# Supporting data controllers in assessing the risk of a personal data breach

EDPS-ENISA Conference: Towards assessing the risk in personal data breaches

Brussels, 5 April 2019

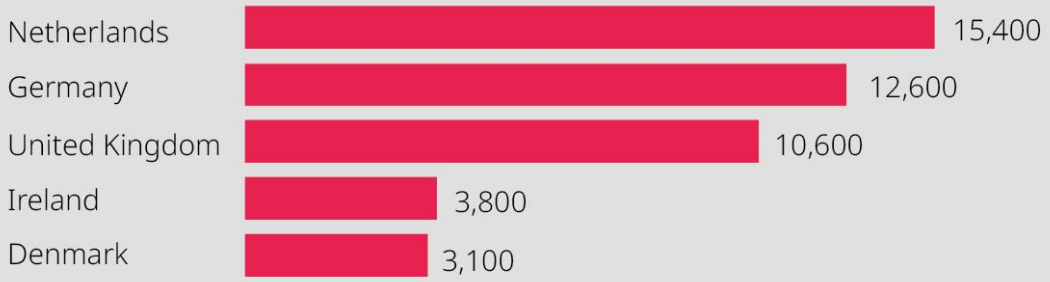
Prof. Dr Patrick Van Eecke

DLA PIPER

More than 59,000 data breaches were reported in the eight months after GDPR came into force.

DLA PIPER

## Reported GDPR data breaches per country*

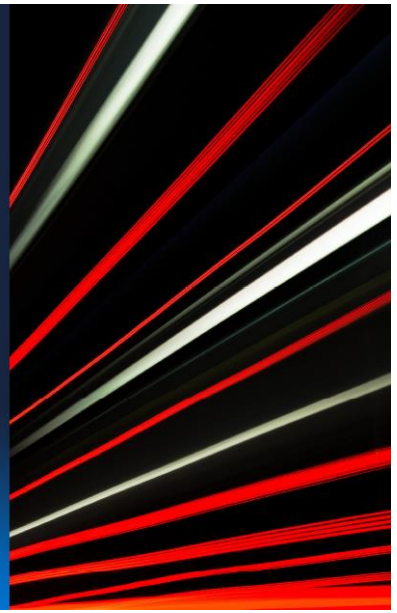



DLA PIPER

*From 25 May 2018 to 28 January 2019

DLA PIPER

91 GDPR-related fines have been imposed in EEA member states since 25 May 2018. The highest fine to date was imposed on Google for €50 million.



## Per capita country rankings

DATA BREACHES PER 100,000 PEOPLE


DLA PIPER

# Data breaches: the issue

## Data breach notification duty

GDPR requires companies to notify data breaches to the regulatory authorities and the wider public

## Short deadline

The notification needs to be done within a very short time frame: 72 hours after the company has become aware of the data breach

## Trigger based on the severity of the data breach

If "risk" to the rights and freedoms of natural persons: regulatory authories need to be informed.

