Cross-Border 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.

Datainspektionen

Version 1.2 – 2018-08-27

Continues on the next page ➔

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:

.....

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. Has the data breach resulted in a risk to the rights and freedoms of natural persons?

☐ Yes
☐ No

If you replied no 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 a above, you should not fill in this form. You should instead fill in the Data breach notification form (for non-cross border notifications).

Continues on the next page ➔

5. Is your main establishment in Sweden? Please only mark one box.

- ☐ A. Your central administration is in Sweden and decisions on purpose and means for the processing are not taken in any other country within the EU/EEA
- ☐ B. Your central administration is in another country than Sweden but the decisions on purpose and means for the processing are taken in Sweden
- ☐ C. You do not have your central administration in Sweden and the decisions on purpose and means for the processing are taken in another country than Sweden

If you replied c above, you should not notify the Swedish Data Protection Authority. You should instead notify your "lead authority".

The lead supervisory authority is the supervisory authority of the main establishment or of the single establishment of the controller. The controller's main establishment' is: the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.

6. Which other countries are concerned by the data breach?
Mark all relevant boxes.

- ☐ Austria
- ☐ Belgium
- ☐ Bulgaria
- ☐ Croatia
- ☐ Cyprus
- ☐ Czech Republic
- ☐ Denmark
- ☐ Estonia
- ☐ Finland
- ☐ France
- ☐ Germany
- ☐ Greece
- ☐ Hungary
- ☐ Ireland
- ☐ Iceland (EES)
- ☐ Italy
- ☐ Latvia
- ☐ Liechtenstein (EES)
- ☐ Lithuania
- ☐ Luxembourg
- ☐ Malta
- ☐ Netherlands
- ☐ Norway (EES)
- ☐ Poland
- ☐ Portugal
- ☐ Romania
- ☐ Slovakia
- ☐ Slovenia
- ☐ Spain
- ☐ Sweden
- ☐ United Kingdom

A supervisory authority is a concerned authority if any of the following applies:
– you are established on the territory of the Member State of that supervisory authority
– data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing.

Continues on the next page ➔

Controller

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

Contact person/s for the data breach notification

10. Name of the contact person/s *	The name of the person/s whom the data protection authority can contact.
.....	
11. The role of the contact person/s * Please only mark one box.	
☐ Data protection officer ☐ Other Internal reference:	
12. E-mail address of the contact person/s *	
.....	
13. Postal address of the contact person/s	
.....	
14. Phone number of the contact person/s *	
.....	

Continues on the next page ➔

The data breach

15. When did the data breach occur? *

.....

16. Is the data breach still ongoing?

☐ Yes

☐ No

If you replied Yes above, go to question 18. If you replied No above, go to question 17.

17. When did the data breach cease?

Year-month-day:

.....

18. When did you become aware of the data breach? *
The time is mandatory.

.....

19. Your notification is submitted later than 72 hours after the time of discovering the data breach. Describe the reasons why.

.....

Continues on the next page ➔

20. What has happened in relation to the data breach? *
Please mark all relevant boxes.

- ☐ Unauthorized disclosure: Personal data has been disseminated in a wrongful way
- ☐ Unauthorized access: Someone within or outside the organisation has accessed information that they were not authorized to access
- ☐ Loss: Information has been lost in some way, for example by a stolen computer or other device
- ☐ Destruction: Someone or something has destroyed information, for example because a computer has been broken
- ☐ Alteration: Personal data has been altered in some way

21. Short description of the data breach

.....

22. How did you become aware of the data breach?
Please only mark one box.

- ☐ Through an automized procedure: technical security measures
- ☐ Through organisational routines, such as regular checks
- ☐ One of our employees has informed us
- ☐ Our processor informed us
- ☐ A person outside the organisation or a data subject informed us

Continues on the next page ➔

23. What kind of data breach does the notification relate to?

- ☐ A digital device has been lost
- ☐ A document has been lost/damaged
- ☐ An E-mail message has been lost or opened by an unauthorized person
- ☐ Hacking
- ☐ Malware Phishing - Incorrect disposal of personal data on paper
- ☐ E-waste (personal data still present on obsolete device)
- ☐ Personal data has been published unintentionally
- ☐ Unauthorized verbal disclosure of personal data
- ☐ Other

.....

24. In your or your organisation's opinion, why did the data breach occur? Please only mark one box.

- ☐ Human error: a single mistake
- ☐ Lack of organisational routines or procedures: systematic errors
- ☐ Technical errors, such as software bugs, program settings
- ☐ Intentional attacks from someone within the organisation: internal attacks
- ☐ Antagonistic attacks: attacks from outside
- ☐ Unknown reason
- ☐ Other

.....

Continues on the next page ➔

25. Within which field of activity did the data breach occur?
Please only mark one box.

- ☐ Health and medical care
- ☐ Social services
- ☐ Schools: preschool, primary and secondary education
- ☐ University or college
- ☐ Other post-secondary education
- ☐ Research
- ☐ Finance and insurance
- ☐ Credit information
- ☐ Debt collection
- ☐ Other business activity
- ☐ Police
- ☐ Other judicial authorities
- ☐ Non-profit organisations or economic associations
- ☐ Municipal authority
- ☐ Governmental authority
- ☐ Other

.....

