

**Federal Law of 27 July 2006 N 152-FZ  
ON PERSONAL DATA**

**Adopted by State Duma on 8 July 2006  
Approved by Council of Federation on 14 July 2006**

**Chapter 1. General Provisions**

**Section 1. Sphere of Regulation**

1. This Federal Law regulates activities related to the processing of personal data by federal, regional and other state agencies (hereinafter, “state agencies”), municipal and other local authorities (hereinafter, “municipal authorities”), legal entities and individuals, both automatically and manually, provided that manual data processing is by its nature similar to automatic data processing.

2. This Federal Law does not apply to activities related to:

1) personal data processing by individuals exclusively for personal or family needs, provided that such processing does not infringe upon the rights of individuals whose data are being processed;

2) storage, arrangement, registration and use of personal data contained in the files kept by the State Archives of the Russian Federation and in other archive files as envisaged by the Russian laws on the archive system;

3) processing of data for the purposes of their registration with the Unified Register of Private Entrepreneurs due to the activities of such individuals as private entrepreneurs, provided that such data are processed in compliance with laws of the Russian Federation; or

4) processing of personal data which are referred to state secrecy by law.

**Section 2. Aim of Federal Law**

The aim of this Federal Law is to procure the protection of a person’s rights and liberties while processing his/her personal data, including the right to privacy, personal and family secrecy.

**Section 3. Basic Terms of Federal Law**

In this Law the following terms are used:

1. **personal data** – any information referring to a particular individual or which can be used to verify an individual identity (hereinafter, “individual concerned”) including his/her surname; given name; patronymic; year, month, day and place of birth; address; marital status; social and property status; education; occupation; and income level, etc.

2. **operator** – state agency, municipal authority, legal entity or individual who organizes and/or processes personal data as well as determines the purposes and scope of personal data processing;

3. **personal data processing** – actions (operations) with personal data, including collection, arrangement, accumulation, storage, specification (updating, changing), use, distribution (including transfer), anonymizing, blocking and destruction of personal data;

4. **distribution of personal data** – actions related to the transfer of personal data to specific persons (transfer of personal data) or making the data available to the general public, including publication in the media, distribution via communication networks or otherwise granting access to personal data;

5. **use of personal data** – actions (operations) performed on personal data by the operator for decision-making and other purposes which entail legal consequences for the individual concerned or third persons or otherwise affect rights and liberties of the individual concerned or third persons;

6. **blocking of personal data** – the temporary cessation of collection, arrangement, accumulation, use or distribution of personal data (including transfer of personal data);

7. **destruction of personal data** – actions performed on personal data contained in the respective database that prevent such data from being restored or actions aimed at the physical destruction of the tangible medium of personal data;

8. **anonymization of personal data** – actions performed on personal data that do not permit the identity of the individual concerned to be verified solely from such anonymized data;

9. **personal data database** – information system that contains personal data as well as information technologies and hardware used for data processing, either automatically or not;

10. **confidentiality of personal data** – the compulsory requirement not to allow distribution of personal data without the consent of the individual concerned (unless permitted by law) which is imposed on the operator or a person who has obtained access to personal data;

11. **cross-border transfer of personal data** – cross-border transfer of personal data by an operator from the Russian Federation to a foreign state agency, foreign legal entity or individual located in a foreign state; and

12. **publicly available personal data** – personal data open to general use on the grounds that consent was given by the individual concerned or personal data to which the law requirement on confidentiality does not apply.

#### **Section 4. Legislative Grounds for Protection of Personal Data in the Russian Federation**

1. The Russian legislation on data protection is based on the Constitution of the Russian Federation and international treaties entered into by the Russian Federation and is comprised of this Federal Law and other federal laws which regulate particular issues related to personal data processing.

2. On the grounds of and pursuant to the federal laws, state agencies may, within their scope of competence, adopt regulations with respect to particular issues related to personal data

processing. Such regulations governing particular issues of personal data processing shall not include provisions that would restrict personal rights. Such regulations shall be officially published, except where publication of the regulations and certain provisions thereof contain data where access to such data is limited by federal laws.

