Rödl & Partner

# NEWSLETTER BELARUS

# BUILDING BRIDGES

Issue:
October 2021

## Personal data protection | New law in Belarus

www.roedl.de/belarus | www.roedl.com/belarus

Rödl & Partner

# NEWSLETTER BELARUS

# BUILDING BRIDGES

Issue: October 2021

Content of this issue:


→ Personal data protection: Ongoing status

→ DPL: overview

→ Duties and compliance measures

→ Liability

→ Summary

→ To-do steps

# → Personal data protection: Ongoing status

### Ongoing data protection regulations

The existing regulation of personal data processing and protection in Belarus is rather sketchy and does not comply with worldwide accepted standards in this area. To date, Belarus has neither a comprehensive law in force governing personal data protection, nor a specialized state authority in charge of personal data issues.

Although there exist certain provisions on personal data protection stipulated in the Law "On information, informatization and protection of information" and other regulations, the exact scope of measures to be adopted in the field of data protection by businesses is vague. For this reason, there is no well-established law-enforcement practice in the area of personal data processing, which therefore makes this field rather unambiguous for businesses.

The first draft of the "Belarusian GDPR" was published as early as in 2016. In 2019, the bill on personal data was passed in the first hearings of the Belarusian Parliament and then the issue was postponed for a while.

Finally, Belarus implemented its tailor-made regulation, exclusively dedicated to data protection issues.

### The first Belarusian Personal Data Protection Law

In May 2021 the Belarusian Law on Personal Data Protection (the "**DPL**") was officially adopted and even now it can be considered as a breakthrough in the field of data protection. The DPL stands for the first comprehensive law specifically dedicated to the regulation of personal data processing and protection in the entire history of Belarus. What is more important for European business is that the DPL pursues the approaches to data protection much the same as reflected in the GDPR within many fields.

The DPL enters into force on **November 15, 2021**. Meanwhile, the implementation of the DPL requires companies to proceed with the review of their business processes in order to ensure compliance with new requirements once the DPL enters into force.

This newsletter may serve as a brief overview of the primary issues to be noted in connection with personal data protection in the light of the newly adopted DPL.

# → DPL: overview

## General information

It shall be noted that the primary provisions of the DPL are drafted based on the ones used within the GDPR as well as common approaches to the regulation of personal data processing used in many countries worldwide. For the first time in Belarus all the key elements of the personal data protection system have become regulated in more or less comprehensive manner.

| Key personal data protection issues covered by the DPL | |
|---|---|
| 1) | Definition of personal data and other basic concepts related to data protection |
| 2) | General requirements (basic principles) for personal data processing |
| 3) | Consent of the data subject, ways for obtaining such consent, other grounds for personal data processing |

| Key personal data protection issues covered by the DPL | |
|---|---|
| 4) | Rights of personal data subjects |
| 5) | Obligations of operators and authorized persons (similar concepts in GDPR are controllers and processors) |
| 6) | Creation of the state body in charge of personal data issues (data protection authority) |

## Scope of the DPL

The DPL covers personal data issues either with involvement of private companies and individuals, as well as state authorities and organizations. Same as applied in virtue of generally accepted approaches, personal, family and other similar purposes of personal data usage as well as state secrets issues are excluded from the scope of the DPL.

The DPL is mainly applied to **automated data processing** (i.e. via electronic means). Non-automated processing (hard documents) is subject to DPL requirements if the information in hard documents allows identification of personal data (e.g. databases, lists, etc.).

## Key concepts

According to the DPL, personal data stand for **any information** referring to a natural person already identified or a natural person which can be identified. Moreover, the DPL defines the **special personal data**, which are subject to different legal regime and comprise, *inter alia*, the ones as follows:

- biometrical (e.g. fingerprints);
- genetical (e.g. health issues);
- racial or national identity, religious and political commitments.

**Please note**
The DPL does not directly define if an online location data, IP address and information about the user's online behavior (cookie) are referred to as personal data. In order to minimize the possible risks, until eventual clarifications from the to-be-established data protection authority, this data should be treated as the personal ones.

The DPL uses concepts of "operator", "authorized party", "authorized data protection authority", which are very similar to the GDPR concepts of "controller", "processor" and "supervisory authority" respectively.

| DPL definitions | GDPR definitions |
|---|---|
| Operator | Controller |
| Authorized party | Processor |
| Authorized body for the protection of personal data subjects | Supervisory authority |

**An operator** stands for a person which processes personal data **independently**, while an **authorized party** does so on behalf of or in the interests of the operator **in virtue of a respective contract** therewith. By default, any person or a company which processes personal data is deemed as the operator and therefore being subject to the DPL requirements.

