Comparing privacy laws:

GDPR v. Russian Law on Personal Data

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

GORODISSKY

About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Gorodissky & Partners was founded in 1959 and it is one of the largest and prestigious national law firms in Russia and Ukraine. The firm has outstanding legal expertise in the areas of IP and TMT. It provides domestic and foreign clients with comprehensive and professional legal services in respect of all IP and intangible assets, including patents, copyrights, software, know-how and trademarks, among others. Gorodissky & Partners also has a dedicated team of lawyers dealing with TMT-sector, who have a wide and practical experience of advising clients in the fields of IT and outsourcing, media and advertising, Internet and e-commerce, data protection and privacy, data audits and compliance, data management and transactions, litigation, enforcement and prevention of data breaches. Its clients include major Russian and global companies, SMEs, FMCGs, pharmaceutical and industrial organizations, financial institutions and banks, JVs and start-ups, online game corporations and e-trade businesses. The firm is headquartered in Moscow, with 12 additional branch offices in Russia and one in Ukraine.

Contributors

OneTrust DataGuidance™
Alexis Kateifides, Angela Potter, Holly Highams, Christopher Campbell, Tooba Kazmi, Angus Young, Claudia Strugnell, Victoria Ashcroft

Gorodissky & Partners
Sergey Medvedev, PhD, LLM, Stanislav Rumyantsev, PhD, CIPP/E

Image production credits:

Cover/p.5/p.51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents

Introduction 5

1. Scope
1.1. Personal scope 7
1.2. Territorial scope 9
1.3. Material scope 10

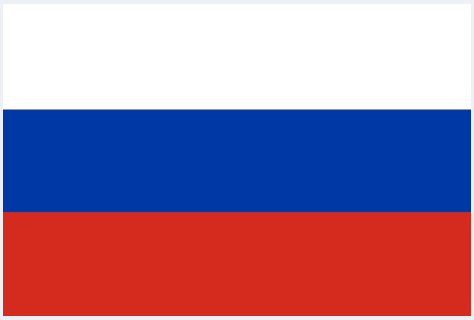
2. Key definitions
2.1. Personal data 12
2.2. Pseudonymisation 14
2.3. Controller and processors 15
2.4. Children 17
2.5. Research 18

3. Legal basis 19

4. Controller and processor obligations
4.1. Data transfers 21
4.2. Data processing records 26
4.3. Data protection impact assessment 27
4.4. Data protection officer appointment 28
4.5. Data security and data breaches 30
4.6. Internal policies 32
4.7. Notification of processing 33

5. Individuals' rights
5.1. Right to erasure 34
5.2. Right to be informed 35
5.3. Right to object 36
5.4. Right to access 37
5.5. Right not to be subject to automated decision-making 39
5.6. Right to data portability 40

6. Enforcement
6.1. Monetary penalties 41
6.2. Supervisory authority 43
6.3. Other remedies 45



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the Federal Law of 27 July 2006 No. 152-FZ on Personal Data ('the Law on Personal Data') both aim to guarantee protection for individuals' personal data and apply to organisations that collect, use, or share such data.

In particular, both laws share similar provisions, for example, in relation to legal basis for processing. Under both the GDPR and the Law on Personal Data, data processing shall only be lawful if the data subject has given consent to processing, where processing is necessary for the performance of a contract, as well as for compliance with a legal obligation, among other things. In addition, the GDPR and the Law on Personal Data both outline fairly consistent cross-border data transfers obligations, providing that such transfers only take place to countries ensuring an adequate level of protection. Moreover, both laws are fairly consistent in relation to the appointment of a data protection officer ('DPO').

However, the Law on Personal Data differs from the GDPR in some significant ways, particularly with regard to definitions, controller and processor obligations, and territorial scope. Where the GDPR provides for the definition of both data controller and processor, the Law on Personal Data only refers to operators. The GDPR also grants special protection to children's personal data and sets out the minimum age of consent with regard to information society services, as well as appropriate measures for providing information to children. The Law on Personal Data does not grant special protection to children's personal data or outline similar specific requirements on the same.

Unlike the GDPR, the Law on Personal Data does not provide particular provisions on territorial scope. The GDPR outlines specific provisions on extraterritorial scope and applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services or the monitoring of behaviour.

The GDPR and the Law on Personal Data also differ greatly in terms of penalties, both financial and otherwise. The GDPR provides significantly larger financial penalties, of up to €20 million or 4% of global turnover, compared to those provided by the Code of Administrative Offences of the Russian Federation of 30 December 2001 No. 195-FZ ('the Code of Administrative Offences'), in which the maximum single administrative fine for violation of the Law on Personal Data is RUB 18 million (approx. €260,000). In addition, unlike the GDPR, the Law on Personal Data establishes that DPOs may incur administrative liability for non-compliance with the Law on Personal Data.

This guide aims to assist organisations in understanding and comparing the relevant provisions of the GDPR and the Law on Personal Data, to ensure compliance with both pieces of legislation.

Structure and overview of the Guide

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the Law on Personal Data.

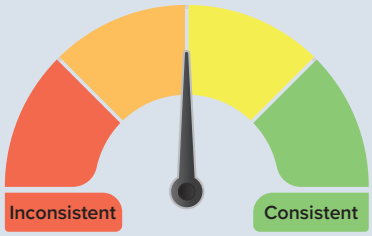
Key for giving the consistency rate

Consistent: The GDPR and Law on Personal Data bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and Law on Personal Data bear a high degree of similarity in the rationale, core, and the scope of the provision considered; however, the details governing its application differ.

Fairly inconsistent: The GDPR and Law on Personal Data bear several differences with regard to scope and application of the provision considered, however its rationale and core presents some similarities.

Inconsistent: The GDPR and Law on Personal Data bear a high degree of difference with regard to the rationale, core, scope and application of the provision considered.



Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope

The GDPR applies to data controllers and data processors, who may be businesses, public bodies, institutions as well as not for profit organisations, whilst the Law on Personal Data applies to 'operators' that are defined as state agencies, municipal authorities, legal entities or individuals that organise and/or carry out (alone or jointly with other persons) the processing of personal data and determine the purposes of data processing, the content of personal data, and the actions (operations) related to personal data.

Both pieces of legislation protect living individuals with regard to the use of their personal data. The GDPR provides that individuals are protected regardless of their nationality and/or residency, while the Law on Personal Data does not specifically outline this issue.

GDPR	Law on Personal Data
Articles 3, 4(1) Recitals 2, 14, 22-25	Articles 1, 2, 3, 6, 9

Similarities

GDPR	Law on Personal Data
The GDPR **only protects living individuals**. Legal persons' personal data is not covered by the GDPR.	The Law on Personal Data **protects the rights and freedoms of individuals** in the processing of personal data, including the protection of the rights to integrity of privacy, personal and family secrets. Data processing must be legal and fair. Furthermore, the Law on Personal Data does not cover legal persons' personal data, and it is expressly stated that personal data must relate to a physical person (data subject).
The GDPR applies to businesses, public bodies, institutions as well as not for profit businesses.	The Law on Personal Data governs the processing of personal data carried out by federal government bodies, state authorities, legal entities and individual persons using automated means, including information and telecommunication networks, or without the use of such means to the extent set forth by the law.

Differences

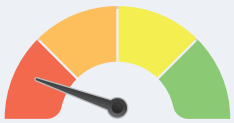
GDPR	Law on Personal Data
Article 4(1) of the GDPR **clarifies** that a data subject is '**an identified or identifiable natural person**.'	The Law on Personal Data does **not explicitly define** a data subject, however Article 3(1) of the Law on Personal Data outlines that personal data is 'any information relating to directly or indirectly identified or identifiable physical person (data subject).'
The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'	The Law on Personal Data does **not** outline requirements on nationality or place of residence in relation to the processing of personal data of data subjects.

GDPR	Law on Personal Data

Differences (cont'd)

The GDPR applies to a '**data controller**' that is defined by the fact that it establishes the **means** and **purposes of the processing.**	The Law on Personal Data does **not provide the definition of 'data controller,'** but instead applies the concept of an 'operator' which is defined as a state agency, municipal authority, legal entity or individual who independently or, in cooperation with other entities, organises, and/or processes personal data, as well as determines the purpose and scope of data processing, and the actions (operations) related to personal data.
The GDPR sets several obligations that apply to '**processors**' which are entities that process personal data **on behalf of controllers**.	The Law on Personal Data **does not provide the definition of 'processor,'** but instead applies to the concept of 'a party that process personal data under operator's instruction.' Such parties may perform data processing, subject to data subject's consent, on the basis of the corresponding agreement (including state contract) or by operation of the special state or municipal act.
The GDPR **does not protect the personal data of deceased individuals**, and is left to Member States to regulate.	Under Article 9(7) of the Law on Personal Data **if a data subject dies, the consent to the processing of their personal data will be given by the heirs** of the data subject, unless the data subject gave such consent while they were alive.

