Latvian Implementation of the GDPR

by Ieva Andersone and Jūlija Valpētere, Sorainen, with Practical Law Data Privacy Advisor
Law stated as of 12 Sep 2019 • Latvia

A Practice Note discussing the requirements of Latvia's Personal Data Processing Law which implements the EU General Data Protection Regulation (GDPR). This Note discusses the applicability of the Latvian data protection law and key provisions, such as rules for processing special categories of personal data and criminal conviction or offense data, the age of child consent, limitations on the scope of data subjects' rights, processing for journalistic purposes or academic, artistic, or literary expression, processing personal data in official publications, and processing for scientific or historical research, statistical purposes, or archiving in the public interest.

Contents

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) took effect on May 25, 2018, replacing the EU Data Protection Directive (Directive 95/46/EC) (EU Directive) and the prior Latvian data protection law. The GDPR introduced a single legal framework across the EU. However, the GDPR includes several provisions allowing EU member states to enact national legislation specifying, restricting, or expanding some requirements.

Latvia enacted the Personal Data Processing Law (PDPL), which aligns Latvian law with the GDPR. The PDPL also changes some of the GDPR's requirements. Organizations must understand how the PDPL's requirements vary and when they apply in addition to the GDPR.

This Note discusses the applicability of Latvian data protection law and key provisions of the PDPL, including requirements on:

- Processing special categories of personal data.
- Processing criminal conviction or offense data.
- The age of child consent.
- Limiting the scope of data subjects' rights and data controllers' related obligations.
- Processing personal data for journalistic purposes or academic, artistic, or literary expression.
- Processing personal data in official publications.
- Processing for scientific or historical research, statistical purposes, or archiving in the public interest.

Applicability of the GDPR and Latvian Law

The GDPR applies to:

- Data controllers and data processors that process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place in the EU (Article 3(1), GDPR).
- Data controllers and data processors not established in the EU that process personal data about EU data subjects when the processing activities relate to:
  - offering goods or services to EU data subjects, regardless of whether they require payment; or
  - monitoring their behavior that takes place in the EU.

- (Article 3(2), GDPR.)

Some EU member states have passed national laws that include a territorial scope provision that mirrors Article 3 of the GDPR, while other countries' laws have slightly modified the applicability language in this Article. However, the PDPL does not include a provision similar to or modifying the GDPR's scope provision or a general provision stating the territorial scope of the PDPL, therefore Article 3, GDPR applies.

For more on the GDPR's applicability and scope, see Practice Note, Determining the Applicability of the GDPR.

Data Protection Officers

The GDPR requires data controllers and data processors to appoint a data protection officer (DPO) under certain circumstances (Article 37(1), GDPR; see Practice Note, Data protection officers under the GDPR and DPA 2018). The GDPR allows EU member states to require DPO appointments in additional situations (Article 37(4), GDPR). The PDPL does not require appointing a DPO under additional circumstances or change the requirements or obligations applicable to DPOs under the GDPR.

The PDPL requires that DPOs satisfy the criteria specified in GDPR Article 37(5), which requires DPOs to have certain professional qualities and expert knowledge of data protection law and practice (Section 17, PDPL). Data controllers and data processors may appoint a person as DPO who appears on the Inspectorate's list of DPOs or may choose to appoint another person who satisfies the GDPR's requirements (Section 17, PDPL). The Inspectorate's list of DPOs only includes persons who have passed the qualification exam provided for in the PDPL (Sections 18 to 20, PDPL).

Processing Special Categories of Personal Data

The GDPR prohibits processing special categories of personal data unless an exception applies (Article 9(1), GDPR). Special categories of personal data include:

- Racial or ethnic origin.
- Political opinions.

- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Data concerning health or sex life.
- Sexual orientation.

(Article 9(1), GDPR.)

GDPR Exceptions Permitting Processing

GDPR Article 9(2) includes several exceptions to the prohibition on processing special categories of personal data. Some of these exceptions require data controllers to consult EU or member state law to determine a lawful basis for processing.

