

Data leak procedure

This is the data leak procedure of the Netherlands Heart Institute. This procedure applies to all activities of the Netherlands Heart Institute and should be followed by all our staff, whether you are working in Utrecht or on one of our projects in one of the academic medical centres.

What is a data leak?

We define a data leak as the possibility that personal data of any kind has been leaked outside our organisation. For example:

- you leave a USB stick containing sensitive data somewhere in a meeting room
- you mail an excel file containing names and e-mail addresses to the wrong person
- you discover that personal data on a web site is not served over an encrypted (SSL) connection
- etc

There are two key elements in the definition of a data leak:

- “possibility” if it was possible for an outsider to get access to the data we should treat it as a data leak, even if there is no evidence that anyone actually accessed it
- “outside” meaning that the data has leaked outside our organisation

What to do first?

Report a data leak immediately to privacy@heart-institute.nl. After you send your e-mail please phone 088-2333600 and draw attention to the e-mail.

We risk high fines if we fail to report the data leak to the *Autoriteit Persoonsgegevens* within 72 hours.

Therefore, report the issue without delay! If you are not sure if there was a data leak, report it anyway.

What happens next?

The Netherlands Heart Institute has an official responsible for data protection: Susan van den Berg

After your report the leak, Susan will contact you and determine as accurately as possible:

- which type of data has potentially been exposed?
- how many persons are concerned?
- has the data actually been accessed by unauthorised third parties?
- which (technical) measures need to be taken to make our data safe again?
- should the leak be reported to the *Autoriteit Persoonsgegevens*?
- should we inform the persons concerned?

The data protection official will report the leak to the *Autoriteit Persoonsgegevens* and to the persons concerned if she deems this necessary.

The data protection official will produce a detailed report of all the information gathered and all the steps taken.