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE
GORODISSKY



Inconsistent

1.2. Territorial scope

Unlike the GDPR, the Law on Personal Data does not provide specific provisions on exterritorial scope. The GDPR applies, in particular, to the activities of data controllers or processors 'established' in the EU, irrespective of whether data processing takes place within the EU or not. In addition, the GDPR applies to the processing of personal data of EU data subjects by a controller or processor not established in the EU, if they offer goods or services to, or monitor the behaviour of, individuals within the EU.

Although not specifically addressed in the Law on Personal Data, according to the Federal Service for the Supervision of Communications, Information Technology and Mass Communications ('Roskomnadzor'), the Law on Personal Data shall apply to legal entities processing the personal data of Russian data subjects, including the offices of non-Russian companies, if such offices are physically located in Russia and process personal data in Russia.

GDPR	Law on Personal Data
Articles 3, 4(1) Recitals 2, 14, 22-25	Article 1(1)

Similarities

GDPR	Law on Personal Data
Not applicable.	Not applicable.

Differences

GDPR	Law on Personal Data
In relation to **exterritorial scope**, the GDPR applies to organisations that do not have any presence in the EU, but that offer goods, services or monitor the behaviour of individuals in the EU.	The Law on Personal Data does **not** specifically outline or provide provisions on territorial scope.
The GDPR **applies** to organisations that have presence in the EU. In particular, under Article 3, the GDPR applies to entities or organisations established in the EU, notably entities that have an '**establishment**' in the EU or if processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not.	The Law on Personal Data does **not** directly address this issue. Although not specifically addressed in the Law on Personal Data, according to Roskomnadzor, the Law on Personal Data shall apply to legal entities processing the personal data of Russian data subjects, including the offices of non-Russian companies, if such offices are physically located in Russia and process personal data in Russia.

1.3. Material scope

The GDPR and the Law on Personal Data apply to the processing of personal data by automated means, however the GDPR specifies non-automated means of processing can include those systems which form part of a filing system, whilst the Law on Personal Data applies to processing of personal data through the use of automated means, including via an informational-telecommunication network, or without automated means if the nature of the manual processing is similar to automated data processing, i.e. allows an individual to search for personal data located in card catalogues or archives with the use of any algorithm.

Both the GDPR and the Law on Personal Data apply to personal data defined as any information directly or indirectly relating to a natural person. Both pieces of legislation apply to the processing of personal data through operations that are similar.

In addition, the GDPR and the Law on Personal Data define and provide requirements for processing special categories of personal data. Neither the GDPR nor the Law on Personal Data apply to the processing of personal data for personal or household purposes, provided that the rights of data subjects are not violated.

GDPR	Law on Personal Data
Articles 2, 4(1), 4(2), 4(5), 4(6) Recitals 15-21, 26	Articles 1, 3(1), 3(3), 3(8), 6(2), 10

Similarities

The GDPR applies to personal data which is defined as any information that **directly or indirectly relates to an identified or identifiable individual**.

The Law on Personal Data applies to personal data, meaning any information **directly or indirectly relating to an identified or identifiable natural person** (data subject).

The GDPR applies to the **'processing' of personal data**. The definition of 'processing' covers 'any operation' performed on personal data 'such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

The Law on Personal Data applies to the **processing of personal data**, and defines it as 'any action (operation) or a set of actions (operations) realised by means of automation facilities or without such facilities as involving personal data, including the collection, recording, systematising, accumulating, storing, updating (renewing, altering), retrieving, using, transferring (disseminating, providing and accessing), depersonalising, blocking, deleting and destroying of personal data.'

The GDPR defines **'special categories of personal data'** as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric

The Law on Personal Data defines **'special categories of personal data'** as data 'concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, health, or sex life and provides specific requirements for its processing.'

GDPR	Law on Personal Data

Similarities (cont'd)

data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. and provides specific requirements for its processing.'	
The GDPR provides the definition of '**pseudonymisation**' as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'	The Law on Personal Data provides for the '**depersonalisation**' of personal data. Article 3(9) of the Law on Personal Data defines this as 'actions performed on personal data that make it impossible to determine the identity of the subject without the use of information in addition to such anonymised data.'
The GDPR excludes from its application the processing of personal data by individuals for purely personal or **household purposes**. This is data processing that has 'no connection to a professional or commercial activity.'	The Law on Personal Data does not apply to personal data being processed by individuals exclusively for **personal and family needs**, provided there is no violation of rights of the data subjects.

Differences

Anonymous data is outside the scope of the GDPR. Anonymous data is information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The Law on Personal Data does **not** contain similar rules on anonymisation.
The GDPR applies to the processing of personal data wholly or partly by **automated means** and to processing other than by automated means which form part of a filing system.	The Law on Personal Data applies to processing both **automatically and manually**, provided that the manual processing is, by its nature, similar to the automatic processing.

2. Key definitions

2.1. Personal data

Fairly inconsistent

'Personal data' is broadly defined under both the GDPR and the Law on Personal Data. Both the GDPR and the Law on Personal Data define special categories of personal data. The Law on Personal Data provides for a separate definition of 'biometric personal data' which includes physiological and biological features of a person.

Whilst the GDPR provides for identification through online identifiers, the Law on Personal Data does not address this form of identification.

The Law on Personal Data defines 'depersonalisation' of personal data whilst the GDPR provides for the pseudonymisation of personal data.

GDPR Articles 4(1), 4(14), 9 Recitals 26-30	Law on Personal Data Articles 3(1), 3(3), 3(9), 5(7), 10(1), 11(1)

Similarities

'Personal data' is defined as '**any information relating to an identified or identifiable natural person' ('data subject')**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Personal data' is defined as **any information relating directly or indirectly to an identified or identifiable physical person** ('subject of personal data'). The Law on Personal Data does not distinguish between direct and indirect personal data.

The GDPR defines **special categories of personal data** (or 'sensitive data') as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'

The Law on Personal Data defines **special categories of personal data** as data concerning race, nationality, political views, religious or philosophical beliefs, health status or an individual's intimate life, and convictions.

The GDPR defines '**biometric data**' as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural

The Law on Personal Data defines '**biometric data**' as 'information concerning the physiological and biological characteristics of an individual from which they may be

GDPR	Law on Personal Data

Similarities (cont'd)

person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.'	identified (biometric personal data) and that is used by a controller to establish the identity of that data subject may be processed only subject to the written consent of the data subject, with the exception of the cases stipulated in 11(2).'

Differences

The GDPR explains in its recitals that in order to determine whether a person is identifiable, 'account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person' to identify the individual directly or indirectly. In its recitals, the GDPR specifies that **online identifiers** may be considered as personal data, such as IP addresses, cookie identifiers, and radio frequency identification tags.	The Law on Personal Data does **not** address identification through online identifiers.
The GDPR does not apply to anonymised data, where the data can no longer identify the data subject.	The Law on Personal Data does not specifically address the application to anonymised data.

2.2. Pseudonymisation

The concept of pseudonymisation is similar under the GDPR and the Law on Personal Data in that it is the processing of personal data in a manner that make it impossible to determine the identity of the data subject without the use of additional information. However, the Law on Personal Data provides the definition of 'depersonalisation' for the concept.

The GDPR introduces pseudonymisation as a data security measure (Article 32), while the Law on Personal Data provides for the depersonalisation as an alternative to the destruction of data.

GDPR	Law on Personal Data
Articles 4(5), 11 Recitals 26, 28	Articles 3(3), 3(9)

Similarities

'**Pseudonymisation**' is defined under the GDPR as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'

The definition of '**depersonalisation**' is provided under Article 3(9) of the Law on Personal Data as actions performed on personal data that make it impossible to determine the identity of the data subject without the use of additional information.

Differences

Anonymous data is specifically outside the scope of the GDPR. Anonymous data is information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The Law on Personal Data does **not** specifically address the application to anonymised data.

