

Data Breaches

Obligations of Controllers and Processors and Rights of Data Subjects

Prof. Dr. Norbert Nolte

14 November 2019



Freshfields Bruckhaus Deringer

Why is this all relevant?

Regulators determined to issue substantial fines

*„I think that what is important for us is to **enforce strongly and firmly** where there has been misuse of data, because if we don't use the sanctions and if we don't swing towards the pointy area of our regulation ... that means that shoddy data practices from [violating] companies are benefiting from that.“*

Elisabeth Denham, ICO

The fact that something went wrong is (preliminary) proof of failure

*„The Controller shall implement [...] appropriate technical and organisational measures **to ensure and to be able to demonstrate** that processing is performed in accordance with this regulation.“*

Art. 25 (a) GDPR

Transactions are a source of liability

*„The ICO's investigation found that Marriott **failed to undertake sufficient due diligence** when it bought Starwood and should have done more to secure systems“*

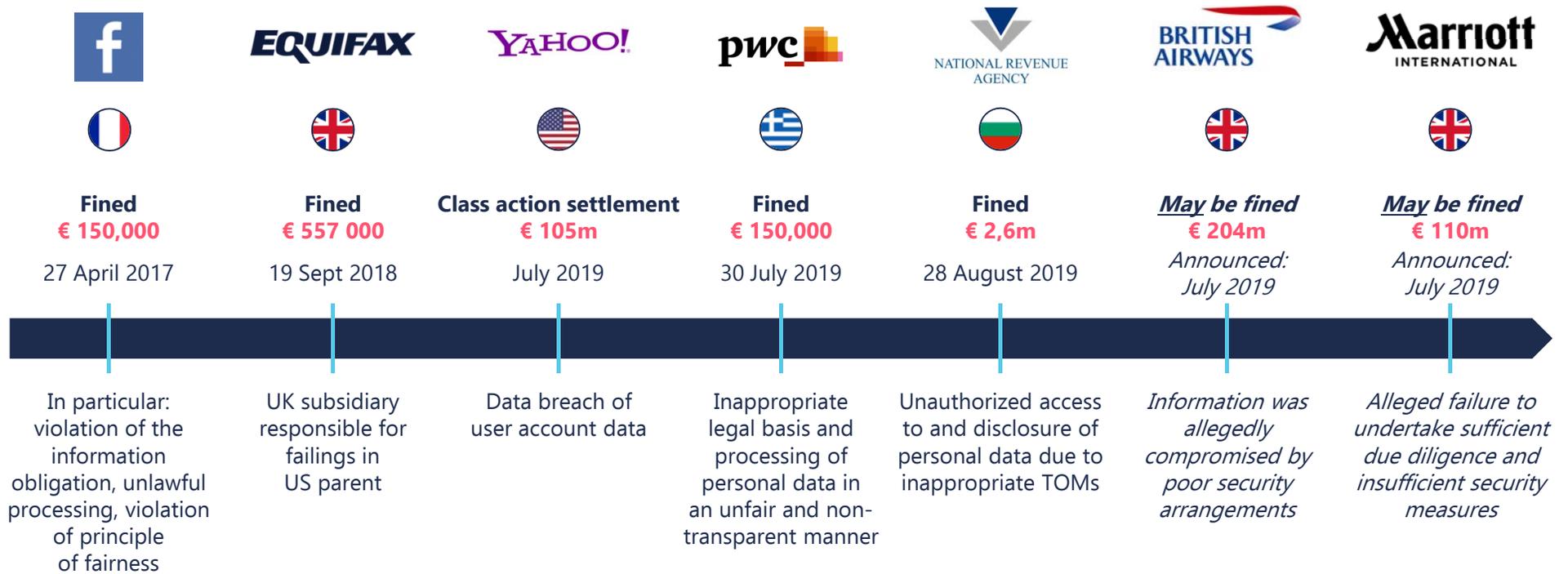
ICO, Press Statement, 9 July 2019

„If you don't think your target has both cyber and privacy risk, then you haven't spent enough time learning about your target.“