## Data protection authority

The to-be-established authorized body for the protection of the personal data subjects in Belarus (the "**data protection authority**") will perform largely the same control and protection functions as the supervisory authority stipulated by the GDPR. It shall be vested with the powers as follows:

- supervise personal data processing by the operators / authorized parties;
- examine complaints over personal data processing and, if necessary, require operators / authorized parties to change, block or delete personal data, which have been obtained in an illegal way or being inaccurate ones;
- to define the list of countries that have an adequate level of data protection and provide authorization for cross-border transfers where required;
- clarify regulations on personal data protection.

The creation of the data protection authority is expected in a short run.

→ DPL: overview

# Personal data processing: key requirements

The DPL affects the entire range of data flow and operations to be performed with personal data comprising its collection, systematization, storage, changing, usage, depersonalization, blocking, distribution and ultimately deletion. The DPL outlines the following key requirements (principles) for personal data processing:

| Requirement | Scope of requirement |
|---|---|
| Transparency | – by default, personal data processing requires a consent of a natural person while such person should be aware of the operations performed with the one's data |
| Purpose limitation | – purposes of personal data processing shall be clearly declared initially at the point of data collection and data shall not be used for any other purposes except for the declared ones |
| Accuracy | – personal data being processed must be correct and up-to-date at all stages of its processing |
| Restricted usage | – personal data shall be stored only during the period required for achievement of the declared purposes of their processing |
| Confidentiality | – protection against unauthorized or accidental access as well as any other illegal actions in relation to personal data shall be ensured |
| Liability | – persons processing personal data shall be in charge for incompliance issues |

→ DPL: overview

# Consent of natural persons

By default, the consent of a natural person for processing of one's personal data (the "**Consent**") is required for whatever means of processing.

## Form of the Consent

Finally, the DPL directly provides that the Consent can be **obtained by electronic means**, namely:

- by entering SMS code received;
- by ticking a check-mark in the respective web resource; as well as
- by any other means acknowledging the consent for personal data processing.

The written form of the Consent (hard documents) can be applied for these purposes as well. The respective Consent can be revoked by a natural person at any time. The primary principle of obtaining the Consent is **its opt-in nature** (a tacit consent for processing is not deemed as compliant with the DPL).

**Example**
The Consent check mark on the website being already filled out (☑) is not compliant with the DPL. The user shall tick it on one's own thus clearly expressing one's Consent.

## Notice on processing

Prior to obtaining the Consent the company, intending to process personal data of one's natural person, shall familiarize such person with the information as follows:

- data on the operator, which will process personal data;

- purposes of processing;
- list of personal data to be collected;
- list of operations to be performed with personal data;
- list of any other authorized parties, which will process personal data (if any);
- duration of processing as well as other information required for transparency of the data processing.

### Exceptions

The DPL provides for the cases where the Consent is not required. Such cases comprise, *inter alia*, the ones when personal data are processed for the purposes as follows:

- for employment reasons and in the course of employment relations;
- for the purposes of fulfillment a contract with a person;
- for certain reasons set forth statutory, e.g. during administrative of criminal cases, for AML and anticorruption purposes;
- with respect to the personal data specified in a document already submitted to the operator by a natural person.

→ DPL: overview

## Data flow

### Cross-border transfer

By default, the DPL provides for the "adequacy criterion" when it comes to cross-border transfer. This means, that the data protection authority shall approve the list of foreign countries which ensure the adequate level of legal protection (**"safe countries"**). A cross-border transfer of personal data to such safe countries **is allowed** without any other peculiarities.

The eventual transfer of personal data to "non-safe countries" by default is prohibited. The exceptions comprise, *inter alia*, the cases as follows:

- a natural person clearly expressed one's consent for cross-border transfer and has been informed about eventual risks in connection therewith;
- the data are transferred for the purposes of fulfillment of a contract with a natural person;
- the data are transferred for the purposes of AML compliance.

### Third-party transfer

A company which obtained personal data of one's natural person shall process them on their own. The engagement of the third parties for such purpose (authorized parties) is allowed subject to a separate contract on data processing being in compliance with statutory requirements.

By default, a separate consent for such third-party transfer is not required to be obtained by an authorized party, although it is the operator being in charge before a natural person for the actions of the engaged third party.

→ DPL: overview

## Rights of natural persons

Once a company collects the data of a natural person, the latter becomes vested with multiple rights in connection with processing of such data. The primary rights are summarized in the table below:

| Key rights of natural persons |
|---|
| – To revoke the Consent (for personal data processing) |
| – To obtain particular information on processing of one's personal data from an operator |
| – To seek for modification of one's personal data stored if they become outdated on inaccurate |

| Key rights of natural persons |
|---|
| – To obtain the information on transfer of one's personal data towards the third parties |
| – To seek for termination of one's personal data processing as well as their deletion |

# → Duties and compliance measures

## General information

The DPL directly introduces the vast range of the duties to be performed by legal entities dealing with personal data in Belarus. In brief, an operator / authorized party are under legal obligation to implement the measures as follows:

- Legal measures;
- Organizational measures;
- Technical measures.