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE
GORODISSKY

2.3. Controllers and processors

Fairly inconsistent

Unlike the GDPR the concept of 'data controller' and 'data processor' are not provided in the Law on Personal Data. Instead, the Law on Personal Data defines an operator as 'a state body, municipal body, legal or natural person, alone or together with other persons organisation and (or) processing personal data, as well as defining processing purposes of personal data, the scope of personal data to be processed, actions (operations) performed with personal data.' Operators can appoint a third-party responsible for organising the processing of personal data provided that the data subject has provided consent.

The GDPR establishes detailed requirements in relation to the processing of personal data by data controllers and data processors. The Law on Personal Data establishes similar requirements for operators, as well as for third parties processing personal data under the instruction of the operator.

GDPR	Law on Personal Data
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 90, 93	Articles 3(2), 5(6), 6, 18.1, 19, 21

Similarities

Data controllers **must comply with the purpose limitation and accuracy principles** and **rectify** the data subject's **personal data if it is inaccurate** or **incomplete**.

Operators **must not process personal data outside of the specific, predetermined and legitimate purposes** of collection and operators must take necessary measures to **remove or clarify incomplete or inaccurate personal data**.

Data controllers must **implement technical and organisational security measures**.

Operators must **implement organisational and technical, as well as legal, security measures when** processing personal data to ensure security of personal data.

Differences

Under the GDPR, a **data controller** is a natural or legal person, public authority, agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others.

There is **no concept of data controller** under the Law on Personal Data. An **operator** is a state body, municipal body, legal or natural person, alone or together with other persons or organisations processing personal data, as well as defining processing purposes of personal data, the scope of personal data to be processed, and actions (operations) performed with personal data (Article 3(2)).

A **data processor** is a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**.

There is **no definition of a data processor** under the Law on Personal Data. However, the Law on Personal Data does provide that an operator can appoint

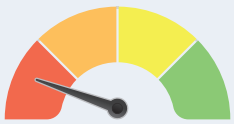
GDPR	Law on Personal Data

Differences (cont'd)

	another person, responsible for organising the processing of personal data under the instruction of the operator on the basis of a contract, including a state or municipal contract, or by operation of the special state or municipal act, with the consent of the data subject. Such a person processing personal data, on behalf of an operator, must comply with the principles and rules for processing of personal data established in the Law on Personal Data.
Other obligations imposed on data processors include the requirement to **keep a record of data processing activities**; to **implement appropriate technical and organisational measures**: processors must **ensure security** for processing data, which could include encryption or pseudonymisation practices; assist the controller to **undertake data protection impact assessments** ('DPIA') prior to the processing; designate a DPO when required by the law, including where the processor processes personal data on a larger scale; processors are required to notify the controller of any breach without undue delay after becoming aware of a breach.	Other **obligations imposed on operators and the third parties processing personal data under the instruction of operators** include the requirement to **ensure** the **confidentiality and security** of the personal data processed and comply with the rules of processing personal data provided for by the Law on Personal Data, in particular, those outlined in Article 19. **Recording, systemisation, accumulation**, **storage**, **clarification** and **extraction** of Russian citizens' personal data on the Internet must take place using databases located in the Russian territory.

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE
GORODISSKY

2.4. Children



Inconsistent

The GDPR grants special protection to children's personal data. It provides specific provisions, including, by setting the minimum age of consent with regard to information society services, as well as appropriate measures when providing information to children, among other things.

The Law on Personal Data does not grant special protection to children's personal data or outline specific requirements on the same.

GDPR	Law on Personal Data
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Article 9(6)

Similarities

GDPR	Law on Personal Data
The GDPR does **not** define 'child' nor 'children.'	The Law on Personal Data does **not** define 'child' nor 'children.'

Differences

GDPR	Law on Personal Data
The GDPR considers children as '**vulnerable natural persons**' that merit specific protection with regard to their personal data. Specific protection should be given when children's personal data is used for marketing or collected for information society services offered directly to a child.	The Law on Personal Data does **not** outline the specific protections that should be given to children's personal data.
Where the processing is based on consent, consent of a parent or guardian is required for providing information society services to a **child below the age of 16**. EU Member States can lower the age limit, which, in any case, cannot be lower than 13. Data controllers are required to make reasonable efforts to verify that consent is given or authorised by a parent or guardian.	The Law on Personal Data does **not** specifically address the age of minors.
The GDPR does not provide for any exception for a controller that is **not aware that it provides services to a child**. It is not clear whether the consent requirement will apply if the child's personal data is unintentionally collected online. 'Fostering healthy children' is not an exemption for not obtaining consent.	The Law on Personal Data does **not** outline any exceptions for a controller that is not aware that it provides services to a child.
When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.	There are **no** specific rules for privacy notices aimed at children.

2.5. Research

Fairly inconsistent

Both the GDPR and the Law on Personal Data address the processing of personal data for research purposes. The GDPR has specific provisions regarding the processing of personal data for 'historical or scientific research,' as well as for 'statistical purposes.' Similarly, the Law on Personal Data mentions the processing of personal data for 'statistical' or 'other research purposes' with reference to the professional journalistic, scientific, literary or other creative activities.

GDPR	Law on Personal Data
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 89 Recitals 33, 159, 160, 161	Articles 6(9), 15, 18(4)

Similarities

Under the GDPR, the processing of personal data for research purposes is subject to some **specific rules** e.g. with regard to the purpose limitation principle.

Under the Law on Personal Data, the processing of personal data for the purposes of statistical or other research purposes is generally permitted, on the **condition** that the data is depersonalised; the only exceptions mentioned are for the purposes of promoting goods and services on the market, and for the purpose of political campaigning, which may be done under the preliminary data subject consent.

Differences

Processing of **special categories** of personal data is permitted if it is necessary for **scientific or historical research purposes or statistical purposes**, subject to the purpose limitation principle, and certain safeguards being implemented.

There is **no** exception in the Law on Personal Data for processing special categories of personal data for research purposes or statistical purposes.

Under the GDPR, the data subject's **right to erasure does not apply to** the extent that **processing is necessary for research purposes**.

There is **no** explicit mention in the Law on Personal Data regarding requesting the erasure of data that is being processed for research purposes.

3. Legal basis

Both the GDPR and the Law on Personal Data mention several legal grounds for the lawfulness of processing personal data. A lawful basis for processing personal data may consist of at least one of those legal grounds and will vary per personal data processing activity, scope and purpose.

GDPR	Law on Personal Data
Articles 5, 6, 7, 9, 85, 89 Recitals 32, 39-50, 153	Article 6

Similarities

Under Article 6 (1)(a) of the GDPR, **data processing shall be lawful** to the extent that the data subject has given **consent** to the processing of his or her personal data for one or more specific purpose; for **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; for compliance with **a legal obligation** to which the controller is subject (Article 6(1)(c) of the GDPR); in order to protect the **vital interests** of the data subject or of another natural person (Article 6 (1)(d) of the GDPR); for the performance of a task carried out in the **public interest** or in the exercise of **official authority** vested in the controller; and for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Under Article 6 (1)(1) of the Law on Personal Data, **data processing shall be lawful** if it is made, *inter alia*, under the **consent** of the data subject for data processing; for the **performance of a contract** to which the data subject is party, or the beneficiary, or guarantor, as well as for conclusion of the contract under the initiative of data subject or contract under which the data subject will be a beneficiary or guarantor; the extent it is necessary for the performance of purposes set forth by the international treaty of the Russian Federation or law, for exercising and performing **legal functions, authorities and obligations** on the operator (Article 6 (1)(2) of the Law on Personal Data); and for the protection of life, health and other **vital interests** of the data subject, provided that the receipt of data subject's consent is impossible (Article 6 (1)(6) of the Law on Personal Data); for performance of **official authorities** of federal agencies, state bodies, execution bodies and municipal bodies; and it is necessary for the exercise of rights and **legitimate interests** of the operator and third parties, including in cases set forth by the laws on debt recovery, micro-financial activity, or for the achievement of public purposes, provided that rights and freedoms of data subject are not violated.

The GDPR provides exemption to the processing of special categories of personal data which is **publicly available**.

The Law on Personal Data allows the processing of personal data which has been made **publicly available** by the data subject at his/her request.