3. Specific federal laws and other legal acts of the Russian Federation with respect to manual processing of personal data can be adopted regarding this Federal Law.

4. If international treaties entered into by the Russian Federation establish regulations different from those provided by this Federal Law, the regulations of such international treaties shall apply.

## **Chapter 2. Principles and Conditions of Personal Data Processing**

### **Section 5. Principles of Personal Data Processing**

1. The following principles shall be followed when processing personal data:

- 1) legality of goals, faithful and diligent conduct when processing personal data;
- 2) compliance with purposes determined and declared at the time of collection of personal data to process personal data exclusively within the scope of the authorities granted to them;
- 3) compliance of scope and character of personal data to be processed and methods of processing with intended purposes of such data processing;<sup>1</sup>
- 4) reliability of personal data, adequacy of personal data for processing purposes, inadmissibility to process personal data irrelevant to the purposes declared at the time of collection; and
- 5) inadmissibility to integrate information databases created for different purposes;

2. Personal data shall be stored in a way that allows verification of the identity of the individual concerned only to the extent necessary for processing purposes. Personal data shall be destroyed upon achieving the set goals as well as when such goals cease to be relevant.

### **Section 6. Conditions of Personal Data Processing**

1. Personal data processing by the operator shall be subject to the consent of the individual concerned subject to the exceptions described in part 2 of this Section.

2. No consent of the individual concerned referred to in part 1 of this Section is required in the following circumstances:

- 1) personal data are processed on the grounds of a federal law that sets forth the purpose, conditions of obtaining personal data, categories of individuals whose data shall be

---

<sup>1</sup> This is a literal translation of the Russian clause.

processed as well as scope of the operator's authority;

2) personal data are processed pursuant to an agreement to which the individual concerned is a party;

3) personal data are processed for statistical or other research purposes, provided that personal data have been anonymized;

4) personal data processing is required for the protection of the life, health or other vital interests of the individual concerned but it is not possible to obtain his/her consent;

5) personal data are processed for mail delivery purposes, for collection of fees by telecommunication providers and for the purpose of settling disputes with telecommunication providers;

6) personal data are processed by journalists for professional purposes or by other persons for research, literary or other creative purposes, provided that the rights and liberties of the individual concerned are not infringed thereby; and

7) processing of personal data which are subject to public disclosure, including the data of public officers, civil servants and candidates to state or municipal elective offices.

3. Sections 10 and 11 of this Federal Law respectively establish procedures for processing special categories of personal data and biometric personal data.

4. If the operator subcontracts a third person to process personal data, a material condition of the respective agreement shall be the subcontractor's undertaking to provide for the confidentiality and protection of the personal data to be processed.

## **Section 7. Confidentiality of Personal Data**

1. Operators and third persons having access to personal data shall provide for the confidentiality of such data except in cases envisaged by part 2 of this Section.

2. The confidentiality requirement does not apply to:

1) anonymized personal data; or

2) publicly available personal data.

## **Section 8. Public Sources of Personal Data**

1. Public sources of personal data (such as reference books and directories) may be created for database purposes. The following data may be included in such public sources with the consent of the individual concerned: surname, given name, patronymic, year and place of birth, address, customer's number, occupation and other personal data submitted by the individual concerned.

2. Personal data may be at any time removed from the public sources upon request of the individual concerned, on the grounds of a court ruling or by a directive of the competent state agency.

## **Section 9. Individual's Consent to Personal Data Processing**

1. The individual concerned decides whether to submit his/her personal data and gives his/her consent to data processing at his/her sole discretion, except as in cases envisaged in part 2 of this Section. The individual may revoke his/her consent to personal data processing.

2. This Federal Law and other federal laws describe situations when the individual concerned is obliged to provide his/her personal data for the purposes of the protection of national security, morals, health, rights and legal interests of third persons, as well as for defense and state security purposes.

3. The operator bears the burden of proof that the individual's consent to personal data processing has been obtained. If publicly available personal data are processed, the operator bears the burden of proof that such personal data have been made open to general use.

