AUTORITEIT
PERSOONSGEGEVENS

EDPS – ENISA Conference

Towards assessing the risk in personal data breaches

Max Rozendaal | Brussels | 04-04-2019

Statistics Data Breach Notifications (DBN)

- DBN since 2016
- 21.000 DBN in 2018
- 2000-2300 DBN per month

Types of DBN

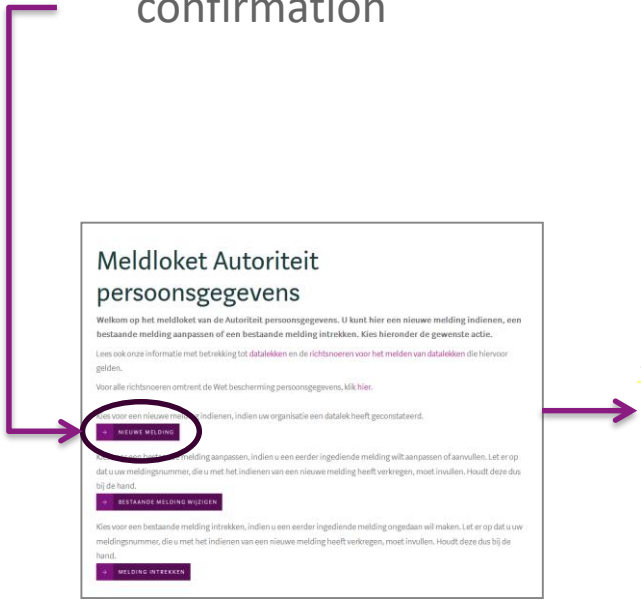
- Financial and medical sector, public government
- Letters sent to wrong addressees
- Human error
- Hacking / malware / phishing

Risk assesment by controller

- Controller: 90% negligible or limited risk
- NL SA: 30-35% preliminary investigation
- Difference in assessment
- Hacking / malware / phishing

Notifying

- Web form to report
- Automatic receipt confirmation



Autoriteit Persoonsgegevens

- Automatic categorisation

- Intake team assessment

- Bulk assessment

Automatic categorisation

Criteria:

- **Sensitive personal data**
- **Vulnerable groups**
- **Hacking, malware, phishing**
- **>2500 persons affected**?

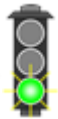
Yes

- **Data subjects notified**?

No

Yes

No



Assessment in practice

- Breach: November 2016
- Notification: November 2017
- Dataset on 57 million data subjects

Nature of data

- Online identities
- Special categories of data
- Other sensitive data

Online identities

- Username and password
- Hashing algorithms
- MD5 vs. modern algorithm

Amount of data

- Large amount of categories of data
- Large amount of data subjects
- Balancing test

Moment of risk assessment; notification to Data Subject

- Controller: moment of knowledge of breach
- NL SA: moment of notification to NL SA
- Circumstances change in meantime

AUTORITEIT
PERSOONSGEGEVENS

Risk assessment

Do not underestimate risks to data subjects

Max Rozendaal | Brussels | 04-04-2019