GDPR	Law on Personal Data
Differences	
The GDPR allows the processing of **special categories** of personal data where the processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.	The Law on Personal Data allows the processing of **personal data** for certain judicial and enforcement (execution) purposes.
The GDPR outlines that processing for archiving purposes in the **public interest, scientific or historical research** purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with purpose limitation, and under Recital 153 and Article 85 that the processing of personal data for **journalistic, academic, artistic purposes or literary expression** should be subject to derogations or exemptions from certain provisions of the GDPR if necessary.	The Law on Personal Data allows the processing of personal data for the performance of **professional journalistic, media, scientific, literary or other creative activities**, provided that rights and freedoms of the data subject are not violated.
The GDPR does **not** specifically address this issue.	The Law on Personal Data allows the processing of personal data which is subject to **mandatory publication or disclosure** in accordance with the applicable law.

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE
GORODISSKY

4. Controller and processor obligations

4.1. Data transfers

Fairly consistent

According to the GDPR, the cross-border transfer of personal data may take place where either the transfer is based on an adequacy decision, the transfer is subject to appropriate safeguards, or specific derogations apply.

The Law on Personal Data provides for cross-border data transfers to countries ensuring an adequate level of protection and such transfers do not require any specific authorisation. Transfers may be prohibited or restricted in order to protect the constitutional system of Russia, ensure public security and defence, among other things. Data transfers to the rest of the world can only be performed based on derogations. Russian law does not provide any rules on appropriate safeguards, such as Standard Contractual Clauses ('SCCs') or Binding Corporate Rules ('BCRs').

GDPR	Law on Personal Data
Articles 44-49 Recitals 101-116	Articles 12, 18(5)

Similarities

The GDPR permits the transfer of personal data to an international organisation or a third country, or specific sectors or territory within that third country, which ensures an **adequate** level of protection as assessed by the European Commission.

Russian law considers all parties to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108') as the countries ensuring an **adequate** level of protection. In addition, Roskomnadzor approved a list of countries that are not party to Convention 108, but still ensure an adequate level of protection of data subject rights in the opinion of Roskomnadzor. Currently, there are 22 countries on the list including Australia, Canada, Japan, South Korea and others. Roskomnadzor must assess whether the laws and data security measures adopted by a country correspond to what is prescribed by Convention 108.

In the **absence of the adequacy decision** or appropriate safeguards, the data transfer can be grounded on several derogations, among other things:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual

The transfer of personal data to countries **not ensuring an adequate level of protection** can be grounded on one of the following conditions:

- the data subject has consented in writing, and the written consent contains a number of requisites prescribed by the Law on Personal Data;
- the transfer is necessary for the performance of a contract to which the data subject is a party;
- the transfer is necessary for protecting the constitutional system of Russia, ensuring public security and defence,

Similarities (cont'd)

measures taken at the data subject's request;
- the transfer is necessary for important reasons of public interest; and
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

security and safe functioning of transport, protecting interests of a person, society and state with a view to unlawful intrusions into the transportation system (all such cases must be prescribed by federal laws of Russia); and
- the transfer is necessary in order to protect life, health, and other vital interests of the data subject or of other persons, where it is impossible to receive the data subject's written consent.

Differences

The GDPR establishes several criteria for the **adequacy assessment**. Among other things, the Commission should take into account the third country's accession to Convention 108 and its the Protocol (CETS No. 223) ('the Protocol'), and other international commitments the third country or international organisation has entered into.

Under the Law on Personal Data **cross-border-transfer** of personal data may be conducted to foreign states that are parties to Convention 108 and to other foreign states that provide adequate protection of the right of data subjects, among other things.

Under the GDPR, in the absence of the adequacy decision or appropriate safeguards, the data transfer can be grounded on one of the following **derogations**:
- the data transfer is necessary for the **conclusion or performance of a contract** concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for the establishment, exercise or **defence of legal claims**; or
- the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case, among other things.

The Law on Personal Data does **not** provide similar derogations.

In the absence of an adequacy decision, the cross-border transfer is possible if enforceable data subject rights and effective legal remedies for data subjects are available in the destination country, and if the controller or processor has provided **appropriate safeguards**, such as SCCs, BCRs, or an approved code of conduct, etc.

The Law on Personal Data does **not** contain any concept of appropriate safeguards applicable to the cross-border transfers such as SCCs, BCRs, or an approved code of conduct, etc.

GDPR	Law on Personal Data

Differences cont'd

The GDPR **does not** provide for any personal data localisation requirements.

According to Article 18(5) of the Law on Personal Data, **operators must ensure the recording, systemisation, accumulation, storage, clarification (update, change) and extraction of personal data of Russian Federation nationals with the use of databases located in the territory of the Russian Federation** when collecting such personal data in any manner, including via the internet. Therefore, it may be implied that it is illegal to collect the personal data of Russian citizens and store it in a non-Russian data store without the use of a database physically located in Russia. There are several exceptions from this localisation requirement (e.g. where the processing is necessary for performing a legal obligation, during litigation, and/or when conducting scientific studies). Russian nationals' personal data can be transferred across borders upon fulfilment of the localisation requirement.

GDPR Portal

The most comprehensive resource for the development and maintenance of your GDPR programme.

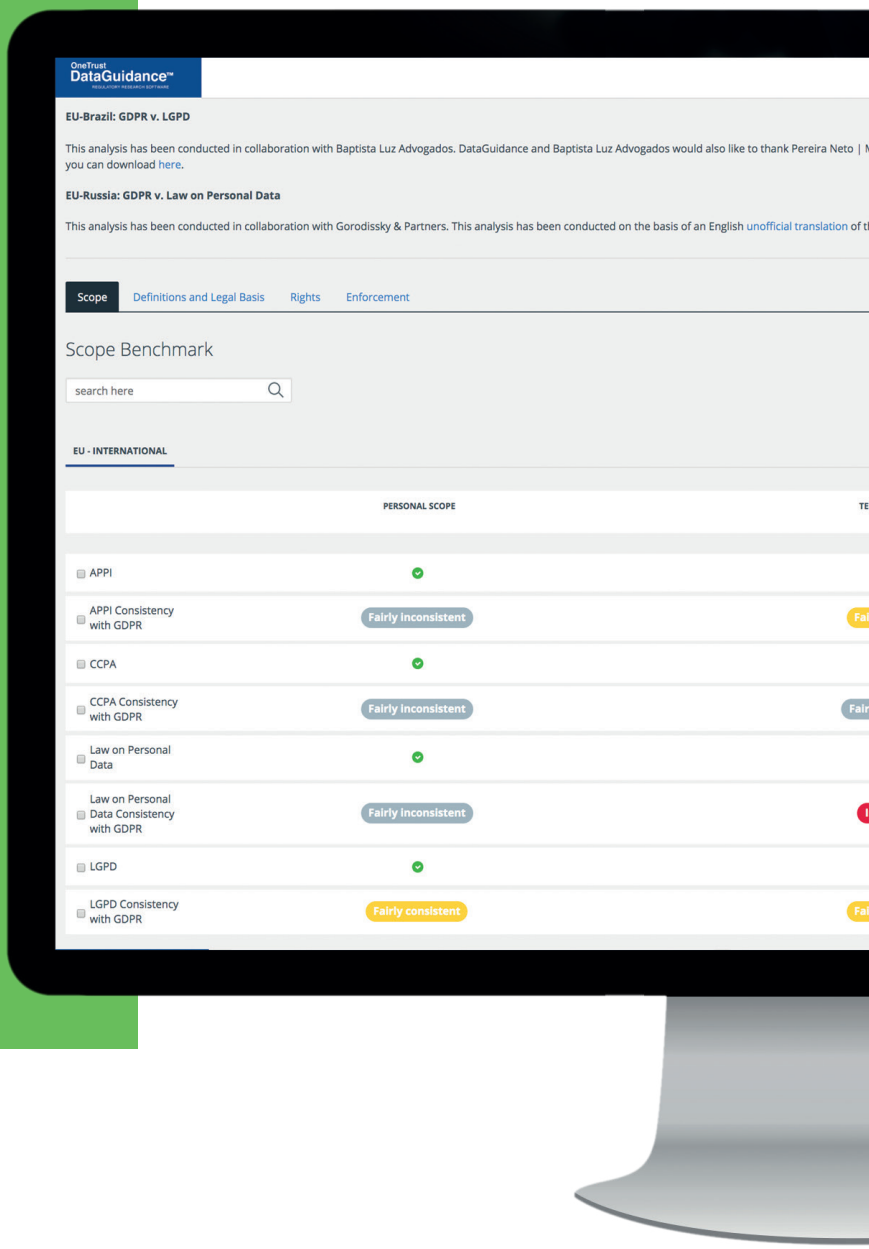
- Understand obligations and requirements across key topics and sectors
- Track developments regarding Member State implementation and regulatory guidance
- Apply expert intelligence to make business decisions
- Utilise GDPR specific checklists and templates