4. In certain cases envisaged by this Federal Law, processing of personal data is allowed upon obtaining the individual's consent in writing only. Such written consent of the individual concerned to processing of his/her personal data shall include the following information:

1) surname, given name, patronymic, address of the individual concerned, basic identity document number, date of basic identity document issue and issuing authority;

2) name (surname, given name and patronymic) and address of the operator intending to obtain the individual's consent;

3) purpose of personal data processing;

4) list of personal data to be processed with the consent of the individual concerned;

5) operations to be performed on the personal data with the consent of the individual concerned; general description of methods applied by the operator when processing personal data; and

6) the term for which the consent is given as well as the procedure of revoking the consent.

5. No separate consent to processing of particular personal data is required if the written consent of the individual concerned covers such particular personal data.

6. If the individual concerned is incapacitated, the written consent shall be given by his/her legal representative.

7. In case of the death of the individual concerned, the written consent to personal data processing shall be given by heirs of such individual, provided such consent was not given by the individual concerned *inter vivos*.

## **Section 10. Special Categories of Personal Data**

1. Processing of special categories of personal data such as race, nationality, political, religious, philosophic views, health and private life, are not permitted save as in cases envisaged in part 2 of this Section.

2. Processing of special personal data listed in part 1 of this Section is permitted in the

following cases:

1) the individual concerned has given his/her written consent to the processing of such personal data;

2) the personal data are open to general use;

3) the personal data relate to the health of the individual concerned and should be processed for the protection of his/her life, health, other vital interests or of the life, health or other vital interests of third persons but it is not possible to obtain the consent of the individual concerned;

4) the personal data are processed for medical, preventive, or diagnostic purposes, when providing medical or social services on the condition that such personal data are processed by professional doctors bound by medical secrecy in accordance with applicable laws of the Russian Federation;

5) personal data of members of non-governmental or religious organizations are processed by the respective organizations in compliance with applicable laws of the Russian Federation and for legitimate purposes set forth by the constituent documents of such organization that personal data shall not be distributed without the written consent of the individual concerned.

6) personal data are processed for the administration of justice;

7) personal data are processed under the laws of the Russian Federation on state security, criminal investigation or on the grounds of law enforcement regulations of the Russian Federation.

3. Personal data on previous convictions may be processed by state agencies and municipal authorities within their competence as established by the laws of the Russian Federation as well as by other persons in cases and subject to procedures established in respective federal laws.

4. Processing of special categories of personal data in the cases described in parts 2 and 3 of this Section shall be promptly discontinued if the reasons for which personal data are processed have ceased to exist.

#### **Section 11. Biometric Personal Data**

1. Physiologic data that allows the identity of the individual to be verified (biometric personal data) may be processed with the written consent of the individual concerned subject to exceptions in part 2 of this Section.

2. No consent of the individual concerned is required if biometric personal data are processed for the administration of justice or in cases envisaged by the laws of the Russian Federation on state security, criminal investigation, state service, law enforcement and in relation to crossing the state borders of the Russian Federation.

#### **Section 12. Cross-Border Transfer of Personal Data**

1. Before transferring personal data, the operator shall make certain that the foreign state

of the territory to which the personal data are to be transferred procure a sufficient level of personal data protection.

2. Cross-border transfers of personal data to foreign states that provides a sufficient level of personal data protection shall be performed in compliance with this Federal Law and may be prohibited or restricted in order to protect the national security, morals, health, rights and legal interests of people as well as for state defense and security reasons.

3. Cross-border transfers of personal data to foreign states that do not procure a sufficient level of personal data protection are allowed in the following cases:

- 1) the consent of the individual concerned has been obtained;
- 2) for purposes established by international treaties entered into by the Russian Federation regarding cooperation on visa matters as well as international treaties regarding cooperation in civil, family and criminal proceedings;
- 3) in cases envisaged by federal laws when this is required for the protection of national security, for state defense and security reasons;
- 4) performance of an agreement to which the individual concerned is a party;
- 5) protection of the life, health and other vital interests of the individual concerned or of third persons, if it is not possible to obtain the written consent of the individual concerned.

