Form valid from
2016-02-01

Reference nr
18-3192

Owner
Telia Company AB
GSO Group Security

Report on personal data breach and integrity incident

– Personal data sent to wrong customer

	Requested data	Specifications
	Query 1 – 7: to be sent in, within 24 hours after verification, as an initial report	
1.	Name of the provider	*Telia Company AB*
2.	Identity and contact details of the data protection officer or other contact point where more information can be obtained	***Controlcenter.em@teliasonera.com***
3.	Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident	*2018-01-23 in a digital customer survey. Then work started to find the customer and get proper facts.* *2018-01-26 10:20 was the incident confirmed.*
4.	Circumstances of the personal data breach (e.g. loss, theft, copying)	*When a customer contacts Telia via the web, the system asks the customer to fill in the phone number and / or email address to get an answer to the case. If the customer does not enter a phone number, the system will pick up a previously entered phone number from the customer and previous contacts with Telia via the web. If the customer no longer has this number and a new customer received the number, updates on the case will reach the wrong customer. This is what happened in the present case.* *The field for the email address is mandatory so the same problem cannot be encountered.*
5.	Nature and content of the personal data concerned	*Name, address, email address, phone number and customer number*
6.	Technical and organisational measures applied (or to be applied) by the provider to the affected personal data	*The current customer information that was seen by another person will be deleted. Telia will also contact the other person to request deletion of any information that the person has received incorrectly.*

7.	Relevant use of other providers (where applicable)	*N/A*
	Query 8 – 16: to be sent in, within 72 hours after the initial report	
8.	Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved)	*A customer contacted Telia via the web and the web system provides a phone number from earlier web contacts if the customers does not fill in any number. In this case the customer had terminated the old number and a new customer had received the number. The updates on the web case reach wrong customer.*
9.	Number of subscribers or individuals concerned	*One.* *Telia is now investigating the possibility of other customers being affected with the same breach.*
10.	Potential consequences and potential adverse effects on subscribers or individuals	*Customer personal data was exposed for one other person. Telia will urgently contact that person and explain the circumstances then ask for deletion* *There is no sign on abuse of customer credential. Observed neither by the customer nor by Telia.*
11.	Technical and organisational measures taken by the provider to mitigate potential adverse effects	*Telia will release a new configuration for the actual web system so customers always needs to fill in a phone number for further contacts. The release will be launched this week.*
Possible additional notification to subscribers or individuals		
12.	Content of notifications	*One, speaker script will come.*
13.	Means of communication used	*Call*
14.	Number of subscribers or individuals notified	*One*
Possible cross-border issues		
15.	Personal data breach involving subscribers or individuals in other Member States	*N/A*
16.	Notification of other competent national authorities	*N/A*

Form valid from
2016-02-01

Reference nr
18-3192