OneTrust
DataGu
REGULATORY

Global Regulatory

40 In-House Legal Researchers, 50

Monitor regulatory dev
and achieve glo



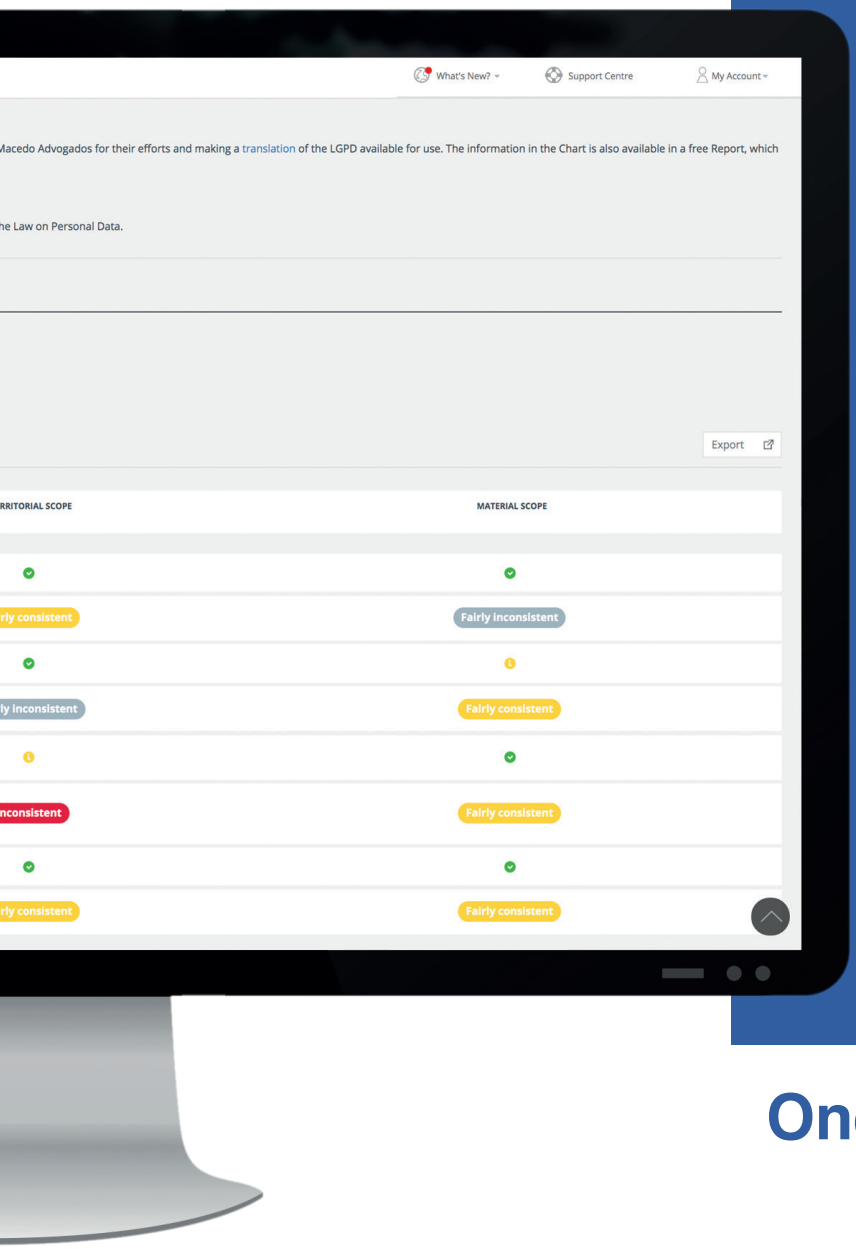
idance™

RESEARCH SOFTWARE

Research Software

00 Lawyers Across 300 Jurisdictions

elopments, mitigate risk
obal compliance.



GDPR Benchmarking

Understand and compare key provisions of the GDPR with relevant data protection law from around the globe.

- Compare requirements under the GDPR to California, Japan, Brazil, Russia and Thailand with a dedicated comparative tool
- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

www.dataguidance.com

4.2. Data processing records

The GDPR requires that the controllers and processors maintain a detailed record of their processing activities in writing, including in electronic form.

The Law on Personal Data does not contain any similar record requirements. In practice, many companies record their processing operations for demonstrating compliance and determine the content of such records by themselves.

GDPR Articles 30 Recitals 13, 39, 82	Law on Personal Data Article 18.1(3)

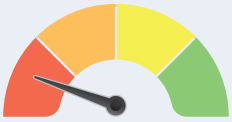
Similarities

Not applicable.	Not applicable.

Differences

Controllers and processors **must** keep records of processing activities. The GDPR establishes that **data controllers must record**: a) the name and contact details of the controller; b) the purposes of the processing; c) a description of the categories of data subjects and of the categories of personal data; d) the categories of recipients to whom the personal data will be disclosed; e) international transfers of personal data, with the identification of third countries or international organisations, and the documentation of suitable safeguards adopted; f) the estimated time limits for erasure of the categories of data; and g) a general description of the technical and organisational security measures adopted. The GDPR establishes that **data processors must record**: a) the name and contact details of the processor; b) the categories of processing conducted on behalf of each controller; c) international transfers of personal data, with the identification of third countries or international organisations, and the documentation of suitable safeguards adopted; and d) a general description of the technical and organisational security measures adopted.	Operators **may decide to** keep records of their data processing activities if they find this measure appropriate for demonstrating their compliance.
The purpose of the records is to demonstrate **compliance** with the GDPR. The records must be available to the supervisory authority (on request) so that they might serve for monitoring of processing operations.	The Law on Personal Data requires that the data operators document their **compliance**. The documents outlining such compliance must be presented on request of Roskomnadzor. Operators may decide how to document their compliance.

4.3. Data protection impact assessment



According to the GDPR, the controller must carry out a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. The GDPR establishes detailed rules on how to carry out the DPIA. The controller must consult with the supervisory authority prior to processing where the DPIA indicates that the processing would result in a high risk in the absence of risk mitigation measures.

The Law on Personal Data mentions (only once) an 'assessment of harm.' Operators may decide on whether to conduct this assessment by themselves.

GDPR Articles 35, 36 Recitals 175, 84, 89-93	Law on Personal Data Article 18.1(1)(5)

Similarities

Not applicable.	Not applicable.

Differences

The GDPR outlines, among other things, that the **DPIA** must contain an assessment of the risks to the rights and freedoms of data subjects, and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance.	There is **no** specific requirement however, the Law on Personal Data notes that the assessment by operators should contain an 'assessment of harm' that may be suffered by the data subjects in case of breaching the Law on Personal Data, and the comparison of this harm with measures envisaged to fulfil the data operator's obligations under the Law on Personal Data.
The DPIA must contain a systematic description of the **envisaged processing operations** and the processing purposes, and an assessment of the necessity and proportionality of the processing operations in relation to the purposes.	The Law on Personal Data does **not** require the assessment of these circumstances.
The GDPR prescribes that a DPIA should be conducted **prior to** the data processing.	The Law on Personal Data does **not** specifically address this issue.

4.4. Data protection officer appointment

Fairly consistent

The GDPR requires that controllers and processors appoint a DPO in some cases. The DPO is a person with expert knowledge of data protection law and practices who should assist the controller or processor to monitor internal compliance with the GDPR. Companies may appoint a single DPO for a group of companies.

The Law on Personal Data also introduces the position of the DPO whose role is close to what is prescribed by the GDPR. However, there are several important differences between DPOs under the GDPR and the Law on Personal Data.

GDPR Articles 37-39 Recital 97	Law on Personal Data Article 22.1

Similarities

The GDPR outlines the **tasks** of the DPO which include the responsibility to:

- **inform and advise** the controller or the processor and the employees who carry out processing of their obligations under the GDPR and other data protection provisions; and
- **data subjects may contact the DPO** with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR.

