

Data Breach Notification

according to article 33 in the general data protection regulation (GDPR).

If you are not able to answer all the questions, you can complement the notification once you have more information about the breach. In this case, the supplementation should be done promptly. Fields marked with an asterisk (*) should be filled in before submitting the application.

When amending a previously made personal data breach notification, only changed or updated fields are required.

Avoid entering information that you do not want to disclose.

Everything that you report here will become an official document. This means that anyone can request access to the document, and the document will have to be disclosed depending on the outcome of an assessment of whether secrecy applies. Therefore, we recommend that you only reply to the questions asked and that you do not provide more information than necessary in the free text fields. Should you nevertheless choose to provide information that is confidential in your view, you should use the free text field at the end of the form to describe which information this applies to. It is always the Swedish Data Protection Authority who finally decides whether a document can be disclosed or not.

Information about how the Swedish Data Protection Authority processes your data can be found on our website.

Version 1.5 – 2019-01-03



Should the breach be notified to the Swedish Data Protection Authority?

1. Is this a new data breach notification or is it an amendment or addition to a previous notification. Please only mark one box.

- New notification
- Amendment or addition. Please enter the code that was provided in the e-mail confirming reception of the first notification:

Internal reference number:

2. Incorrect incident report?

If a previously made notification has subsequently been determined to not concern a personal data breach, please state the reasons below.

3. Is the data breach unlikely to result in a risk to the rights and freedoms of natural persons?

- Yes
- No

If you replied yes above, the data breach does not need to be notified to the Swedish Data Protection Authority. Therefore, you will not need to send the form to the Swedish Data Protection Authority. However, you will still need to document the breach.

A risk to the rights and freedoms of natural persons may for example be that they lose control over their data, that they are deprived of their rights, that they are subject to discrimination, identity theft or fraud, financial loss, damage to the reputation or loss of confidentiality protected by professional secrecy or confidentiality. Please only mark one box.

4. Is it a cross-border data breach? Has the data breach occurred in Sweden or in another country? Please only mark one box.

- a. The data breach has occurred in Sweden and does not affect individuals in other countries
- b. The data breach has occurred in Sweden but also affects data subjects in other countries
- c. The data breach has occurred in at least one other country other than Sweden

If you replied b or c above, you should fill in the form for cross-border breaches instead of this form.

Controller

5. Name of the organisation *	Please enter the name of the controller where the data breach occurred.
6. Corporate identity number *	Please enter the corporate identity number for the controller where the data breach occurred.
7. Postal address of the controller *	

Contact person/s for the data breach notification

8. Name of the contact person/s *	The name of the person/s whom the data protection authority can contact.
9. The role of the contact person/s * Please only mark one box.	
<input type="checkbox"/> Data protection officer <input type="checkbox"/> Other	
10. E-mail address of the contact person/s *	
11. Postal address of the contact person/s	
12. Phone number of the contact person/s *	

The data breach	
13. When did the data breach occur? *	
14. When did you become aware of the data breach? * The time is mandatory.	
15. Your notification is submitted later than 72 hours after the time of discovering the data breach. Describe the reasons why.	
16. What has happened in relation to the data breach? * Please mark all relevant boxes.	
<input type="checkbox"/> Unauthorized disclosure through mailings of e-mail/letter/text message <input type="checkbox"/> Unauthorized disclosure: other <input type="checkbox"/> Unauthorized access: Someone within or outside the organisation has accessed information that they were not authorized to access <input type="checkbox"/> Loss: Information has been lost in some way, for example by a stolen computer or other device <input type="checkbox"/> Destruction: Someone or something has destroyed information, for example because a computer has been broken <input type="checkbox"/> Alteration: Personal data has been altered in some way	
17. Short description of the data breach	