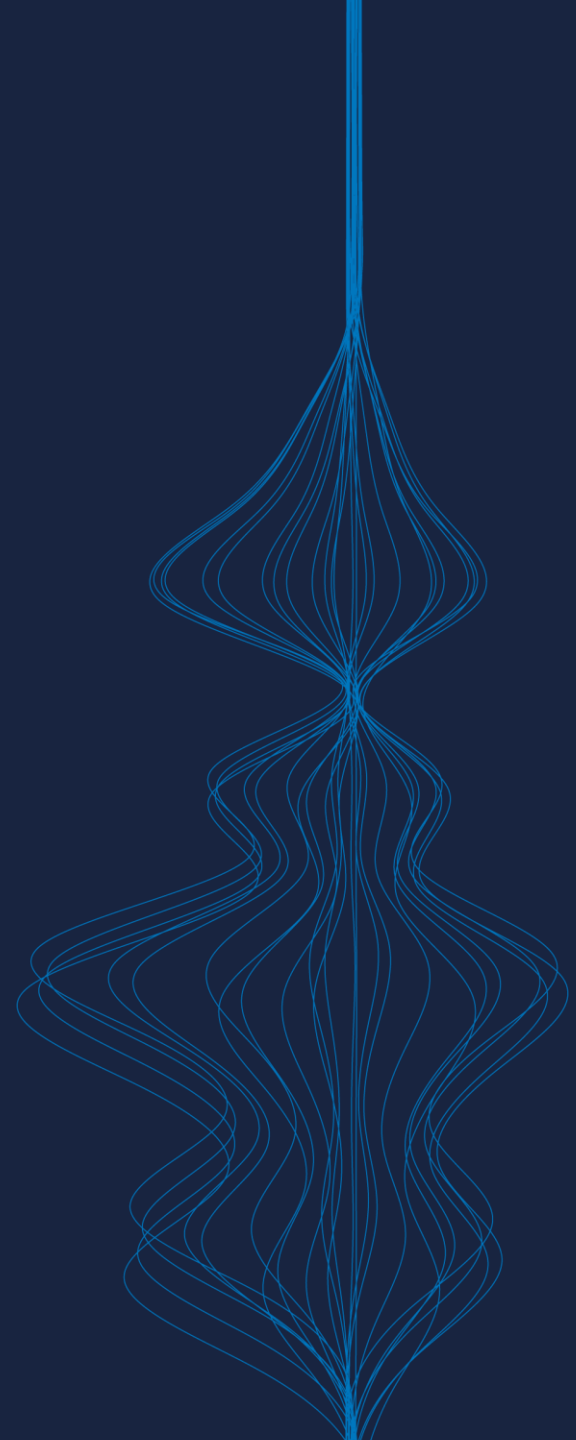
If "high risk" to the rights and freedoms of natural persons: the victims need to be informed as well.

## Documentation obligation

The assessment whether or not to notify needs to be documented including the facts relating to the personal data breach, its effects and the remedial action taken

## Potential sanctions

Sanctions for not notifying a risk or high risk data breach may lead up to 10 million euro or 2% of the global annual turnover of the company.



# Data breaches: the challenge

**Unclear description of notification triggers**

The triggers to notify (risk/high risk) are not well described by the legislator making it difficult for companies to assess the severity of the data breach.

**"Gut feeling" assessment**

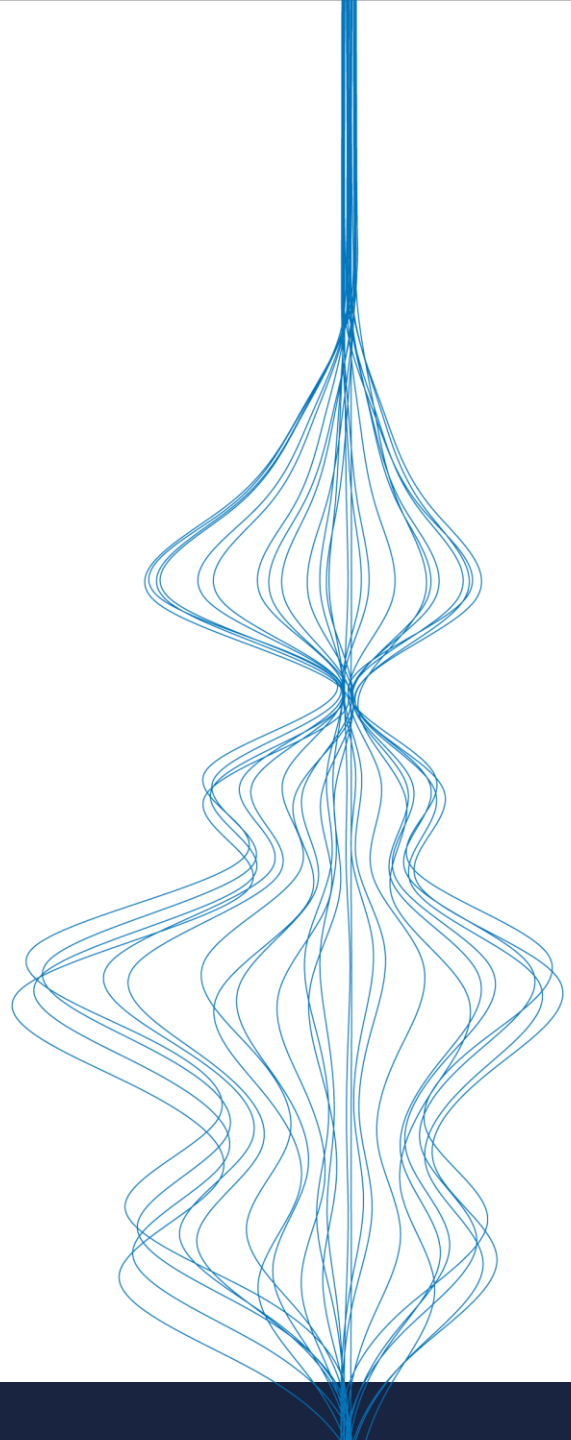
Measuring the severity of a breach is therefore often based on simple gut feeling and ad hoc decisions, without using clear criteria and a consistent approach,

