Erasmus MC
University Medical Center Rotterdam

Data leaks

Eric Neeleman, Manager IT

Actualiteit

News Items - 24-11-2016

NOS: Ziekenhuizen lekken dagelijks privacy gevoelige informatie

Trouw: Ziekenhuizen melden elke dag datalek

In huis: Elke maand een datalek.

Data leaks

Since the 1st of January 2016 new national privacy regulations came into effect. These regulations also apply to our data.

Amongst other things a new law **Reporting data leaks** came into effect:

Data leaks which may have serious consequences for the people involved (participants in our studies), must be reported within 48 hours (or two days) at the National Supervisory Authority, “De autoriteit persoonsgegevens”. In certain instances, also the subjects whose personal data have been leaked, should be informed.

What is a Data leak ?

A data leak involves access to, destruction, modification or release of personal information in an organization without this being the intent of this organization.

A data leak not only includes the release (leakage) of data, but also unlawful processing of data.

Personal data are facts that say something about identifiable (not anonymous) person.

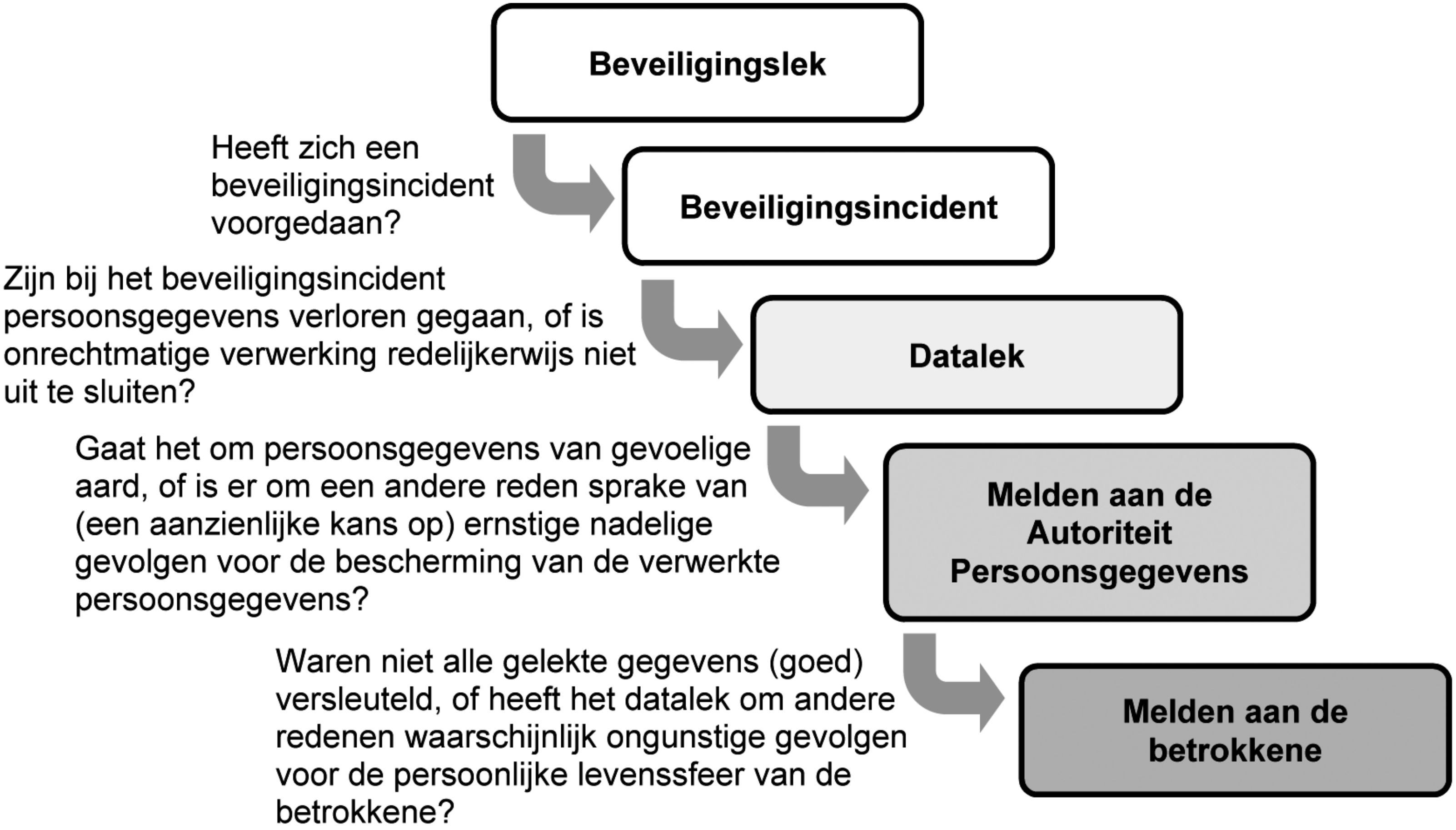
Concequences for Erasmus MC

Data breaches that may have serious adverse effects on the persons concerned must be reported within 48 hours (or two days) after discovery to the Authority for Personal Data.