The Law on Personal Data outlines the **tasks** of the DPO which include the responsibility to:

- **inform** the operator's employees of the provisions of Russian personal data laws, internal privacy policies, and data protection requirements; and
- organise the receipt and consideration of requests and **inquiries of data subjects** and their representatives and/or monitor the receipt and consideration of such requests and inquiries.

The controllers and processors should communicate the **contact details** of the DPO to the supervisory authority.

The **contact details** of the DPO should be specified in the data processing notice to Roskomnadzor.

The DPO may fulfil **other tasks and perform other duties**.

Under the Law on Personal Data, the DPO may fulfil **other tasks and perform other duties**.

Under the GDPR the tasks of the DPO also include the responsibility to **monitor compliance** with the GDPR, other data protection provisions and with the data protection policies of the controller or processor and providing advice where requested as regards the DPIA and monitor its performance.

Under the Law on Personal Data the tasks of the DPO also include the responsibility to **internally monitor** the compliance of the operator and its employees with the Russian personal data laws, internal privacy policies, and data protection requirements.

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE
GORODISSKY

GDPR	Law on Personal Data

Differences

The DPO must be **appointed in the following cases**: • the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; • the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or • the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.	All operators (legal entities) must appoint the DPO **without exceptions**.
A **group** of undertakings may appoint a single DPO.	Under the Law on Personal Data, **each legal entity** must officially appoint the DPO independently of its affiliates. It is illegal to designate one person on behalf of the whole group of companies. However, several companies may use one and the same person as their DPO since the external service providers are not prohibited.
The DPO shall be designated on the basis of **professional qualities** and, in particular, expert knowledge of data protection law and practices and the ability to fulfil his/her tasks.	There are **no** specific requirements about the DPO's professional qualities, education or expert knowledge.

4.5. Data security and data breaches

Both the GDPR and the Law on Personal Data provide for a set of data security measures. While the Law on Personal Data focuses mostly on securing computer systems, the GDPR contains general requirements applicable to all kinds of the data processing.

An important difference between the Law on Personal Data and the GDPR is that the Law on Personal Data does not establish any mechanism for demonstrating compliance, such as the approved code of conduct or certification under the GDPR.

The Law on Personal Data does not contain the data breach notification requirements similar to those prescribed by the GDPR.

GDPR	Law on Personal Data
Articles 32-34 Recitals 74-77, 82, 83, 85-88	Articles 19, 21(3)

Similarities

The controller and processor must **protect personal data** from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

The operator must implement appropriate legal, organisational and technical measures to **protect personal data** against accidental or unlawful access, destruction, alteration, blockage, copy, provision, distribution, and other unlawful actions.

The controller and processor must implement technical and organisational measures to ensure appropriate **level of security**.

The operator must implement legal, technical and organisational measures to ensure one of four possible **levels of security**. The Russian Government establishes these levels with regard to the computer systems used for the personal data processing. The security measures for manual processing are not systematised according to the security levels.

The GDPR outlines the following examples of technical and organisational measures: to **ensure the ongoing confidentiality**, integrity, availability and resilience of processing systems and services; a process for **regularly testing**, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; and the ability to restore **the availability and access** to personal data in a timely manner in the event of a physical or technical incident.

The Law on Personal Data provides for the following list of technical and organisational measures: to ensure necessary **technical and organisational measures** in respect of the computer systems in order to comply with the security requirements necessary for supporting the security levels established by the Government of Russia; to **inspect the efficiency** of the implemented personal data security measures prior to putting the computer systems into operation; **determine and identify** security risks relating to the data processing in the computer systems; and the ability to restore personal data which was modified or destroyed as a result of unauthorised access.

GDPR	Law on Personal Data
Differences	
The GDPR prescribes that **pseudonymisation and encryption** of personal data is a technical and organisational measure taken to ensure data security.	The Law on Personal Data does **not** outline pseudonymisation (depersonalisation) as a data security measure.
The GDPR does not outline the use of specific information security tools, however, it outlines the necessity, where appropriate, for the adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element to demonstrate compliance with the requirements set out in Article 32(1).	Under the Law on Personal Data operators must use **information security tools** of which compliance with the information security requirements of the Russian law is duly assessed (as necessary).
The GDPR does not specifically outline the necessity to record computer data media as a personal data security measure, however, the GDPR provides that data controllers and processors should **maintain records of processing activities**.	The Law on Personal Data outlines **keeping records of all computer data media** as a technical and organisational measure to protect personal data.
Controllers and processors may adhere to an approved **code of conduct** or an approved certification mechanism to demonstrate compliance with the security requirements of the GDPR.	There are **no** codes of conduct or certification mechanisms in Russia.
The GDPR prescribes that the controller **notify data breaches** to the supervisory authority unless a breach is unlikely to result in a risk to the rights and freedoms of natural persons.	The Law on Personal Data does **not** contain similar notification requirements. If the operator received Roskomnadzor's inquiry about a possible data breach, the operator must investigate the matter and report to Roskomnadzor.
The controller must **notify** the **data subject** of a data breach without undue delay if this data breach is likely to result in a high risk to the rights and freedoms of natural persons.	The Law on Personal Data does **not** contain similar notification requirements. If the operator receive data subject's inquiry about a possible data breach, the operator must investigate the matter. When the data breach is found and eliminated, the operator must report to the data subject.

4.6. Internal policies

Fairly inconsistent

Both the GDPR and the Law on Personal Data prescribes the adoption of internal policies in order to ensure and demonstrate compliance with the legislation. In both cases, the controllers (operators) may determine the content and structure of the policy documents.

The Law on Personal Data mentions several issues to be specifically addressed in the policies and requires that the operators make their privacy policies accessible for public.

GDPR	Law on Personal Data
Article 24 Recital 78	Article 18.1

Similarities

The implementation of **data protection policies** is understood as a part of technical and organisational measures aimed at ensuring and being able to demonstrate that data processing is performed in accordance with the GDPR.

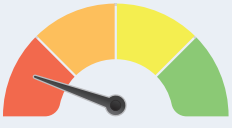
Under the Law on Personal Data, the operator must issue **documents** defining its policies in relation to the processing of personal data, among other things.

Differences

Controllers must implement the internal policies 'where proportionate.' The GDPR does **not** give more details on how to draft such policies and what issues must be covered.

Under the Law on Personal Data **internal policies** should **outline** 'the operator's policy with regard to the personal data processing,' data breach identification and prevention procedures and data breach elimination procedures.

4.7. Notification of processing



Inconsistent

The general obligation to notify supervisory authorities existed in some Member States prior to the GDPR. According to Recital 89, this obligation is now abolished because it produced administrative and financial burdens, and it did not in all cases contribute to improving the protection of personal data.

In Russia, there is an obligation to notify Roskomnadzor of data processing. In addition, although not outlined under the Law on Personal Data, Roskomnadzor records all notifications and maintains a public register of operators available at www.rkn.gov.ru.

GDPR Recital 89	Law on Personal Data Article 22

Similarities

Not applicable.	Not applicable.

Differences

Under Recital 89 of the GDPR, general notification obligations have been **abolished** and instead 'replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which, in particular, involve using new technologies, or are of a new kind and where no DPIA has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.'	Operators **must notify** Roskomnadzor of their intended data processing operations prior to commencing such operations. The notification is a detailed document. It can be filled out online and in hard copy (in Russian only). The notifications are recorded in the Register of Operators. The operator must update its record in the Register of Operators. The updates must be submitted to Roskomnadzor within 10 business days from the day when the record becomes outdated. For example, this may happen when the operator runs new processing activities or deals with new categories of data.

5. Rights

5.1. Right to erasure

Both the GDPR and the Law on Personal Data allow individuals to request the deletion of their personal information.

It should be highlighted that whilst the GDPR provides for exemptions to the right to erasure, the Law on Personal Data does not.

GDPR Articles 12, 17 Recitals 59, 65-66	Law on Personal Data Articles 14(1), 21(3-5)

Similarities

Under the GDPR, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where inter alia the personal data are **no longer necessary in relation to the purposes for which they were collected** or otherwise processed, or in the event when the personal data have been **unlawfully processed**.

Under the Law on Personal Data, the data subject may request that the operator delete (erase) personal data if such data is **unlawfully processed**.

The GDPR provides under Article 19 that the data controller **communicates** any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed. Furthermore, Recital 59 of the GDPR outlines that the controller should respond to such requests from the data subject without undue delay, at the latest within one month, as well as provide reasons where the controller does not intend to comply with any such requests.

