Latvia - Data Breach

TABLE OF CONTENTS

2. FINANCIAL SERVICES SECTOR

July 2020

GENERAL

1. LEGAL REQUIREMENT | OFFICIAL RECOMMENDATION

Please note that the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') now applies. You can read further information regarding breach notification requirements under the GDPR as part of our GDPR - Data Breach Guidance Note.

The GDPR in Latvian law is implemented by the Personal Data Processing Law of 21 June 2018 ('the Law'), while the Data Protection Directive with respect to Law Enforcement (Directive (EU) 2016/680) is implemented by the Law on the Processing of Personal Data in Criminal Proceedings and in Administrative Violation Proceedings of 8 July 2019 (only available in Latvian here).

The national supervisory authority for data protection matters, the Data State Inspectorate ('DVI'), has published various guidelines summarising the right of data subjects and obligations of data controllers (only available in Latvian here). In addition to its own guidelines, and specifically in relation to issues related to data breach notification requirements, the DVI further recommends the Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679.

Furthermore, the DVI has developed a procedure for data breach notification (only available in Latvian here) ('the Data Breach Notification Procedure').

2. NATIONAL VARIATIONS

While the general notification provisions of the GDPR are applicable also in the work of state institutions, the Law envisages liability for state officials who fail to comply with the obligations of data protection and non-disclosure.

At the time of publication of this Guidance Note, amendments of Personal Data Processing Law are being passed through the Cabinet of Ministers (only available in Latvian here) ('the Draft Law'). Within the discretion provided in Article 83(7) of the GDPR, the Draft Law does not impose fines on public authorities. Instead, it currently envisages an administrative fine of up to €1000 for state officials in cases of failure to comply with technical requirements of data protection. Failure to notify the DVI could be seen as an aggravating factor.

Section 305 of the Criminal Law of 17 June 1998 envisages liability for state officials for failure to comply with the procedures of special protection of persons set out by law or disclosure of identification data or the location of a person under protection. The liability applies regardless of compliance with notification requirements. The applicable punishments include deprivation of liberty for a period of up to one year or temporary deprivation of liberty, community service, or a fine.

3. PENALTIES

Penalties are applied by the DVI in accordance with Article 83 of the GDPR. Violation of the notification requirement gives rise to administrative sanctions of up to either €10 million or 2% of the annual worldwide turnover, whichever is higher.

Currently, there is no established practice in Latvia, regarding the amount of penalties applicable in case of failure to comply with the data breach notification requirements.

4. HOW TO

The DVI's Data Breach Notification Procedure (see section 1 above) outlines the procedure for notifying data breaches. In particular, a completed form (only available to download in Latvian here) can be sent to DVI's email address at info@dvi.gov.lv or by registered mail, delivered in person, or submitted to this portal.

TELECOMMUNICATIONS

1. LEGAL REQUIREMENT | OFFICIAL RECOMMENDATION

General requirements for data protection in the sphere of electronic communications are regulated by the Electronic Communications Law of 28 October 2004 (only available in Latvian here; unofficial translation before latest amendments available here) ('the Electronic Communications Law'). However, it explicitly provides that the provisions of GDPR and Commission Regulation (EU) No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under the ePrivacy Directive ('the Regulation') are applicable.

Under Section 68 of Electronic Communications Law, electronic communications merchants are required to comply with data protection requirements. This includes the obligation to notify the DVI in cases of breach of personal data protection. Section 1 of the Electronic Communications Law provides that an electronic communications merchant is a merchant or a branch of a foreign merchant who has the right to perform a commercial activity, to ensure a public electronic communications network or provide electronic communications services.

2. DEFINITION OF A DATA BREACH

Under Section 1 of Electronic Communications Law, a personal data protection violation is defined as the illegal processing of personal data.

However, this definition only applies in the context of the aforementioned Electronic Communications Law. The standard definition found in Article 4(12) of GDPR is in force.

3. WHO MUST NOTIFY A BREACH?

The notification of data breach must be submitted to the DVI by the data controller or his or her authorised representative. In the area of Electronic Communications Law, this obligation applies to the electronic communications merchant (defined in Section 1 of the Electronic Communications Law).

4. WHO MUST BE NOTIFIED?

4.1. Authorities

Under Section 68 of the Electronic Communications Law, electronic communications merchants are required to notify the DVI, which is the competent authority in accordance with Article 55 of the GDPR, of personal data breaches.

4.2. Subscribers

Under Section 68^3 of the Electronic Communications Law, electronic communications merchants were required to notify the subscriber, user or data subject regarding a breach of personal data protection, without undue delay, if such breach is likely to cause consequences for the subscriber, user, or data subject, or their privacy. In addition, Section $68^2$of the Electronic Communications Law further provides that the notification of the breach to the subscriber must contain:

- the information regarding the essence of the breach;
- contact information in order to acquire additional data regarding the breach; and
- the information regarding the measures to mitigate adverse effects of the breach.

However, in accordance with the Amendments to the Electronic Communications Law (only available in Latvian here), Sections 68^2 -68^4 governing the requirements to notify subscribers of the breach, breach notification and the registration of data protection violations been repealed.

The obligation for electronic communications merchants to inform subscribers may arise from Article 34(1) of GDPR. Electronic communications merchants must inform their subscribers if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

The notification must contain:

- name and contact details of the data protection officer or another contact point where more information can be obtained;
- description of the likely consequences of the personal data breach;
- description of the measures taken or proposed to be taken by the electronic communications merchant to address the personal data breach.