**Time consuming assessment**

Many stakeholders being consulted, having different views, resulting in long discussions,

**(lack of) methodology challenged by DPA's**

Regulatory authorities are challenging companies on the methodology they use for assessing the severity of a data breach, claiming that companies do not use a consistent assessment method and that companies do not document their assessment



# Data breaches: the need

**Need for clear criteria**

Clear criteria describing what constitutes a risk/high risk with well described examples

**Need for objective criteria**

Criteria and examples developed by authoritive sources

**Need for combined quantitative & qualitative approach**

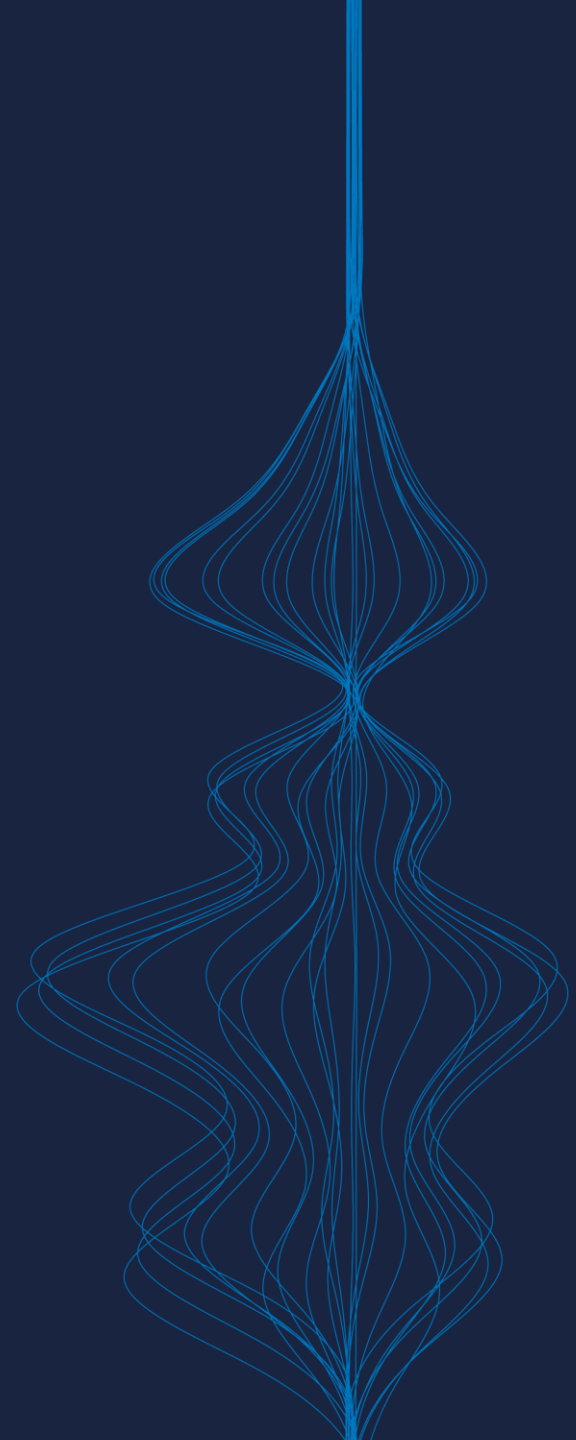
From a gut feeling to a quantitative/qualitative approach