In some cases, even the persons whose personal data have been leaked, should be informed.

In case of a failure to comply with the reporting a fine can be imposed on Erasmus MC of up to € 810 000, - per incident or 10% of the annual turnover.

Checklist



Beveiligingslek

Heeft zich een beveiligingsincident voorgedaan?

Beveiligingsincident

Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan, of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?

Datalek

Gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?

Melden aan de Autoriteit Persoonsgegevens

Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?

Melden aan de betrokkene

Examples data leak or not ?

A lost usb stick with anonymized data

Examples data leak or not ?

A stolen encrypted laptop with pseudo anonymized respondent data.

Examples data leak or not ?

An intrusion in a database by a hacker.

Examples data leak or not ?

A former employee that still has access to a database.

Examples data leak or not ?

A stolen printed medical record

Examples data leak or not ?

A personal computer with personal data infected by Ransomware.

Examples data leak or not ?

Sending emails to large groups of recipients whose addresses are not shielded

Examples data leak or not ?

Accidentally deleted personal data.

What to do ?

Report the data leak **as soon as possible**. Withholding can have major consequences.

Report the data leak to the datamanager of the study.

- o Rotterdam Study (ERGO) -> Frank van Rooij
- o Generation R -> Claudia Kruithof or Marjolein Kooijman

Data Management will take the next steps:

- o Report of the data leak to the head of the department
- o Report of the data leak to Erasmus Legal Affairs (010-70)34986
- o An Email report of the data leak to datalek@erasmusmc.nl

Rules

All employees must abide to the confidentiality agreement they signed. Examples can be found at the Wikipages of Generation R and ERGO.

In particular pay attention to paragraphs 7 and 8: Data should absolutely not be taken out of the Erasmus MC and at the end of the employment all data will be transferred to the data manager.

Any loss of data should be reported to the data manager of the relevant study.

What can I do ?

- Ensure proper security of sensitive data by encryption. This avoids that the data is identifiable.

- Don’t take respondent data outside of the Erasmus MC.

- Don’t distribute personal information via e-mail and / or Cloud services.

- Be aware of the notification obligation data leaks and report if necessary. When in doubt ask the datamanager.

- Make an formal agreement with parties that process your data. This is mandatory! In the agreement must be stated who is responsible in case of a data leak.

- Make agreements on data leak prevention with other organizations with which you cooperate or exchange data.

Encryption Tools

Laptops must be encrypted. If you use a Microsoft Windows PC this can be done with the Microsoft tool: Bitlocker or the free tool: TrueCrypt. TrueCrypt can be found in the Application Catalog under the tab Tools.

Apple laptops must be protected with the standard provided tool FileVault.

USB sticks must be protected. This can be done with TrueCrypt or Bitlocker.

Encryption Tools (2)

7-ZIP

Files that you can protect with 7-Zip sent through the mail with a password. Obviously the password should not be send in the same mail but should be send in a separate message through messaging.

FileSender:

For secure transmission of large amounts of data, you can use https://filesender.surf.nl/

For advice and support, please contact Nano Suwarno or Alwin Koedoot.

Stay Alert

The mentioned tools are safe to use at this moment as far as we know.

Hackers make progress everyday so what is safe today might not be safe tomorrow.

Your Own Device

If you bring your own device into Erasmus MC you will need to comply to the folowing rules:

- The system must have a recent OS (Preferabel the most recent OS)
- A Viruschecker must be activated.
- The system must be protected with a user name / password

  You need a strong, lengthy alphanumeric password, too, not a simple 4-digit numerical PIN
- The system must be encrypted.

If you are not sure wether you comply please contact the system manager.

Your Own Device

Windows laptops:

Bitlocker

Apple laptops:

Filevault must be used to encrypt the the startup disk and work disk on your Mac

USB-stick or any other storage device

Bitlocker, Truecrypt or Veracrypt

More information

http://intranet.erasmusmc.nl/jz/gegevensbescherming/

https://autoriteitpersoonsgegevens.nl/

https://veracrypt.codeplex.com/

Datawiki

Thank You