### **Section 13. Processing of Personal Data by State Agencies and Municipal Authorities**

1. State agencies and municipal authorities create state/municipal databases containing personal data within the scope of their competence established by federal laws.

2. Federal laws may provide for specific requirements for the registration of personal data with state or municipal databases, including requirements to use certain identification markers that would allow personal data contained in the respective state/municipal database to be correlated with the particular individuals.

3. Personal rights and liberties may not be restricted solely due to the fact that various means of processing or identifying personal data contained in state/municipal databases are used. Identification markers for personal data contained in state/municipal databases affecting dignity or disparaging the individual concerned shall not be used.

4. In order to protect personal rights with respect to personal data processing by state agencies or municipal authorities, a public state register may be created. The legal status of such register and the procedures for handling thereof shall be established by a respective federal law.

## **Chapter 3. Rights of Individual**

### **Section 14. Right of Access to Personal Data**

1. The individual concerned has the right to obtain information on the operator, its

domicile, whether the operator holds the individual's personal data as well as the right to get acquainted with such personal data, except in cases envisaged in part 5 of this Section. The individual concerned is entitled to require the operator to correct, block or destroy his/her personal data if such data are incomplete, obsolete, incorrect, were obtained illegally or are irrelevant for the purposes declared at collection thereof. Further, the individual concerned is entitled to take legal measures for the protection of his/her rights.

2. Information on available personal data shall be provided to the individual concerned in a comprehensive form. No personal data of other individuals may be disclosed in relation thereto.

3. Access to personal data is granted to the individual concerned or his/her legal representative on the grounds of either oral or written inquiry. The inquiry shall include the basic identification document number of the individual concerned or his/her legal representative, date of its issue and issuing authority and shall be signed by the individual concerned or his/her legal representative. The inquiry may be sent by e-mail, in which case it shall bear an electronic signature in accordance with the laws of the Russian Federation.

4. On the grounds of an oral or written inquiry, the individual concerned has the right to obtain information related to the processing of his/her personal data, including:

- 1) confirmation that his/her personal data are processed by the operator as well as information on the purpose of such processing;
- 2) the methods of processing personal data used by the operator;
- 3) information on persons who have access to the personal data or persons to whom such access can be granted;
- 4) a list of personal data processed and the sources from which personal data were obtained;
- 5) the duration of processing and storage of the personal data; and
- 6) information on the possible legal consequences of personal data processing for the individual concerned.

5. The rights of the individual concerned to access of his/her personal data are restricted in the following cases:

- 1) processing of personal data, including personal data obtained in the course of criminal investigation or security service operations, for the state defense or law enforcement purposes;
- 2) processing of personal data by criminal investigation agencies due to the arrest of the individual concerned as a suspect, indictment made against the individual concerned or putting him/her under restraint, except for cases when the suspect or the accused has the right to get acquainted with respective personal data in pursuance of the criminal procedure legislation of the Russian Federation; and
- 3) providing personal data infringes the constitutional rights and liberties of third persons.



**Section 15. Personal Rights During the Processing of Personal Data for Promotional or Marketing Purposes**

1. Personal data processing for the promotion of goods, works or services by means of direct contacts with potential customers via telecommunication means as well as in the course of political campaigns are subject to the prior consent of the individual concerned. Such personal data processing shall be declared performed without prior consent of the individual concerned unless the operator gives proof of obtaining such consent.

2. Upon the request of the individual concerned, the operator shall promptly discontinue his/her personal data processing for the purposes described in part 1 of this Section.

**Section 16. Rights of Individual in Cases when Decisions are made based on the Automatically Processed Personal Data**

1. It is prohibited to make decisions that entail legal consequences for the individual concerned or otherwise affect his/her rights and legal interests solely on the grounds of automatically processed personal data, except in the cases envisaged by part 2 of this Section.

2. A decision which entails legal consequences for the individual concerned or otherwise affects his/her rights and legal interests may be made solely on the grounds of the automatically processed personal data if the individual's consent thereto has been obtained in writing as well as in cases described in federal laws, which should establish, *inter alia*, measures for the protection of personal rights and legal interests.