The exceptions requiring a basis in EU or member state law include when the processing is necessary for:

- Carrying out the data controller's obligations and exercising the data controller's or data subjects' rights in the fields of employment law, social security, and social protection (Article 9(2)(b), GDPR).
- Reasons of substantial public interest (Article 9(2)(g), GDPR).
- Purposes of preventive or occupational medicine to assess a data subject's working capacity, medical diagnosis, or for the provision of health or social care or treatment, the management of health or social care systems and services, or under a contract with a healthcare professional (Article 9(2)(h), GDPR).
- Reasons of public interest in the area of public health (Article 9(2)(i), GDPR).
- Archiving in the public interest, scientific or historical research purposes, or statistical purposes (Article 9(2)(j), GDPR).

Other GDPR Article 9 exceptions provide a sufficient legal basis for processing special categories of personal data without the need for a further basis in EU or member state law, including when the data subject consents to processing (Articles 9(2)(a), 9(2)(c), 9(2)(d), 9(2)(e), and 9(2)(f), GDPR).

EU or member state law may prohibit the use of data subject consent as a legal basis for processing special categories of personal data (9(2)(a), GDPR). However, the PDPL does not prohibit this.

For more on processing special categories of personal data under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Special categories of personal data.

PDPL Exceptions That Permit Processing Special Categories of Personal Data

The PDPL permits organizations to process special categories of personal data, including biometric data used for uniquely identifying a person:

- On the grounds specified in GDPR Article 9(2). If the organization relies on the GDPR Article 9(2) exceptions that require a basis in EU or member state law, processing must be based on a Latvian law that authorizes the processing for the purposes covered in the relevant Article.
- Based on other laws and regulations that permit processing genetic, biometric, or health data, as permitted by GDPR Article 9(4), which allows EU member states to introduce further conditions and limitations on processing these data categories.

(Section 25(2), PDPL.)

Processing Criminal Conviction and Offense Data

The GDPR only permits processing personal data relating to criminal convictions or offenses when:

- Carried out under the control of official authority, for example, the police.
- Authorized by EU or member state law providing for appropriate safeguards for data subjects.

(Article 10, GDPR.)

The PDPL does not include a provision authorizing processing this data under additional circumstances. The PDPL only allows public authorities to process criminal conviction or offense data (Section 34, PDPL). Processing by public authorities is outside the scope of this Note.

Processing for Secondary Purposes

The GDPR generally restricts data processing to the original collection purpose unless an exception applies, for example:

- The data subject consents to processing for a secondary purpose.
- An EU or member state law, which is a necessary and proportionate measure to safeguard certain important objectives, permits the processing for a secondary purpose (see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights).

(Article 6(4), GDPR.)

The PDPL permits processing personal data for secondary purposes if either:

- The processing:
  - is not otherwise prohibited by applicable laws; and
  - satisfies the grounds for data processing specified in the GDPR Articles 6 or 9.
- The processing is compatible with the original processing purpose under GDPR Article 6(4).

(Section 25(3), PDPL.)

Without data subject consent, any secondary processing purpose must be compatible with the original processing purpose. To determine the secondary processing purpose's compatibility, the data controller should consider the criteria specified in GDPR Article 6(4).

The PDPL also explicitly permits secondary processing by public authorities in the area of criminal law:

- If the data subject consents.
- To prevent immediate significant threat to public security.
- Under the Law Enforcement Directive (EU Directive 2016/680).
- For use in administrative or civil proceedings or the activity of public officials authorized by law if the processing relates to:
  - preventing, detecting, investigating, or prosecuting criminal offenses;
  - enforcing criminal penalties;
  - proceedings regarding criminally acquired property;
  - compulsory measures of a medical or correctional nature;
  - criminal liability measures applicable to legal entities such as companies, for example, liquidation, restriction of rights, confiscation of property, or recovery of money; or
  - repeated examination of an already adopted court ruling due to newly discovered facts or circumstances.

(Section 34, PDPL.)

Child Consent

For online service providers offering services directly to children (called information society services in the GDPR), the GDPR permits EU member states to lower the age of child consent below 16 years old, provided the age is not lower than 13 (Article 8(1), GDPR).