**Is this possible?**

Yes, it is possible !

**Has it been done before?**

Yes, it has been done before



# Data breaches: the solution

**ENISA algorithm as starting point**

Introduces a Quantitative approach: SE = DPC x EI + CB

**Updated to bring in line with GDPR**

Mitigating factors (Article 34 (3) GDPR)

**Refined by EDBP**

Criteria and examples (eg. severity of consequences for individuals)

**Brings objectivity**

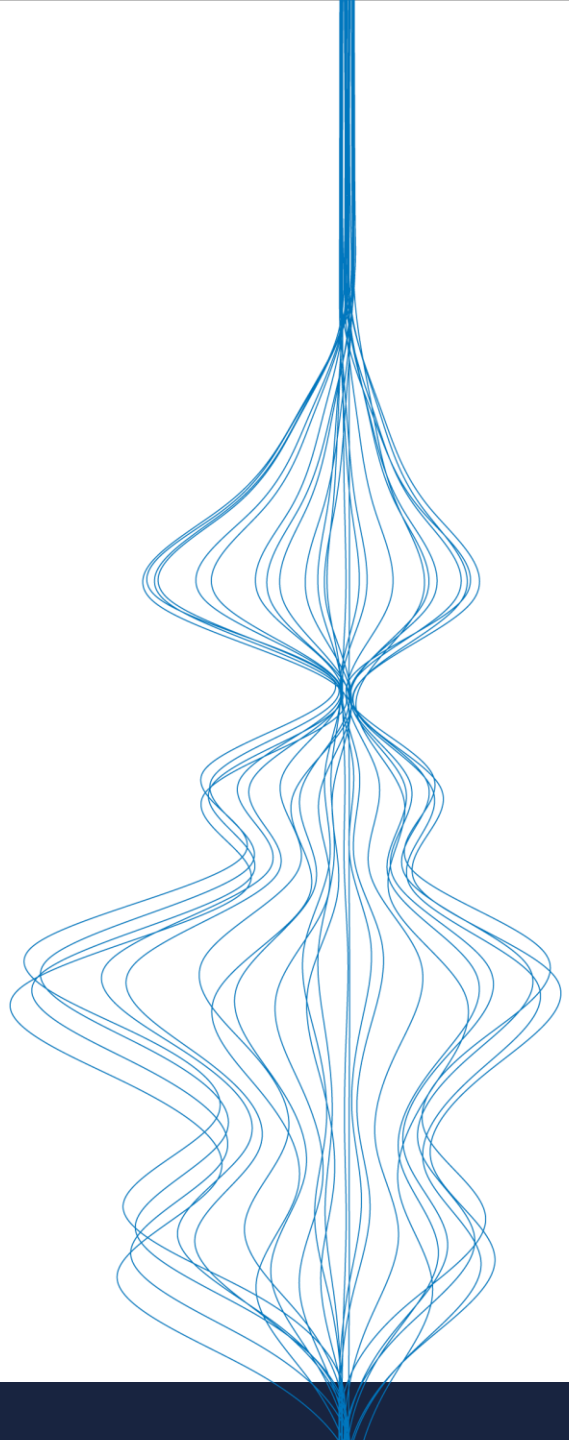
Leads to an objective assessment of "likelihood" and "severity"