The detailed scope and composition of measures to be implemented is left to the discretion of the operators / authorized parties processing personal data. In the meantime, the DPL defines the mandatory measures which formally shall be adopted by **all the companies which process personal data**. The list of such mandatory measures is outlined in a table below.

| Mandatory measures |
|---|
| – To assign an employee in charge of data protection ("data protection officer") |
| – To adopt the internal data protection policies ("internal policies") and ensure unlimited access thereto |
| – To define the procedure on access to personal data |
| – To ensure proper education of employees dealing with personal data as well as familiarize them with the internal policies |
| – To arrange a technical and cryptographical protection of personal data |



## Key issue

As mentioned, the DPL merely provides for just a generalized list of measures without clarification of what should be actually done. The primary controversy which has not been resolved by the DPL is the rule on technical protection of personal data.

The DPL reflects the mandatory duty for an operator to arrange a technical and cryptographical protection of personal data in a way set forth by the Operative Analytical Center before the President of the Republic of Belarus (the "**OAC**"). This contemplates creation of the complex technical system for data protection (data protection system) which should be subsequently certified by OAC.

The ongoing generalized wording of the DPL implies the need for such system **roughly for any company dealing with personal data**. From the practical perspective the creation of such system implies significant time and financial efforts.

With the adoption of the DPL it is expected from OAC to modify their approach and provide for more diversified rules on creation of the data protection system (e.g. depending on the volume and scope of personal data collected). The DPL directly defines that the to-be-established data protection authority shall define such diversified classification.

As to the rest of data protection requirements (i.e. legal and organizational ones) no detailed clarifications over their scope is set forth in the DPL. In the meantime, the DPL directly provides for the "self-reliance principle":

An operator (authorized party) shall define the list and scope of measures, which are sufficient for data protection (with a due regard to the requirements set forth by law)

This means, that by default a company dealing with personal data shall proceed as follows:

- to implement the "mandatory measures" set forth above;
- to implement other measures which can be required for data protection.


# → Liability

The DPL defines the need for a data breach notification. In case of any breach data protection system (e.g. in case of leakage) an operator shall inform the data protection authority within three business days.

Moreover, even now the effective laws provide for liability for data protection breaches which can be faced either by a company dealing with personal data or its officials.

| Type of liability | Form of liability |
|---|---|
| Administrative liability | – Penalty in the amount up to 200 basic units (ca. 1 900 Euro) – for natural persons<br>– Penalty in the amount up to 50 basic units (ca. 480 Euro) – for legal entities |
| Civil law liability | – Compensation for losses and damages; as well as<br>– Compensation for moral harm |
| Criminal liability | – Community service, fine, arrest, deprivation of certain rights or imprisonment for up to five years |

# → Summary

| Key changes in regulation of personal data protection |
|---|
| – Business finally has a clear legal framework for data processing and protection based on similar approaches applied in the EU |
| – By default, personal data processing is allowed only based on the free, unambiguous and informed consent of the personal data subject |

| Key changes in regulation of personal data protection |
| --- |
| – Clear and flexible requirements to the form of consent for data processing |
| – Definition of cases where the consent of the personal data subject is not required |
| – Available list of minimal measures to be adopted by companies dealing with personal data |
| – Administrative, civil law and criminal liability for violation of regulations in sphere of personal data protection has been outlined and significantly strengthened |

# → To-do steps

Despite the availability of certain legal gaps, the DPL marks a substantially new legal framework of personal data protection in Belarus, which is in line with global trends.

The **DPL enters into force on November 15, 2021** and thus it is of essence for businesses operating in Belarus to conduct a "due diligence" of the business processes and to proceed with the appropriate compliance measures in order to meet the requirements of the DPL, in particular:

- to assess the data flow in the company;
- to draft consent forms for personal data processing;
- to prepare and publish a set of documents defining the operator's policy on personal data;
- to appoint and train personnel responsible for personal data protection;
- to develop personal data processing agreements to be concluded between the authorized parties and operators.

Contacts for further information

Yurij Kazakevitch
Head of legal services
Associate Partner
T +375 17 2094 284
M +375 29 6218 974
yurij.kazakevitch@roedl.com

Viktor Marinitch
Lawyer
Senior Associate
T +375 17 209 4284
M +375 29 176 7737
viktor.marinitch@roedl.com

Sign up for our LinkedIn page for news and updates: Rödl & Partner Belarus »

## Imprint

Publisher:
Rödl & Partner
Ul. Rakovskaya, 16B-5H
220004 Minsk, Belarus
T +375 17 2094 284
minsk@roedl.com
www.roedl.de/belarus
www.roedl.com/belarus

Responsible for the content:
Yurij Kazakevitch
yurij.kazakevitch@roedl.com

Layout/Type:
Viktor Marinitch
viktor.marinitch@roedl.com