3. The operator shall clarify to the individual concerned the procedure of making decisions solely on the grounds of the automatically processed personal data, describe possible legal consequences of such decisions, give the individual concerned the option to contest such decision and explain how the individual's rights and legal interests can be defended.

4. The operator shall consider the individual's objections referred to in part 3 of this Section within seven business days and shall notify the individual on the decision made in this respect.

**Section 17. Right to Contest Operator's Actions or Failure to Act**

1. If the individual concerned is of the opinion that the operator is processing his/her personal data in violation of this Federal Law or otherwise infringes his/her rights and liberties, the individual is entitled to contest the operator's actions or failure to act with the authorized protection body or in court.

2. The individual concerned has the right to protect his/her rights and legal interests, including the right to require compensation for losses and/or compensation for moral damage, in court.

**Chapter 4. Operator's Obligations**

### **Section 18. Operator's Obligations at the Time of Collection of Personal Data**

1. At the time of the collection of personal data, the operator shall, upon request of the individual concerned, provide him/her with information listed in part 4 of Section 14 of this Federal Law.

2. If the obligation to provide personal data is established by a federal law, the operator shall explain to the individual concerned the consequences of his/her refusal to provide personal data.

3. If personal data are collected from a third person (other than in cases when such personal data are collected under a federal law or when they are open to public use), before processing such personal data, the operator shall provide the following information to the individual concerned:

- 1) name (surname, given name and patronymic) and address of the operator or its representative;
- 2) purpose of personal data processing and legal grounds thereof;
- 3) supposed recipients of personal data; and
- 4) rights of the individual concerned established by this Federal Law.

### **Section 19. Protective Measures While Processing Personal Data**

1. When processing personal data the operator should take all reasonable organizational and technical measures (in particular, use encryption/cryptographic devices) in order to prevent unauthorized/inadvertent access to personal data, their destruction, alteration, blocking, copying, distribution or performance of other illegitimate acts.

2. The Government of the Russian Federation shall adopt regulations on personal data protection to apply to respective databases and shall elaborate the requirements for tangible mediums of biometric personal data and with respect to storage of such data by means other than in databases.

3. Control of and supervision over compliance with requirements established by the Government of the Russian Federation as set forth by part 2 of this Section shall be carried out by an authorized security agency of the executive power and the federal security service within the scope of their competence. When performing their functions, the state bodies are not allowed get acquainted with personal data contained in databases.

4. Use and storage of biometric personal data other than in databases is allowed only on the condition that the hardware and software used ensure efficient protection of personal data from unauthorized or inadvertent access, destruction, altering, blocking, copying or distribution.

### **Section 20. Operator's Obligations to Process Inquiries of the Individual Concerned, Legal Representatives or the Authorized Body**

1. The operator shall, subject to procedures described in Section 14 of this Federal Law, inform the individual concerned or his/her legal representative of whether the operator holds the respective personal data and shall grant access to such personal data upon oral request of the

individual concerned or his/her legal representative within ten business days of receiving the written inquiry of the individual concerned or his/her legal representative.

2. If the operator refuses to inform the individual concerned or his/her legal representative whether it holds personal data or refuses to grant access to the same, the operator shall give a written notice, which shall include the reference to part 5 of Section 14 of this Federal Law or another federal law, of the grounds on which the access to personal data has been denied. The notice shall be given within seven business days of the receipt of the inquiry from the individual concerned or his/her legal representative.

3. The operator shall allow the individual concerned or his/her legal representative to have access to his/her personal data free of charge. Further, the operator shall correct, destroy or block personal data upon the request of the individual concerned or his/her legal representative if they prove that the respective personal data collected and processed by the operator are incomplete, obsolete, incorrect, were obtained illegally or are irrelevant for the intended purposes. The operator shall then inform the individual concerned or his/her authorized representatives as well as persons to whom personal data of the said individual have been transferred about the changes made.