The PDPL reduces the age of child consent to 13 (Section 33, PDPL). However, it does not change the requirements for obtaining valid consent from children or impose any additional requirements or restrictions on processing personal data about children.

Data Subjects' Rights

The GDPR grants data subjects several rights and imposes several obligations on data controllers relating to those rights in Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) (see Practice Note, Data Subject Rights Under the GDPR). The GDPR permits EU member states to restrict the scope of these data subject rights and data controller obligations when the restriction is a necessary and proportionate measure to safeguard certain objectives (Article 23, GDPR) (see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights).

GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights

EU member states may restrict the scope of data subjects' rights and data controllers' related obligations found in GDPR Articles 12 to 22 and 34 when the restriction is a necessary and proportionate measure to safeguard:

- National security.
- Defense.
- Public security.
- The prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.
- Other important economic or financial public interests of the EU or member state, including:
  - monetary, budgetary, and taxation matters;
  - public health; and
  - social security.
- Judicial independence and proceedings.
- The prevention, investigation, detection, and prosecution of ethics breaches for regulated professions.
- Monitoring, inspection, or regulatory functions connected to the exercise of official authority regarding:
  - national or public security;
  - defense;
  - other important public interests;
  - crime prevention; or
  - breaches of ethics for regulated professions.
- Protection of the individual or the rights and freedoms of others.
- Enforcing civil law matters.

(Article 23(1), GDPR.)

EU or member state laws restricting data subjects' rights to ensure GDPR Article 23 objectives should include provisions on, when relevant:

- The purposes of the processing or categories of processing.
- The categories of personal data.
- The scope of the restrictions.

- The safeguards to prevent abuse or unlawful access or transfer.
- The specification of the controller or categories of controllers.
- Data retention periods and applicable safeguards, considering the nature, scope, and purposes of processing or categories of processing.
- The risks to the rights and freedoms of data subjects.
- Data subjects' rights to be informed about restrictions, unless doing so is prejudicial to the restriction's purpose.

(Article 23(2), GDPR.)

PDPL Exceptions to Data Subject Rights

The PDPL includes provisions limiting or changing the scope of data subjects' access rights (see Access Right), and also restricts several data subject rights in specific processing situations, such as when processing personal data in official publications, for scientific or historical research or statistical purposes, or archiving in the public interest (see Derogations for Specific Processing Situations).

The PDPL also provides that other laws and regulations not referred to in the PDPL may restrict data subjects' rights when necessary to satisfy the GDPR Article 23 objectives (see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights). Restrictions found in other laws or regulations are outside the scope of this Note.

Access Right

A data subject's right to receive certain information under GDPR Article 15 does not apply if disclosing the information is prohibited under laws and regulations on:

- National security.
- National protection.
- Public safety.
- Criminal law.

(Section 27, PDPL.)

The PDPL also restricts a data subject's access rights when the processing is for:

- Ensuring public financial interests in the areas of:
  - tax protection; and
  - prevention of money laundering and terrorism financing.
- Ensuring supervision of financial market participants and functioning of deposit guarantee systems.
- Application of the laws applicable to financial sector activities and macroeconomic analysis.

(Section 27, PDPL.)

The information provided to the data subject under GDPR Article 15 may not include a reference to:

- Public institutions directing criminal proceedings.
- Bodies performing operational activities.
- Other institutions when applicable law prohibits the disclosure of the information.

(Section 27, PDPL.)

Under the PDPL, data subjects may receive information about recipients of their personal data or categories of

recipients within the previous 2 years (Section 27, PDPL).

Derogations for Specific Processing Situations

The GDPR provides additional rules that apply to seven specific processing situations (Articles 85 to 91). These Articles permit EU member states to enact further rules that apply to the specified processing types. The PDPL introduces further rules that apply to processing:

- For journalistic purposes and purposes of academic, artistic, or literary expression (see Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression).
- Personal data held in official documents (see Personal Data in Official Publications).
- For archiving purposes, scientific or historical research, or statistical purposes (see Processing for Scientific or Historical Research, Statistical Purposes, or Archiving in the Public Interest).

Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression

The GDPR does not apply to processing for journalistic purposes, except for GDPR Article 5 (Principles relating to processing of personal data), if the processing meets the following conditions:

- The processing is conducted for freedom of expression and information in a manner that respects the right of a person to private life and it does not affect data subjects' interests which require protection and override the public interest.
- The processing is for the purpose of publishing information for public interest reasons.
- Complying with the GDPR is incompatible with or prevents the exercise of the right to freedom of expression and information.

(Section 32, PDPL.)

The GDPR also does not apply to processing for purposes of academic, artistic, or literary expression, except for GDPR Article 5 (Principles relating to processing of personal data), if the processing meets the following conditions:

- The processing is conducted in a manner respecting the right of a person to private life and it does not affect data subjects' interests which require protection and override the public interest.
- Complying with the GDPR is incompatible with or prevents the exercise of the right to freedom of expression and information.

(Section 32, PDPL.)

Personal Data in Official Publications

The GDPR permits EU member states to establish rules on the disclosure of personal data in official documents held by public authorities and bodies or private bodies performing tasks carried out in the public interest (Article 86, GDPR). The PDPL includes provisions on data processing in official publications.

The following data subject rights do not apply to processing conducted under laws and regulations on official publications:

- Rectification right (Article 16, GDPR).
- Erasure right, with certain exceptions (Article 17, GDPR; see Erasure Right Limitations).
- Processing restriction right (Article 18, GDPR).
- Data portability right (Article 20, GDPR).

- Objection right (Article 21, GDPR).

(Section 28, PDPL.)

A data controller's obligation to communicate rectification, erasure, and processing restriction requests to third-party recipients of the personal data under GDPR Article 19 also does not apply to data processing in official publications (Section 28, PDPL).

Erasure Right Limitations

The publisher of an official publication must erase published data if:

- A decision of the Inspectorate requires erasure.
- The publisher determines that publishing the data in the official publication does not comply with the GDPR.

(Section 28, PDPL.)

The Inspectorate may require erasure if the violation to a data subject's right to a private life is greater than the public benefit of official publication (Section 28, PDPL.)

Processing for Scientific or Historical Research, Statistical Purposes, or Archiving in the Public Interest

Scientific or Historical Research or Statistical purposes

The following data subject rights do not apply to processing for scientific or historical research purposes in the public interest or statistical purposes if honoring these rights renders impossible or seriously impairs achieving the processing's purpose and restricting the right is necessary to achieve the purposes:

- Access right (Article 15, GDPR).
- Rectification right (Article 16, GDPR).
- Processing restriction right (Article 18, GDPR).
- Objection right (Article 21, GDPR).

(Sections 29 and 31, PDPL.)

Archiving in the Public Interest

For processing relating to archiving in the public interest for purposes of creating, collecting, evaluating, preserving, and using national documentary heritage, data subjects must exercise access (Article 15, GDPR) and rectification rights (Article 16, GDPR) under the laws and regulations governing archives (Section 30, PDPL).

The following data subject rights do not apply to processing for these purposes if honoring these rights renders impossible or seriously impairs achieving the processing's purpose and restricting the right is necessary to achieve the purposes:

- Processing restriction right (Article 18, GDPR).
- Data portability right (Article 20, GDPR).
- Objection right (Article 21, GDPR).

(Section 30, PDPL.)

Data controllers' obligation to communicate rectification, erasure, and processing restriction requests to third-party recipients of the personal data under GDPR Article 19 also does not apply to this type of data processing (Section 28, PDPL).

Processing in the Employment Context

The GDPR permits EU member states, by law or by collective agreements, to provide more specific rules on processing personal data in the employment context (Article 88, GDPR). The PDPL does not provide more specific rules on processing in the employment context, therefore, the GDPR applies to employee data processing.

However, organizations should also consider the Employment Law when assessing the purposes and legal bases for processing employee personal data.

For more on relying on employee consent under the GDPR, see Practice Note, Employee Consent Under the GDPR.