The designation 'high risk' is not further defined in the Latvian law. It has to be assessed on a case by case basis every time a data breach notification is sent to the DVI, taking into account the actual consequences and nature of the specific data breach.

4.3. Others

The obligation to notify data subjects is not only limited to subscribers. In the event of a data breach, data controllers should also notify other natural persons whose personal data or privacy may be affected by the data breach.

5. NOTIFICATION REQUIREMENTS

5.1. Type/content of notice

A completed form must be signed and submitted to DVI on-site, by mail or signed with a certified electronic signature and sent by email. The completed form should contain brief information regarding the following:

- contact information;
- date of detection of breach;
- nature of the breach;
- cause of the breach;
- categories of threatened data and approximate number of affected persons;
- type and number of data subjects affected;
- measures taken before the breach;
- consequences;
- actions to be carried out.

5.2. Substitute notice

There are no requirements for substitute notice set in the Latvian law or DVI Inspectorate guidelines. However, according to Article 3(6) of the Regulation, electronic communications merchants should notify the subscriber or any other individual on the personal data breach by means of communication that ensure prompt receipt of information and that are appropriately secured according to the state of the art.

According to Article 34(3) of GDPR, public communications can only be used if communication with individuals affected by the data breach would otherwise involve a disproportionate effort. Thus, in individual cases, it could be possible to inform the subscribers not only individually, but also through advertisements in major national or regional media.

5.3. Timeframe

The notice must be submitted without unnecessary delay, but not later than within 72 hours after becoming aware of the breach as set in Article 33(1) of the GDPR. It is not prohibited to split the notification into several parts and submit them all within this time period if this is seen as more effective by the data controller.

In case of failure to comply with the notification timeframe, reasoning for the delay must be included in the notification.

5.4. Exemptions

The data controller may be exempt from the duty to notify if the data breach is unlikely to pose a risk to the rights and freedoms of individuals as set in Article 33(1) of GDPR and Article 4 of Regulation due to technological protection measures

6. PENALTIES

Penalties are applied by the DVI in accordance with Article 83 of the GDPR. Violation of the notification requirement gives rise to administrative sanctions of up to either €10 million or 2% of the annual worldwide turnover, whichever is higher.

However, there is currently no established practice in Latvia for the amount of fines applied in case of failure to comply with the data breach notification requirements.

7. HOW TO

Information on how to notify a breach is contained in the Data Breach Notification Procedure. In this regard, please see section 4 under General requirements, above.

BREACH NOTIFICATION PROVISIONS IN THE FINANCIAL SERVICES AND HEALTH SECTORS

1. HEALTH SECTOR

The provisions set in Articles 33 and 34 of the GDPR are applicable without specific requirements set in the Latvian law.

According to Article 3 of the Regulation, data concerning health is a special category of data which is likely to adversely affect the personal data or privacy of data subject. In case of the data breach creating a high risk to the data subjects, the health institution may have to inform not only the DVI but also their patients if they are the relevant data subjects impacted by the breach.

According to Section 3 of the Regulation Regarding the Unified Electronic Information System of the Health Sector, the manager of the national health information system is responsible for implementation and compliance with security and technical standards. Therefore, if the data breach occurs on the national health information system's databases, the system manager will be responsible for notifying the DVI.

Sections 9 and 10 of the Law on the Rights of Patients of 17 December 2009 envisages a patient's right to access his or her medical data and expect that it will be protected in accordance with the GDPR. Thus, each health institution is individually responsible for complying with GDPR requirements and storing their patient data in a safe manner. This includes the responsibility to inform the Data State Inspectorate and, if necessary, affected patients.

2. FINANCIAL SERVICES SECTOR

Overall, there are no specific requirements for financial institutions to notify regulators or consumers regarding a data breach. The provisions set in Articles 33 and 34 of the GDPR are fully applicable.

According to Article 3 of the Regulation, data concerning financial information is likely to adversely affect the personal data or privacy of data subject. Thus, in case of breach of financial data with a high risk to data subjects, it is highly recommended for financial institutions to inform not only the DVI but also their clients who are the relevant data subjects.

Furthermore, Section 8(4^1) of the Consumer Rights Protection Law of 18 March 1999 establishes that during the process before entering into a consumer credit contract, any information on consumer income should be obtained and stored in accordance with legal acts on natural person data protection. Thus, each creditor is responsible for compliance with data protection requirements, including its ability to properly notify the DVI and affected consumers upon data breach.

ABOUT THE AUTHORS

Ieva Andersone

Sorainen

Ieva Andersone is a Partner and Head of the Competition & Regulatory practice at Sorainen Latvia. Ieva holds a law degree from the University of Latvia, and an LL.M degree from the University of Cambridge. She is admitted to the Latvian bar as of 2008.

ieva.andersone@sorainen.com

RELATED CONTENT

NEWS POST

Denmark: Datatilsynet expresses serious criticism of the Region of Southern Denmark's failure to conduct new IT system risk assessment, leading to unauthorised access of personal data

NEWS POST

Australia: OAIC releases Notifiable Data Breaches Report for January to June 2020

NEWS POST

USA: FinCEN issues advisory for financial institutions to assist in preventing Coronavirus-related cybercrime

NEWS POST

Romania: ANSPDCP fines Romanian Post RON 9,686.60 for failure to implement adequate security measures

GUIDANCE NOTE

Costa Rica - Cybersecurity