4. The operator shall provide the authorized protection body with information required for such authorized protection body's effective performance of its duties within seven business days of receipt of the respective request.

#### **Section 21. Operator's Obligations to Cure Breaches of Personal Data Processing and to Correct, Block or Destroy Personal Data**

1. If any irrelevant personal data are disclosed or any illegitimate actions of the operator become known, the operator shall, after the receipt of the oral or written request of the individual concerned, his/her legal representative or the authorized protection body, promptly block the personal data of the individual concerned for the entire period while the personal data are being verified.

2. If the personal data prove to be irrelevant, based on documents provided by the individual concerned, his/her legal representative or the authorized protection body or other documents, the operator shall correct personal data and deploy such data.

3. If the operator's illegitimate actions become known, the operator shall cure the breach within three business days of such disclosure. If the breach cannot be cured within three days of the disclosure, the operator shall destroy personal data. The operator shall notify the individual concerned or his/her legal representative about the corrections made or destruction of personal data. If the respective demand was made by the authorized protection body, the operator shall notify the authorized protection body as well.

4. If the goals for which personal data were processed are achieved, the operator shall promptly discontinue processing and destroy personal data within three business days from such date unless otherwise provided by federal laws. The operator shall notify the individual concerned or his/her legal representative and, if the respective demand was made by the authorized protection body, shall notify such authorized protection body as well.

5. If the individual concerned revokes his/her consent to personal data processing, the

operator shall discontinue data processing and destroy personal data within three business days of such revocation, unless otherwise agreed upon by the operator and the individual concerned. The operator shall notify the individual concerned that his/her personal data have been destroyed.

## **Section 22.** Notice about Personal Data Processing

1. Before the operator starts processing personal data, it shall notify the authorized protection body of its intent to process personal data except for in cases envisaged in part 2 of this Section.

2. The operator is entitled to process personal data without first notifying the authorized protection body in the following cases:

- 1) the operator processes its employees' personal data;
- 2) personal data were obtained pursuant to an agreement between the operator and the individual concerned, provided that such data shall not be distributed or transferred to third persons without the consent of the individual concerned and shall be used by the operator solely for the purposes of performance of the agreement or entering into new agreements with the individual concerned in the future;
- 3) personal data of members of a non-governmental or religious organization are processed by such organization in compliance with the laws of the Russian Federation for the purposes established by its constituent documents, provided that personal data shall not be distributed without the written consent of the individual concerned;
- 4) personal data are open to general use;
- 5) personal data include only the full names (surname, given name and patronymic) of individuals;
- 6) personal data are processed for granting one-time access to the operator's premises or for similar purposes;
- 7) processing of personal data contained in databases that pursuant to federal laws have the status of federal electronic databases as well as in state databases created for the defense and security purposes; and
- 8) personal data are processed manually pursuant to the federal laws or regulations of the Russian Federation, which shall establish measures aimed at the protection of processed personal data and observance of personal rights.

3. The notice referred to in part 1 of this Section shall be made in writing and signed by an authorized representative or, if being sent by e-mail, signed electronically in accordance with the laws of the Russian Federation. The notice shall contain the following data:

- 1) name (surname, given name, patronymic) and address of the operator;
- 2) purpose of personal data processing;
- 3) categories of personal data;
- 4) categories of individuals whose personal data are to be processed;
- 5) legal grounds for personal data processing;

6) actions to be made with respect to personal data and general description of methods used by the operator for personal data processing;

7) description of the protective measures to be taken by the operator in the course of personal data processing;

8) date when the personal data processing will begin; and

9) term of personal data processing or conditions for discontinuation of personal data processing.

4. The authorized protection body shall include data referred to in part 3 of this Section in the register of operators and shall register the date of submission of the notice therein within thirty days as of the receipt of the operator's notice. Data in the register of operators, except for information on protective measures taken by the operator, shall be available to the general public.

5. The operator shall not become liable for any costs incurred by the authorized protection body for examination of the operator's notice or inclusion of the respective data in the register of operators.