Other GDPR Derogations

Supervisory Authority

GDPR Article 54 requires each EU member state to establish a supervisory authority. The PDPL establishes the Data State Inspectorate as Latvia's supervisory authority and provides for its organization and operation (Chapters II to IV, PDPL). The Inspectorate has the tasks and powers specified in GDPR Articles 57 and 58. The PDPL also provides the Inspectorate with additional tasks and powers specified in PDPL Sections 4 and 5.

The PDPL authorizes the Inspectorate to perform the following additional tasks, among others:

- Verifying that processing complies with legal requirements when applicable law prohibits a data controller from providing information to a data subject, after receiving a data subject request.
- Ensuring the qualification check of DPOs and maintaining a list of the DPOs who have passed the qualification exam.
- Participating, within its area of competence, in drafting laws and policies and giving opinions on draft laws and policy planning documents prepared by other institutions.
- Providing opinions on the compliance of personal data processing systems created by state and local government institutions.
- Cooperating with foreign supervisory authorities, ensuring information disclosure and access control, and ensuring the prohibition of sending commercial communications to supervisory institutions.
- Representing Latvia in international organizations and activities in the field of data protection.
- Carry out studies, analyze situations, make recommendations, provide opinions, and inform the public about current issues within its area of competence.
- Tasks required by other laws or regulations.

(Section 4, PDPL.)

The PDPL also grants the Inspectorate the following additional powers, among others:

- Inspecting data processing to determine conformity with applicable laws and regulations.
- Investigating administrative offenses, drafting reports, and imposing sanctions.
- Requesting and receiving documents and information necessary for inspections.
- Requesting and receiving the opinion of an independent objective expert within the scope of an inspection.

- Visiting State administration institutions and production facilities, warehouses, commercial, and other non-residential premises owned, possessed, or used by legal and natural persons within Latvia to verify that the operation conforms to applicable laws and regulations.
- Bringing actions before the court for violations of the PDPL or the GDPR.

(Section 5, PDPL.)

Administrative Fines

The GDPR permits EU member states to specify penalties for GDPR violations that are not subject to administrative fines under GDPR Article 83 (Article 84, GDPR). The PDPL does not apply administrative fines to any additional violations beyond what the GDPR states. The Latvian Administrative Violations Code remained in force after the GDPR took effect and governs administrative penalties for PDPL and GDPR violations in addition to the GDPR's provisions on penalties.

For more on enforcement and sanctions under the GDPR, see Practice Note, GDPR and DPA 2018: enforcement, sanctions and remedies (UK).

Complaints on Behalf of Data Subjects

The GDPR permits EU member states, in their national laws, to allow certain bodies, organizations, or associations to lodge a complaint with a supervisory authority independent of a data subject's authorization to lodge the complaint (Article 80(2), GDPR).

The PDPL does not include a provision authorizing this. However, the general provisions of the Administrative Procedure Law and the Law on Submissions, the supervisory authority must accept submissions and complaints by any person and must respond in substance or forward the submission to another responsible institution.

LATVIAN PDPL AND GDPR STATUTORY REFERENCES

Subject Matter	PDPL Section	GDPR Article(s) Permitting Member State Derogation
Requirements for processing special categories of personal data (see Processing Special Categories of Personal Data)	25(2)	9(1) and 9(2)(b), (g), (h), (i), (j)
Processing for secondary purposes (see Processing for Secondary Purposes)	25(3), 34	6(4)
Child consent (see Child Consent)	33	8(1)

Data subjects' rights (see Data Subjects' Rights)	27, 28, 29, 30, 31	23, 86, 89(1) and 89(2)
Requirements when processing for journalistic purposes or academic, artistic, or literary expression purposes (see Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression)	32	85
Processing personal data in official documents (see Personal Data in Official Publications)	28	86
Processing for archiving in the public interest, scientific or historical research, and for statistical purposes (see Processing for Scientific or Historical Research, Statistical Purposes, or Archiving in the Public Interest)	28, 29, 30, 31	89(1) and (2)
Supervisory authority (see Supervisory Authority)	Chapters II to IV, 4, 5	54