<p>18. How did you become aware of the data breach? Please only mark one box.</p>	
<p><input type="checkbox"/> Through an automated procedure: technical security measures</p> <p><input type="checkbox"/> Through organisational routines, such as regular checks</p> <p><input type="checkbox"/> One of our employees has informed us</p> <p><input type="checkbox"/> Our processor informed us</p> <p><input type="checkbox"/> A person outside the organisation or a data subject informed us</p>	
<p>19. In your or your organisation's opinion, why did the data breach occur? Please only mark one box.</p>	
<p><input type="checkbox"/> Human error: a single mistake</p> <p><input type="checkbox"/> Lack of organisational routines or procedures: systematic errors</p> <p><input type="checkbox"/> Technical errors, such as software bugs, program settings</p> <p><input type="checkbox"/> Intentional attacks from someone within the organisation: internal attacks</p> <p><input type="checkbox"/> Antagonistic attacks: attacks from outside</p> <p><input type="checkbox"/> Unknown reason</p> <p><input type="checkbox"/> Other</p>	
<p>20. Within which field of activity did the data breach occur? Please only mark one box.</p>	
<p><input type="checkbox"/> Health and medical care</p> <p><input type="checkbox"/> Social services</p> <p><input type="checkbox"/> Schools: preschool, primary and secondary education</p> <p><input type="checkbox"/> University or college</p> <p><input type="checkbox"/> Other post-secondary education</p> <p><input type="checkbox"/> Research</p> <p><input type="checkbox"/> Finance and insurance</p> <p><input type="checkbox"/> Credit information</p> <p><input type="checkbox"/> Debt collection</p> <p><input type="checkbox"/> Other business activity</p> <p><input type="checkbox"/> Police</p> <p><input type="checkbox"/> Other judicial authorities</p> <p><input type="checkbox"/> Non-profit organisations or economic associations</p> <p><input type="checkbox"/> Municipal authority</p> <p><input type="checkbox"/> Governmental authority</p> <p><input type="checkbox"/> Other:</p>	

Processor	
<p>21. Does the data breach relate to personal data processing that is carried out by a processor or sub-processors? Please only mark one box.</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	
<p>22. Name of the organisation & Corporate identity number</p> <p>Name of the organisation & Corporate identity number:</p> <p>Name of the organisation & Corporate identity number:</p> <p>Name of the organisation & Corporate identity number:</p>	

The personal data and the data subjects	
<p>23. How many data subjects are affected?</p> <p>Exact number:</p>	
<p>If you do not have an exact number, please provide an estimate by marking one of the options below. Please only mark one box.</p> <p><input type="checkbox"/> 1–10 <input type="checkbox"/> 11–100 <input type="checkbox"/> 101–1 000 <input type="checkbox"/> 1 001–10 000 <input type="checkbox"/> 10 001–100 000 <input type="checkbox"/> 100 001–500 000 <input type="checkbox"/> 500 001–1 million <input type="checkbox"/> More than 1 million <input type="checkbox"/> Unknown/No information available</p>	

<p>24. How many data items about data subjects have been affected?</p>	
<p>Exact number:</p>	
<p>If you do not have an exact number, please provide an estimate by marking one of the options below. Please only mark one box.</p> <p><input type="checkbox"/> 1–10</p> <p><input type="checkbox"/> 11–100</p> <p><input type="checkbox"/> 101–1 000</p> <p><input type="checkbox"/> 1 001–10 000</p> <p><input type="checkbox"/> 10 001–100 000</p> <p><input type="checkbox"/> 100 001–500 000</p> <p><input type="checkbox"/> 500 001–1 million</p> <p><input type="checkbox"/> More than 1 million</p> <p><input type="checkbox"/> Unknown/No information available</p>	
<p>25. Which categories of data subjects are concerned? You may choose several options. Please mark all relevant options.</p>	
<p><input type="checkbox"/> The controller’s employees</p> <p><input type="checkbox"/> Users of services offered by the controller</p> <p><input type="checkbox"/> The controller’s customers</p> <p><input type="checkbox"/> Subscribers</p> <p><input type="checkbox"/> Members, due to membership in an organisation or a customer membership</p> <p><input type="checkbox"/> Military staff, i.e. employees in the Swedish Armed Forces</p> <p><input type="checkbox"/> Health and medical care patients</p> <p><input type="checkbox"/> Children</p> <p><input type="checkbox"/> Children in preschool or students in primary and secondary school</p> <p><input type="checkbox"/> Postsecondary students</p> <p><input type="checkbox"/> Vulnerable persons, such as persons with identity protection</p> <p><input type="checkbox"/> Other categories that you consider particularly exposed if personal data are disclosed</p> <p><input type="checkbox"/> Not yet known</p> <p><input type="checkbox"/> Other:</p>	