**Brings consistency in assessment**

Assessment no more dependend on gut feeling and personal views

**Decreases time constraints**

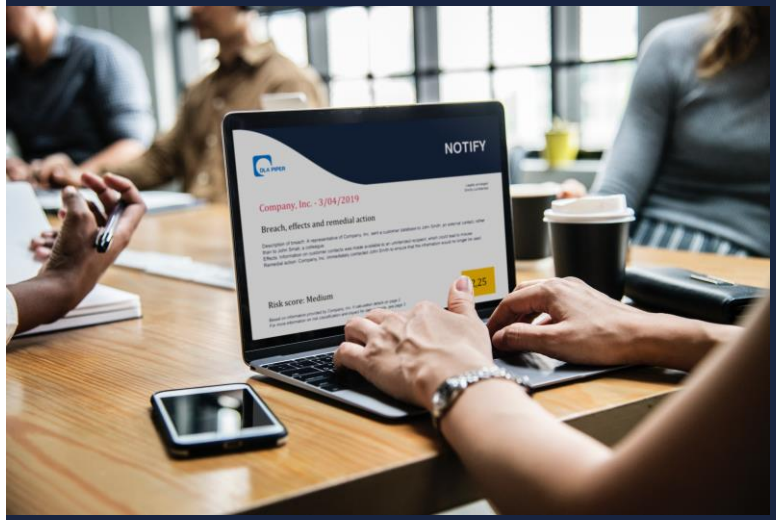
Quantitative approach to be used for a further qualitative discussion between the stakeholders

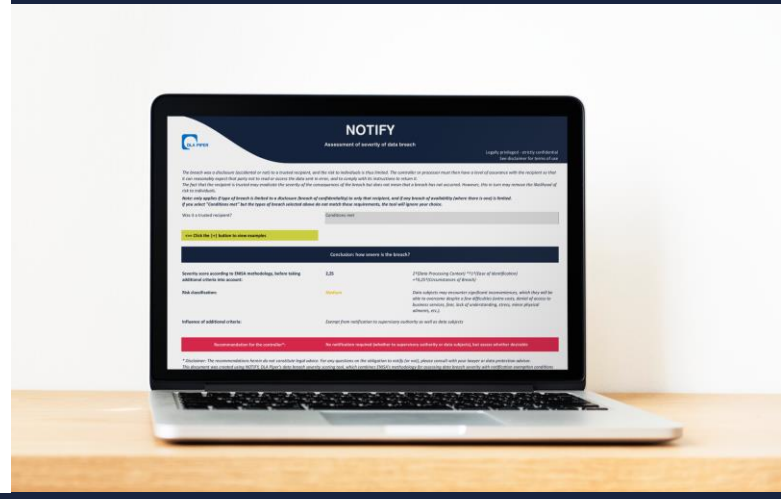


# Notify

- DLA Piper has developed an assessment tool, called Notify, allowing companies to assess the severity of a data breach using a methodology based on objective criteria sourced from official sources
  - Quantitative approach: instead of basing the assessment on ad hoc decision making and gut feeling, the tool uses a quantitative approach measuring the risk of a data breach based on an algorithm
  - Objective approach: the criteria used for building the algorithm and measuring the severity are all drawn from official sources such as the GDPR, European Network Information Security Agency and the European Data Protection Board.
  - Consistent approach: obliging the company to go through a list of questions and having the tool assess the severity based on an algorithm allows for a consistent approach, independent of the person using the tool.
  - Dramatic time savings: Using the tool brings back the severity assessment of a data breach from many hours of conversations and assessments to under one hour.
  - Automated report creation: The tool automatically creates a report that can be used for documentation purposes in line with the GDPR.
  - Free for data protection authorities: Regulatory authorities can use the tool for free

NOTIFY by DLA PIPER



# Thank you