Under the Law on Personal Data the operator must **notify** the data subject, its representative and regulator (as applicable) about the fact of erasure of unlawfully processed data if the unlawful processing was revealed because of the inquiry of the data subject, its representative , or regulator (as applicable).

Differences

Exceptions for data controllers to provide an erasure request are outlined under Article 17(3) of the GDPR and include where processing is necessary for exercising the right of freedom of expression and information; in compliance with a legal obligation which requires processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; for reasons of public interest or public health; archiving purposes in the public interests, scientific or historical research purposes or statistical purposes; and for the establishment, defence or exercise of legal claims.

The Law on Personal Data does **not** provide specific exceptions to providing an erasure request.

5.2. Right to be informed

The GDPR and the Law on Personal Data grant the right of being informed to data subjects and include specific provisions regarding the information that data subjects must be provided when their information is collected and processed.

Unlike the GDPR, the Law on Personal Data does not distinguish between the notice given to individuals where personal data is indirectly obtained.

GDPR	Law on Personal Data
Articles 13, 14 Recitals 60, 61, 62	Articles 14(7), 18(1,2,3,4)

Similarities

Under GDPR where data is obtained directly, the data subject must be **immediately informed**, meaning at the time the data is obtained. The controller must provide the data subject with information, including, their identity, the contact details of its DPO (where applicable), the processing purposes and the legal basis, any legitimate interests pursued, the recipients when transmitting personal data, and any intention to transfer personal data to third countries.

Under the Law on Personal Data, the data subject has the **right to be informed** about data processing in particular: legal basis, purposes and methods of data processing, the identity of the operator, as well as cross-border data transfer.

The right to be informed also includes information about the **duration of storage**, the **rights** of the data subject, the ability to withdraw consent, the right to **lodge a complaint** with the authorities and whether the provision of personal data is a statutory or contractual requirement.

Under the Law on Personal Data, the data subject has the right to be informed on the following: the terms of data processing, including **the duration of storage**, the **rights** of data subject, the identity of person processing personal data under the authorisation of operator.

Under 14(5) of the GDPR, where the personal data is not collected from the data subject, in **exceptional cases** there is no obligation to inform.

Under the Law on Personal Data there are certain **exceptions** to informing the data subject, including in the event when the personal data is public data, or has been obtained from public sources.

If personal data is not obtained from the data subject, he or she must be provided the information within a reasonable period of time, but at latest after a month.

The Law on Personal Data addresses a similar concept under Article 18(3). If personal data is not obtained from the data subject, the operator must inform the data subject about the name and address of the operator or its representative, data processing purpose and its legal basis, assumed users of personal data and other information.

Where the collected personal data is used to directly contact the data subject, he or she has the right to be informed immediately upon being approached.

The Law on Personal Data addresses the obligation to obtain a consent of the data subject.

5.3. Right to object

The GDPR provides data subjects with the right to object to data processing activities under certain circumstance, including profiling. The Law on Personal Data does not address such a right. However, the Law on Personal Data similarly to the GDPR does provide data subjects the right to object to marketing.

GDPR Articles 7, 18, 21	Law on Personal Data Articles 14(1,7), 15(2)

Similarities

Under the GDPR, where personal data are processed for **direct marketing** purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Data subjects have the right to object to **telemarketing or emarketing** and the operator must immediately stop data processing activities (Article 15(2)).

Differences

The GDPR prescribes that data subjects have the **right to object**, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The Law on Personal Data does **not** outline the right to object to data processing under certain circumstances including profiling.

5.4. Right to access

Both the GDPR and the Law on Personal Data establish a right of access which provides data subjects with the right to obtain confirmation from the data controller under the GDPR or the operator under the Law on Personal Data, regarding whether or not their data is being processed, as well as details regarding such processing.

GDPR	Law on Personal Data
Articles 13(1)(f), 15 Recitals 58, 63, 64, 73	Articles 14(1,7), 18(1,2,3,4)

Similarities

The GDPR notes that the data subject shall have the right to obtain from the controller **confirmation** as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: the **purposes** of the processing; where possible, the **envisaged period** for which the personal data will be stored, or, if not possible, the criteria used to determine that period; the existence of **the right to request from the controller rectification** or **erasure** of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; and where the personal data are not collected from the data subject, any available information as to their source.

Under the Law on Personal Data the data subject has the right to obtain from the operator **confirmation** as to whether or not personal data of him or her are being processed, as well as access to the following information: **legal grounds for and purposes** of data processing, as well as the purposes and applied methods of data processing; **terms** of data processing, including duration of storage; **procedure for exploitation** of rights by the data subject as set forth by the Law on Personal Data; and the personal data processed in relation to certain data subject, the **source of their receipt**, unless other procedure is not stipulated by the federal law.

The GDPR notes that the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: the existence of **automated decision-making**, including profiling, and, at least in those cases, meaningful **information about the logic involved**, as well as the significance and the envisaged consequences of such processing for the data subject.

Under the Law on Personal Data a decision based solely on the **automated processing** of personal data that leads to legal consequences for a data subject or otherwise affects their rights and legal interests is permitted only if the data subject has given their **consent**, as well as this the operator is obliged to explain to a data subject the **procedure** whereby a decision is based solely on automated decision making.

GDPR	Law on Personal Data

Similarities (cont'd)

Under the GDPR, data controllers processing the personal data of data subjects must provide data subjects with information when including on the **recipients or categories of recipient to whom the personal data have been or will be disclosed**, in particular recipients in third countries or international organisations.	Under the Law on Personal Data, operators must (under the request of the data subject) provide the name and location of operator processing personal data, **information about persons** (except for employees of the operator), who have **access to personal data** which may be **disclosed** on the basis of agreement with the operator or under federal law.
Under Article 13(1)(f) of the GDPR, the controller shall provide the data subject, where applicable, with information regarding its intention to transfer personal to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, among other things.	Under the Law on Personal Data data subjects must be provided (under their requests) the information about conducted or planned cross-border data transfer.

Differences

Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the **appropriate safeguards** pursuant to Article 46 of the GDPR relating to the transfer.	The Law on Personal Data does **not** provide for the appropriate safeguards for personal data transfers to a third country or to an international organisation (see Section 5.1 below).
The GDPR does **not** specifically require the notification of the same to the data subject.	Under the Law on Personal Data, operators must provide data subjects with the **name or surname, name, middle name, address of person that is performing data processing** under the authorisation of operator, if processing has been authorised or will be authorised to such person.
Where data controllers are processing the personal data of data subjects they should inform them of the right to lodge a complaint with a supervisory authority.	The data subject shall have the right to receive information about the data processing, including the information on how to perform his/her rights. The right to lodge a claim is one of the protected data subject's rights.

5.5. Right not to be subject to automated decision-making

Under the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Under the Law on Personal Data, subject to certain exceptions, it is prohibited to make decisions exclusively on the basis of automated data processing, which give rise to legal implications in relation to a data subject or otherwise affects his or her rights and legitimate interests.

GDPR	Law on Personal Data
Articles 13, 14, 22 Recitals 71, 72, 91	Article 16

Similarities

Under the GDPR, automated decision-making is subject to data subject's **consent**.

Under 13(2)(f) of the GDPR, where personal data is directly obtained or under 14(2)(g) where personal data is indirectly obtained from the data subject the controller must inform of the data subject of the **existence of automated decision** making, including profiling, referred to in Article 22(1) and (4), and at least meaningful information about the logic involved, among other things, in order to ensure fair and transparent processing.

The Law on Personal Data prescribes that automated decision-making is allowed subject to the data subject's written **consent**.

Under the Law on Personal Data the operator must make clear to the data subject the **procedure for making such automated decisions** and possible legal implications associated with such decisions. The operator must review the objection within 30 days from the day of its receipt and notify the data subject about the results of such review.

Differences

The right not to be subject to automated decision-making **shall not apply** if the decision is **necessary for entering into, or performance of, a contract between the data subject and a data controller**; is authorised by EU or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent.

Exceptions to automated processing under the GDPR shall not be based on special categories of personal data referred to in Article 9(1) of the GDPR, unless point (a) or (g) of Article 9(2) of the GDPR applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

The Law on Personal Data does **not** provide for the similar exception. Automated decision-making in relation to the data subject or decisions affecting the rights and interests of the data subject may be made on the basis of exclusively automated data processing only under the **written consent** of the data subject or in cases determined by federal laws, which set forth certain measures for compliance with rights and interests of data subjects.