6. If the data provided by the operator in pursuance of part 3 of this Section are incomplete or irrelevant, the authorized protection body may require the operator to provide the missing or correct data before including the same in the register of operators.

7. If the data referred to in part 3 of this Section have changed, the operator shall notify the authorized protection body within ten business days of the occurrence of such changes.

## **Chapter 5. Control and Supervision over Personal Data Processing; Liability for Breach of this Federal Law**

### **Section 23. Authorized Body in the Sphere of Personal Data Protection**

1. The authorized body in the sphere of personal data protection (hereinafter, "authorized protection body"), that shall be responsible for supervising to ensure that respective activities are carried out in compliance with this Federal Law, shall be a federal agency of executive power in the sphere of information technologies and communications.

2. The authorized protection body will consider inquiries of the individuals concerned regarding compliance of personal data contents and methods of processing with declared purposes and makes relevant decisions.

3. The authorized protection body has the right:

1) to request from legal entities and individuals information necessary for performance by the authorized protection body to perform its duties and obtain such information free of charge;

2) to verify data contained in the operator's notice on personal data processing or to employ other state agencies to do the same within the scope of their competence;

3) to require the operator to correct, block or destroy irrelevant or illegally

obtained personal data;

4) to take measures to suspend or discontinue personal data processing in a way permitted by laws of the Russian Federation, if such personal data are processed without due regard for requirements of this Federal Law;

5) to file lawsuits in order to protect personal rights and to represent interests of the individuals concerned in court;

6) to require the licensing authorities to suspend or revoke the operator's license in a manner prescribed by laws of the Russian Federation, if the license was issued on condition that no personal data may be transferred to third persons without the written consent of the individual concerned;

7) to submit to the public prosecutor's office and other relevant law enforcement agencies materials for the initiation of criminal procedures due to potential breach of personal rights;

8) to propose that the Government of the Russian Federation make amendments to laws and normative acts which regulate personal data protection issues; and

9) to impose administrative liability for breaches of this Federal Law.

4. The authorized protection body shall keep personal data which become known to it in the course of performance of its duties strictly confidential.

5. The authorized protection body shall:

1) procure the protection of personal rights in accordance with this Federal Law and other federal laws;

2) consider complaints and inquiries of individuals and legal entities on matters related to personal data processing and make respective decisions within the scope of its competence;

3) hold the register of operators;

4) take measures for better protection of personal rights;

5) take measures, in a manner established by laws of the Russian Federation, for suspension or discontinuation of personal data processing upon request of an authorized agency of the federal security service;

6) inform, upon request, state agencies and individuals concerned about the state of personal data protection;

7) perform other duties as established by the laws of the Russian Federation.

6. Decisions of the authorized protection body may be contested in court.

7. The authorized protection body shall report on its activities to the President of the Russian Federation, the Government of the Russian Federation and the Federal Council of the Russian Federation annually. Annual reports shall also be published in the media.

8. The authorized protection body shall be financed out of the federal budget.

9. An advisory council shall act in the authorized protection body on a voluntary basis.

The procedure for forming and operating the advisory council shall be set forth by the authorized protection body.

**Section 24.** Liability for Breach of this Federal Law

Persons found guilty in breach of this Federal Law shall bear civil, criminal, administrative, disciplinary and other liability as prescribed by the laws of the Russian Federation.

**Chapter 6. Final Provisions**

**Section 25.** Final Provisions

1. This Federal Law takes effect upon the expiration of one hundred and eighty days since being officially published.

2. When this Federal Law takes effect, personal data included in databases before its enactment shall be processed in compliance with this Federal Law.

3. Personal data databases created before the enactment of this Federal Law shall be brought into accord with this Federal Law by 1 January 2010 at the latest.

4. Operators that started processing personal data before the enactment of this Federal Law that are going to process such data further shall notify the authorized protection body as prescribed by part 3 of Section 22 of this Federal Law by 1 January 2008 at the latest, save as in cases envisaged in part 2 of Section 22 of this Federal Law.

President of the Russian  
Federation

Vladimir Putin

Moscow, Kremlin  
27 July 2006  
N 152-FZ