26. What categories of personal data has been affected by the data breach? Please mark all relevant options.

- Racial or ethnic origin
- Political opinions
- Religious or philosophical belief
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Data about sex life or sexual orientation
- Data about criminal convictions, offence or related security measures
- Personal identity number
- Economic or financial data
- Official documents
- Location data (for example GPS-position, not address information)
- Communication traces
- Communication metadata
- Identifying information (for example name, surname and birthdate combined)
- Contact details
- Unknown
- Other:

27. Was the personal data encrypted? Please mark only one box.

- Yes, all data
- Yes, but not all data
- No
- Unknown

Consequences

28. What may be the consequences of the data breach?

Please mark all relevant options.

- The data subject loses control over his/her own personal data
- Deprivation of rights
- Discrimination Identity theft or fraud
- Financial loss
- Unauthorized reversal of pseudonymisation
- Damage to the reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Any other economic or social disadvantage
- Other:

29. How serious is this data breach in your opinion?

Assess how serious the breach is with regard to the data subjects' privacy, on a scale of 1–4 with 4 being the most serious. Even if you can't assess the effects in detail we would like you to make an estimate of the seriousness.

Please mark only one box

- 1. Negligible
- 2. Limited
- 3. Significant
- 4. Maximal

30. How have you acted after the data breach?	
<p>Date and time:</p> <p>Measures taken:</p>	<p>Describe the action taken. Have you taken measures, or do you intend to take measures in order to solve problems, prevent or mitigate the effects of the data breach?</p>
<p>Date and time:</p> <p>Measures taken:</p>	
<p>Date and time:</p> <p>Measures taken:</p>	
<p>Date and time:</p> <p>Measures taken:</p>	

Information to data subjects	
<p>31. Have you informed the data subjects about the data breach? Please mark only one box.</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>if you replied yes above, go to the next question. If you replied no above, go to question 33.</p>	
<p>32. When did you inform the data subjects?</p> <p>Date:</p> <p>Go to question 36.</p>	
<p>33. Will you inform the data subjects later? Please mark only one box.</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> We have not decided yet</p>	
<p>34. When will you inform the data subjects?</p> <p>Date:</p>	
<p>35. On what grounds are you not going to inform the data subjects?</p> <p><input type="checkbox"/> The data breach does not result in a high risk to the rights and freedoms of natural persons <input type="checkbox"/> The personal data was encrypted or otherwise protected <input type="checkbox"/> We have already taken measures to prevent the risk <input type="checkbox"/> It would involve a disproportionate effort to inform each data subject individually, we have instead provided information to the public <input type="checkbox"/> Supplementary information to previous notification</p>	

Notification in phases/secretcy	
<p>36. This notification will be supplemented. If you are going to complete the notification later you must do so promptly. Please mark only one box.</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	
<p>37. You think that certain information in the notification should be considered confidential. Describe which information that in your view should be confidential and why.</p>	

Do you have any questions?

More information about data breach notifications can be found on our website:

www.datainspektionen.se/pui

If you do not find the answer on our website, you can

e-mail us on [personuppgiftsincident@](mailto:personuppgiftsincident@datainspektionen.se)

datainspektionen.se

or call us on 08-657 61 00.

Contact

The form should be sent by mail to:

Datainspektionen

Box 8114

104 20 Stockholm.

