirmed, the operator must correct the data within 7 working days and lift the block. If unlawful processing is confirmed, the operator must cease such processing within 3 working days; if making processing lawful is impossible, it must destroy the data within 10 working days and notify the data subject and the supervisory authority. In the event of an incident resulting in unlawful or accidental transfer, disclosure, or unauthorized access to personal data, the operator must notify the authorized supervisory body within 24 hours (including likely causes, estimated harm, and responsible contact person), and within 72 hours report the results of the internal investigation and identify responsible persons if possible. Where the processing purpose has been achieved or consent has been withdrawn, the operator must cease processing and destroy the data within 30 days (subject to contractual or legal exceptions); where immediate destruction is impossible, data must be blocked and destroyed within no more than 6 months.	Functional	Intersects With	Data Subject Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns and/or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
Art. 22	N/A	Notification of Personal Data Processing: Before beginning to process personal data, the operator must notify the authorized supervisory body of its intent to process personal data, except in limited cases (e.g., data included in state security systems, processing exclusively without automation means, and transport security cases). The notification must be in written or electronic form and include: the operator's name and address; purposes of processing; security measures and any cryptographic tools used; the name of the person responsible for organizing processing and their contact details; start date of processing; term or conditions for cessation; information on cross-border transfers; the location of databases containing personal data of Russian citizens; and security compliance information. For each processing purpose, the operator must specify categories of data, categories of data subjects, legal basis, list of processing actions, and processing methods. The authorized body enters the information into the operator register within 30 days; the register is publicly accessible (excluding security tool information). Operators must notify the supervisory body of any changes to registered information no later than the 15th day of the month following the month in which the change occurred, and must notify of cessation of processing within 10 working days. No fees may be charged to operators for processing notifications.	Functional	Intersects With	Register As A Data Controller and/or Data Processor	PRI-15	Mechanisms exist to register as a data controller and/or data processor, including registering databases containing Personal Data (PD) with the appropriate Data Authority, when necessary.	5	
Art. 22.1	N/A	Persons Responsible for Organizing Personal Data Processing in Organizations: An operator that is a legal entity is required to appoint a person responsible for organizing the processing of personal data. This person reports directly to the executive body of the organization and receives instructions from it. The operator must provide this responsible person with all the information specified in Article 22 Part 3. The responsible person's duties include: internal monitoring of compliance with personal data legislation; communicating data protection requirements and internal policies to staff; and organizing and/or overseeing the receipt and handling of data subject requests and appeals from data subjects or their representatives.	Functional	Intersects With	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO): (1) Based on professional qualifications; and (2) To be involved in all issues related to how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed.	5	
CH-5	Chapter 5 — Federal State Control (Supervision) over Personal Data Processing. Liability for Violations of This Federal Law	N/A	Functional	No Relationship	N/A	N/A	N/A	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
Art. 23	N/A	Authorized Body for the Protection of the Rights of Personal Data Subjects: The authorized supervisory body is a federal executive authority that independently exercises control and supervision over whether personal data processing complies with Russian law. Its powers include: requesting information from any person; verifying operator notifications; requiring operators to correct, block, or destroy unlawful or inaccurate data; restricting access to unlawfully processed data; seeking suspension or termination of unlawful processing; bringing court actions on behalf of data subjects; referring matters to prosecutors and law enforcement; proposing regulatory improvements; and imposing administrative liability. The body is obliged to protect data subject rights; consider complaints from citizens and legal entities; maintain the operator register and a register of personal data incidents; cooperate internationally with foreign data protection authorities; publish an annual report to the President, Government, and Federal Assembly; and establish requirements and methods for personal data anonymization. Its control and supervision powers may not be delegated to other state bodies.	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 23.1	N/A	Federal State Control (Supervision) over Personal Data Processing: Federal state control and supervision over personal data processing is carried out by the same federal executive authority responsible for controlling compliance with personal data legislation. The subject of supervision is operators' adherence to mandatory requirements established by this Federal Law and related regulations. Supervision is conducted in accordance with Federal Law No. 248-FZ of 31 July 2020 on State Control (Supervision) and Municipal Control, with the exception of inspection activities conducted without interaction with the controlled party. Evidence of harm or threat of harm discovered through monitoring activities without direct contact with an operator serves as grounds for initiating a formal inspection. The detailed regulations governing control activities — including inspections conducted without operator interaction — are approved by the Russian Government.	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 24	N/A	Liability for Violation of the Requirements of This Federal Law: Persons found guilty of violating the requirements of this Federal Law bear liability in accordance with Russian legislation. Moral (non-material) harm caused to a data subject through violation of his or her rights, violation of personal data processing rules, or violation of data security requirements is subject to compensation under Russian law. Compensation for moral harm is awarded independently of and in addition to compensation for material losses and actual damages suffered by the data subject.	Functional	No Relationship	N/A	N/A	N/A	0	
CH-6	Chapter 6 — Final Provisions	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
Art. 25	N/A	Final Provisions: This Federal Law entered into force 180 days after its official publication. Personal data included in information systems before the law's entry into force is subject to the law's requirements from that date. Operators who were processing personal data before 1 July 2011 were required to submit additional information specified in Article 22 Part 3 to the supervisory body no later than 1 January 2013. Operators who processed personal data before the law's entry into force and continued to do so were required to submit the notification under Article 22 Part 3 no later than 1 January 2008. Special rules apply to personal data processing in the context of state and municipal services in the city of Moscow under the relevant territorial accession law. The law was signed by President V. Putin, Moscow, Kremlin, 27 July 2006, No. 152-FZ.	Functional	No Relationship	N/A	N/A	N/A	0	