The Law on Personal Data does **not** have an equivalent to such a rule.

5.6. Right to data portability

The GDPR recognises the right to data portability. The right allows a data subject to request a copy of all personal data that the data subject has provided and a controller processes electronically and which must then be transmitted directly from controller to controller, in order to easily allow the data subject further use of the data.

The Law on Personal Data does not set out the data portability right.

GDPR	Law on Personal Data
Article 20 Recital 68	Not applicable.

Similarities

Not applicable.	Not applicable.

Differences

Under the GDPR, the data subject shall have the **right to receive the personal data concerning him or her**, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and the processing is carried out by automated means.	The Law on Personal Data does **not** set out the right to data portability.

6. Enforcement

6.1. Monetary penalties

The GDPR provides for administrative fines in case of non-compliance. The Law on Personal Data outlines that violations of its terms can incur liability stipulated by Russian legislation.

Although specific fines are not expressly outlined in the Law on Personal Data, the fines for violations are established by the Code of Administrative Offences of the Russian Federation of 30 December 2001 No. 195-FZ ('the Code of Administrative Offences') **recently amended by Federal Law No. 405-FZ on Amending Certain Legislative Acts of the Russian Federation which entered into effect on 2 December 2019**.

GDPR	Law on Personal Data
Articles 83, 84 Recitals 148-152	Article 24

Similarities

Under the GDPR, legal liability is established in the form of **administrative fines**.

Under the Law on Personal Data, entities found guilty of violating the requirements of the Federal Law shall carry **liability** stipulated by Russian Legislation. Monetary fines applicable to companies and their responsible managers are established under the Code of Administrative Offences, in particular Articles 5.39, 5.27 (only violations concerning employee data), 13.11, 13.12(6), 19.7. There are other types of liability (including criminal liability) but they are applied in rare cases.

Differences

Depending on the violation, the GDPR establishes the following maximum amounts of fines: **€10 million or up to 2% of the total worldwide annual turnover**; or **€20 million or up to 4% of the total worldwide annual turnover**.

There is **no** personal liability for the DPO and/or other responsible managers under the GDPR.

The maximum administrative fine for violations of the Law on Personal Data is **RUB 18 million (approx. €260,000)** under Article 13.11(9) of the Code of Administrative Offenses. This fine is established for a repeated violation of Article 18(5) of the Law on Personal Data.

Under the Code of Administrative Offences, **administrative fines can be imposed on both the operator and its responsible managers** whose misconduct resulted in non-compliance with the Law on Personal Data. Such managers are usually **the DPO and/or the CEO**. Roskomnadzor has the authority to decide which person(s), a responsible manager, the operator, or both of them, is/are to be accused of an administrative offence depending on the circumstances of the case. The amount of the fines for the responsible managers are significantly less than the fines for companies. For instance, the responsible manager

GDPR	Law on Personal Data
Differences (cont'd)	
	may be fined for up to **RUB 800,000 (approx. €12,500)** for committing the offence described in the previous paragraph.
The administrative fines may be imposed by the **supervisory authority**.	The administrative fines for the data protection offences are imposed by **court**. Roskomnadzor has the authority to initiate an action and submit it to court.

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE
GORODISSKY

6.2. Supervisory Authority


Fairly consistent

Both the GDPR and the Law on Personal Data prescribe that supervisory authorities shall oversee data processing. Similar to the GDPR, Russian law vests investigative and corrective powers on Roskomnadzor. However, the scope and limits of these powers differ in Russia and the EU. In contrast to the supervisory authorities under the GDPR, Roskomnadzor does not perform the authorisation and advisory functions.

GDPR Articles 51-84 Recitals 117-140	Law on Personal Data Article 23

Similarities

The corrective **powers** of the supervisory authority include, among other things, the following:

- ordering the controllers and processors to provide any **information** required for the performance of the supervisory authority's tasks;
- carrying out **investigations** in the form of audits;
- obtaining access to all personal data and information necessary for the performance of the supervisory authority's tasks;
- obtaining **access to any premises** of the controller and the processor, including to any data processing equipment and means, in accordance with EU or Member State procedural law;
- imposing a temporary or definitive limitation including a **ban on processing**; and
- imposing **administrative fines**.

The **powers** of Roskomnadzor include, among other things, the following:

- ordering the operators to provide any **information** required for the performance of Roskomnadzor's tasks;
- carrying out planned and extra-ordinary **inspection** checks of the operators and their processing activities;
- **accessing** all necessary information and documents in the course of the inspection checks; and
- **accessing premises**, equipment and other means of the operator in the course of the inspection checks;
- operator in the course of the inspection checks;
- taking measures to **suspend or stop personal data processing** if it is incompliant with the Law on Personal Data; and
- initiating an administrative offence action that may result in the imposition of an **administrative fine**.

The rules on the inspection checks are adopted by the Government of the Russian Federation.

The GDPR outlines that the supervisory authority must draw up an **annual report** and make it such a report available to the public, national governmental bodies and EU institutions.

Roskomnadzor must draw up an **annual report** and make it available to the public, the President, the Government, and the Parliament of Russia.

Differences

The investigative powers of the supervisory authority include the review on **certifications** issued according to Article 42(7) of the GDPR.

The Law on Personal Data does **not** provide for the certification mechanism.

GDPR	Law on Personal Data

Differences (cont'd)

The **corrective powers** of the supervisory authority include suspending cross-border data flows, issuing warnings regarding the intended processing, etc.	Roskomnadzor does **not** have such powers.
The supervisory authority has a wide range of **authorisation and advisory powers**, such as advising the controller, authorising contractual clauses, and approving Binding Corporate Rules, among other tasks.	Roskomnadzor does **not** have similar advisory or authorisation powers in the field of personal data. However, Russian law generally prescribes that any person may submit an inquiry to a state body and this state body must respond in writing. Russian data operators often use this mechanism for receiving certain advice from Roskomnadzor.

6.3. Other remedies

Fairly consistent

Both the GDPR and the Law on Personal Data guarantee the data subject's rights to lodge a complaint with the supervisory authority and seek for the compensation of material and non-material damage in a legal action. There are some procedural differences, for instance, relating to the distribution of burden of proof. In contrast with the GDPR, the Law on Personal Data makes no exceptions from the rule that the processor is liable only to the controller.

In addition, according to Russian law, some violations may lead to the complete blockage of access to websites from the territory of Russia. This mechanism constitutes a preventive measure, rather than a form of liability. That is why the access can be unblocked when the data breaches are eliminated. The GDPR does not establish any similar rules.

GDPR Articles 79-82 Recitals 141-147	Law on Personal Data Articles 23(2)(3.1), 24

Similarities

Under the GDPR, the data subject has the right to **lodge a complaint** with the supervisory authority. The supervisory authority must inform the data subject of the progress and outcome of his/her complaint.

Under the Law on Personal Data, the data subject has the right to **lodge a complaint** with the supervisory authority.

The data subject has the right to an **effective judicial remedy** against a controller and processor if he/she considers that his/her rights are infringed.

The data subject has the right to an **effective judicial remedy** against an operator if he/she considers that his/her rights are infringed.

The data subject may bring an action to compensate **material or non-material damage**. The GDPR does not set out minimum or maximum amounts of such compensations.

Under the Law on Personal Data the data subject may bring an action for recovery of **material or non-material damage**.

Differences

The **controller or processor must prove** that they are not responsible for the event giving rise to the damage.

The court **distributes the burdens** between the plaintiff and the defendant. The general rule is that each party must prove its own arguments.

The **controller is liable** for the damage caused by the processor. However, in some cases the processor may bear direct liability before the data subject.

The **processor is always liable** to the controller, and the controller is liable to the data subject.

There is **no** such mechanism under the GDPR.

Roskomnadzor may **block access to a website** containing personal data that is illegally processed on the ground of an effective court decision. The web-blockage is effective for all connections from the territory of Russia.

Gorodissky & Partners

Practicing since 1959

IP / TMT

GORODISSKY

Head Office:
B. Spasskaya Str., 25, bldg. 3
Moscow 129090, Russia
Tel.: +7(495) 937 6116
Fax: +7(495) 937 6104/6123
E-mail: pat@gorodissky.ru
www.gorodissky.com