

Attention! Please note that the translation of this document into the English language is for information only. Officially you have to address the supervisory authority, i.e. State Data Protection Inspectorate, in the Lithuanian language.

Form approved by
29 August 2018 Order No 1T-82(1.12.E) of
the Director of the State Data Protection
Inspectorate

(Recommended form of the notification of personal data breach)

(name of the data controller (legal person), name of the representative of the data controller, name, surname of the data controller (natural person))¹

(registration number and address of the registered office of the legal person or personal identification number, date of birth (if the personal identification number is not available) of the natural person and personal data processing place)

(telephone number and/or e-mail address and/or electronic message delivery box address)

To the State Data Protection Inspectorate

**NOTIFICATION
OF A PERSONAL DATA BREACH**

_____ No _____
(date) (letter No)

1. Description of the personal data breach

1.1. Date and time of the personal data breach:

Date _____ Time _____

of the personal data breach

Date _____ Time _____

of detection of the personal data breach

1.2. Place of the personal data breach (tick as appropriate):

Information system

¹ Where the notification of personal data breach is given according to Article 29 of the Republic of Lithuania Law on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection of Criminal Acts or Criminal Prosecution Therefor, Enforcement of Sentences or National Security or Defence (hereinafter referred to as the "Law"), only the data of the data controller (legal person) shall be indicated.

- Database
- Server
- Website
- Cloud computing services
- Portable/mobile devices

- Files structured otherwise than by automatic means (archive)
- Other _____

1.3. Circumstances of the personal data breach (tick as appropriate):

- Loss of confidentiality of personal data (unauthorised access or disclosure)
- Loss of integrity of personal data (unauthorised change of personal data)
- Loss of access to personal data (loss, destruction of personal data)

1.4. Approximate number of data subjects whose personal data has been breached:

1.5. Categories of data subjects whose personal data has been breached (distinguished according to the particular distinctive character):

1.6. Categories of personal data the security of which has been breached (tick as appropriate):

- Personal data identifying the person (name, surname, age, date of birth, sex etc.):

- Special categories of personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health, data concerning sex life or sexual orientation):

- Data relating to criminal convictions and offences:

- Login data and/or identification numbers of the person (for example, personal identification number, payer code, passwords):

- Other:

- Not known (at the moment of service of the notification)

1.7. Approximate number of personal data the security of which has been breached:

1.8. Other information concerning the personal data breach which, in the opinion of the data controller, is relevant:

2. Possible consequences of the personal data breach

2.1. In case of loss of confidentiality:

- Wider spread of personal data than necessary and loss of control of the data subject in respect of personal data (for example, spread of personal data in the Internet)
- Association of different information (for example, association of the address of the place of residence with the location of the person in real-time)
- Possible use for the purposes other than the established ones or unlawful purposes (for example, for commercial purposes, identity fraud purposes, purposes of use of information against a person)
- Other

2.2. In case of loss of integrity:

- Change into incorrect data as a result of which the person may be deprived of the possibility to use the services
- Change into valid data so that processing of personal data was diverted (for example, stolen identity of the person by associating the data identifying one person with the biometric data of another person)
- Other

2.3. In case of loss of access to data:

- Services may not be provided due to the lack of personal data (for example, disturbance of administrative processes as a result of which such data as the person's health records cannot be accessed and health services cannot be provided to the parties or the rights of the data subject cannot be exercised)
- Proper services cannot be provided due to errors in personal data processing processes (for example, the person's health records no longer contain information on the person's allergies, the respective information is no longer available in the tax return as a result of taxes cannot be properly calculated etc.)
- Other

2.4. Other:

3. Measures assumed to address the breach or mitigate its possible effects

3.1. Measures applied with a view to reducing the impact on the data subjects:

3.2. Measures applied with a view to addressing the personal data breach:

3.3. Measures assumed with a view to preventing reoccurrence of the breach:

3.4. Other:

4. Recommended measures aimed at mitigating the consequences of the personal data breach

5. Notification of the data subjects of the personal data breach

5.1. Data concerning the fact of notification:

- Yes, the data subjects were notified (specify the date) _____
- No, but they will be notified (specify the date) _____
- No

5.2. Reasons of the failure to notify the data subjects whose personal data has been breached:

- No, since the rights and freedoms of the data subjects are not at great stake (specify why)

- No, since appropriate technical and organisational measures that render the personal data unintelligible to any person who is not authorised to access it are implemented (specify what measures)
- No, since appropriate technical and organisational measures preventing a high risk to the rights and freedoms of the data subjects are implemented (specify what measures)____

No, since this would involve a disproportionate effort and the information has been made publicly available (or a similar measure has been applied) (specify when and where the information was published or, if another measure has been applied, specify what measure was applied and when it was applied)

No, since the data subjects whose personal data has been breached have not been identified yet

5.3. Information which was provided to the data subjects (a copy of the notification to the data subject may be attached):

5.4. Method of notification of the data subjects:

- By mail
- By e-mail
- Otherwise _____

5.5. Number of the notified data subjects _____

6. Person who may provide more information on the personal data breach (data protection officer or another contact person)²

6.1. Name and surname _____

6.2. Telephone number _____

6.3. E-mail address _____

6.4. Position _____

6.5. Name and address of the workplace _____

7. Reasons of delay to submit the notification to the State Data Protection Inspectorate

8. Other relevant information

(position)

(signature)

(name, surname)

² Where the notification of personal data breach is given according to Article 29 of the Law, the data referred to in paragraphs 6.4 and 6.6 hereof shall not be specified.