Continues on the next page ➔

Processor

26. Does the data breach relate to personal data processing that is carried out by a processor or sub-processors?
Please only mark one box.

- ☐ Yes
- ☐ No

27. Name of the organisation & Corporate identity number

Name of the organisation & Corporate identity number:

.....

Name of the organisation & Corporate identity number:

.....

Name of the organisation & Corporate identity number:

.....

The personal data and the data subjects

28. How many data subjects are affected?

Exact number:

.....

If you do not have an exact number, please provide an estimate by marking one of the options below. Please only mark one box.

- ☐ 1–10
- ☐ 11–100
- ☐ 101–1 000
- ☐ 1 001–10 000
- ☐ 10 001–100 000
- ☐ 100 001–500 000
- ☐ 500 001–1 million
- ☐ More than 1 million
- ☐ Unknown/No information available

Continues on the next page ➔

29. How many data items about data subjects have been affected?

Exact number:

.....

If you do not have an exact number, please provide an estimate by marking one of the options below. Please only mark one box.

- ☐ 1–10
- ☐ 11–100
- ☐ 101–1 000
- ☐ 1 001–10 000
- ☐ 10 001–100 000
- ☐ 100 001–500 000
- ☐ 500 001–1 million
- ☐ More than 1 million
- ☐ Unknown/No information available

30. Which categories of data subjects are concerned? You may choose several options. Please mark all relevant options.

- ☐ The controller's employees
- ☐ Users of services offered by the controller
- ☐ The controller's customers
- ☐ Subscribers
- ☐ Members, due to membership in an organisation or a customer membership
- ☐ Military staff, i.e. employees in the Swedish Armed Forces
- ☐ Health and medical care patients
- ☐ Children
- ☐ Children in preschool or students in primary and secondary school
- ☐ Postsecondary students
- ☐ Vulnerable persons, such as persons with identity protection
- ☐ Other categories that you consider particularly exposed if personal data are disclosed
- ☐ Not yet known
- ☐ Other

.....

Continues on the next page ➔

31. 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

.....

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

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

Continues on the next page ➔

Consequences

33. 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

.....

34. What other consequences may be the result of the data breach?

Confidentiality breaches

- ☐ A larger distribution of personal data than necessary or consented by the data subjects
- ☐ Personal data may be linked with other information about the data subjects
- ☐ Other

.....

Integrity (alteration) breaches

- ☐ Incorrect personal data may have been processed by mistake
- ☐ Personal data may have been processed for other purposes than originally intended
- ☐ Other

.....

Availability breaches

- ☐ Loss of the ability to provide a critical service to the data subjects
- ☐ Alteration of the ability to provide a critical service to the data subjects
- ☐ Other

.....

Continues on the next page ➔

35. 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

36. How have you acted after the data breach?

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?

Date and time:

Measures taken:

Date and time:

Measures taken:

Date and time:

Measures taken:

Date and time:

Measures taken:

Continues on the next page ➔

Information to data subjects

37. Have you informed the data subjects about the data breach?
Please mark only one box.

☐ Yes

☐ No

If you replied Yes above, go to question 38.
If you replied No, go to question 39.

38. When did you inform the data subjects?

Date (Year-Month-Day)

.....
Go to question 43.

39. Will you inform the data subjects later?
Please mark only one box.

☐ Yes

☐ No

☐ We have not decided yet

If you replied Yes above, go to question 40. If you replied No, go to question 41. If you replied We have not decided yet, go to question 46.

40. When will you inform the data subjects?

Date (Year-Month-Day)

.....
Go to question 46.

41. On what grounds are you not going to inform the data subjects?

☐ a. The data breach does not result in a high risk to the rights and freedoms of natural persons

☐ b. The personal data was encrypted or otherwise protected

☐ c. We have already taken measures to prevent the risk

☐ d. It would involve a disproportionate effort to inform each data subject individually, we have instead provided information to the public

If you replied a or b above, go to question 46.
If you replied c, go to question 42.
If you replied d, go to question 44.

Continues on the next page ➔

42. Describe the measures taken in order to prevent the risks so that information to the data subjects is not required.	
..... Go to question 46.	
43. How have you provided information to the data subjects?	
..... Go to question 45.	
44. Describe in what way you have informed the public or what other measures you have taken in order to inform the data subjects in an efficient way. Fritextfält, max 150 tecken.	
.....	
45. What information have you provided to the data subjects? Please attach the information to the form.	
.....	

Continues on the next page ➔

Notification in phases/secrecy	
46. This notification will be supplemented. If you are going to complete the notification later you must do so promptly. Please mark only one box.	
☐ Yes ☐ No	
47. You think that certain information in the notification should be considered confidential. Describe which information that in your view should be confidential and why.	

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@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.

Datainspektionen