Peter Jaffe, Freshfields

Data and cyber breaches

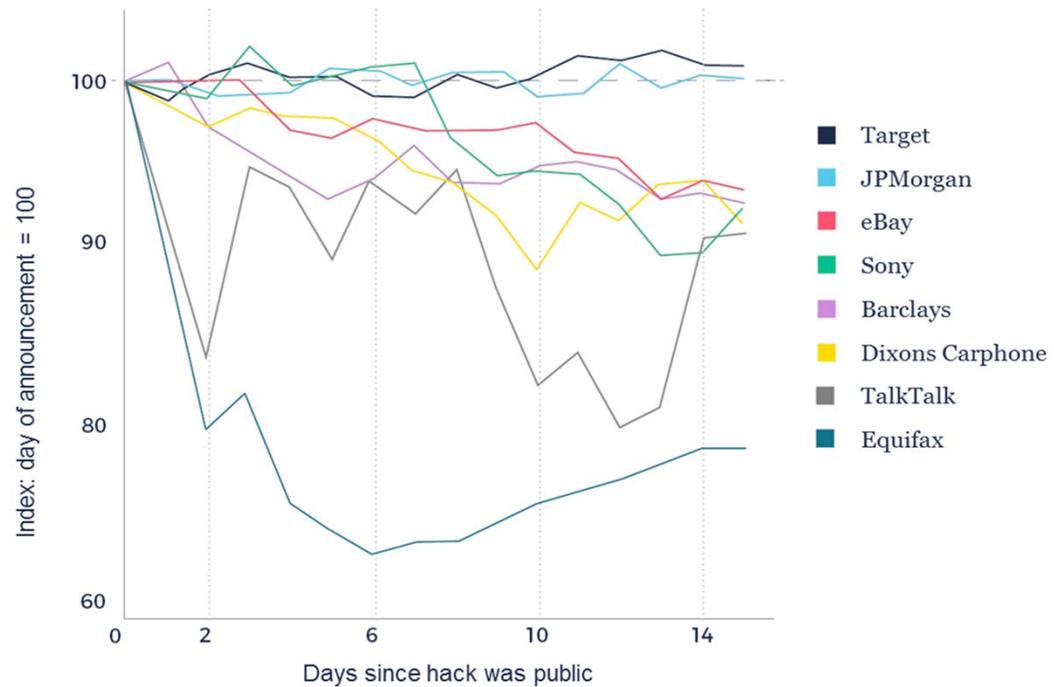
Data protection & cyber fines



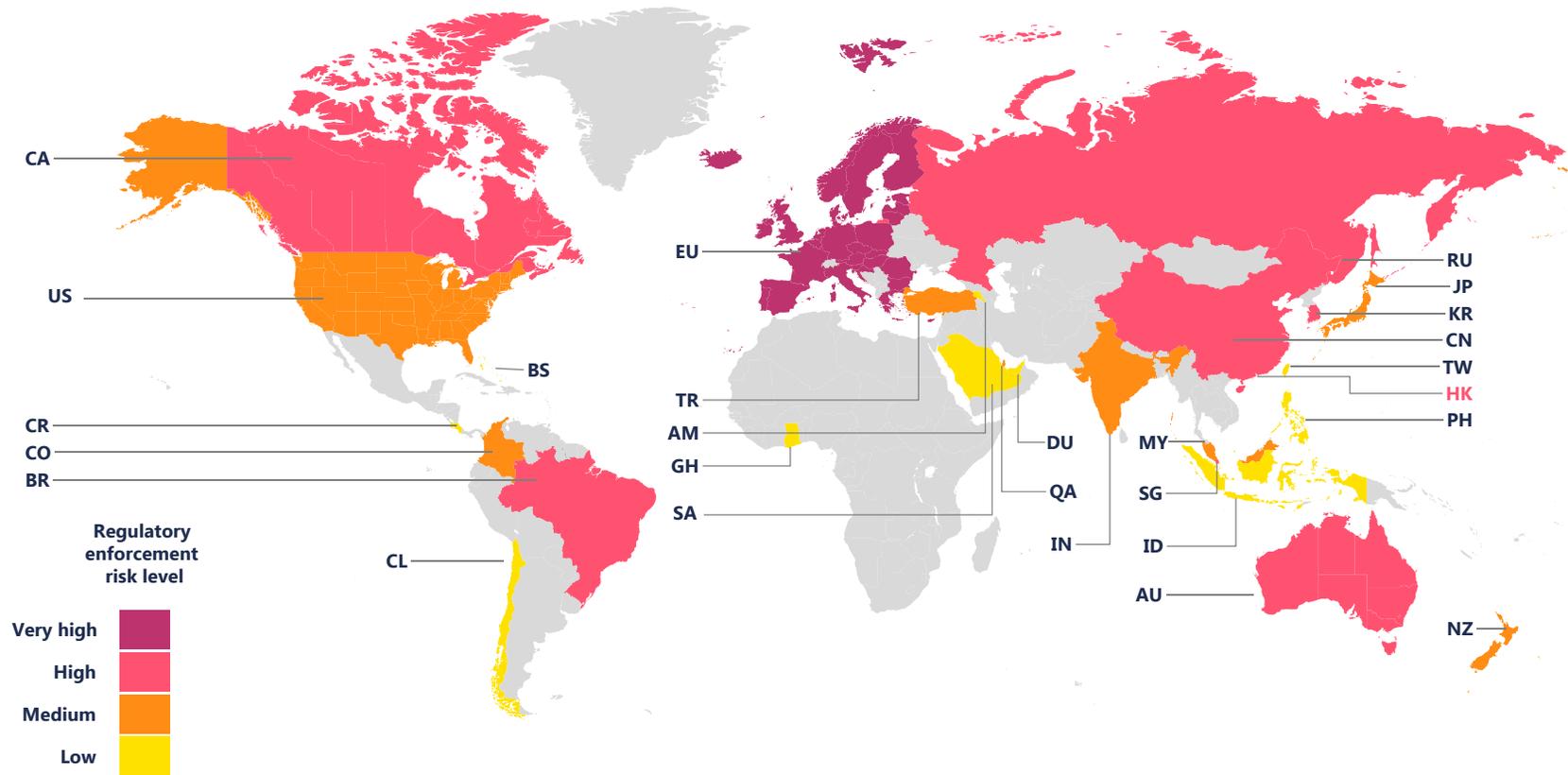
The impact of cyber incidents

From classic risks to market perception

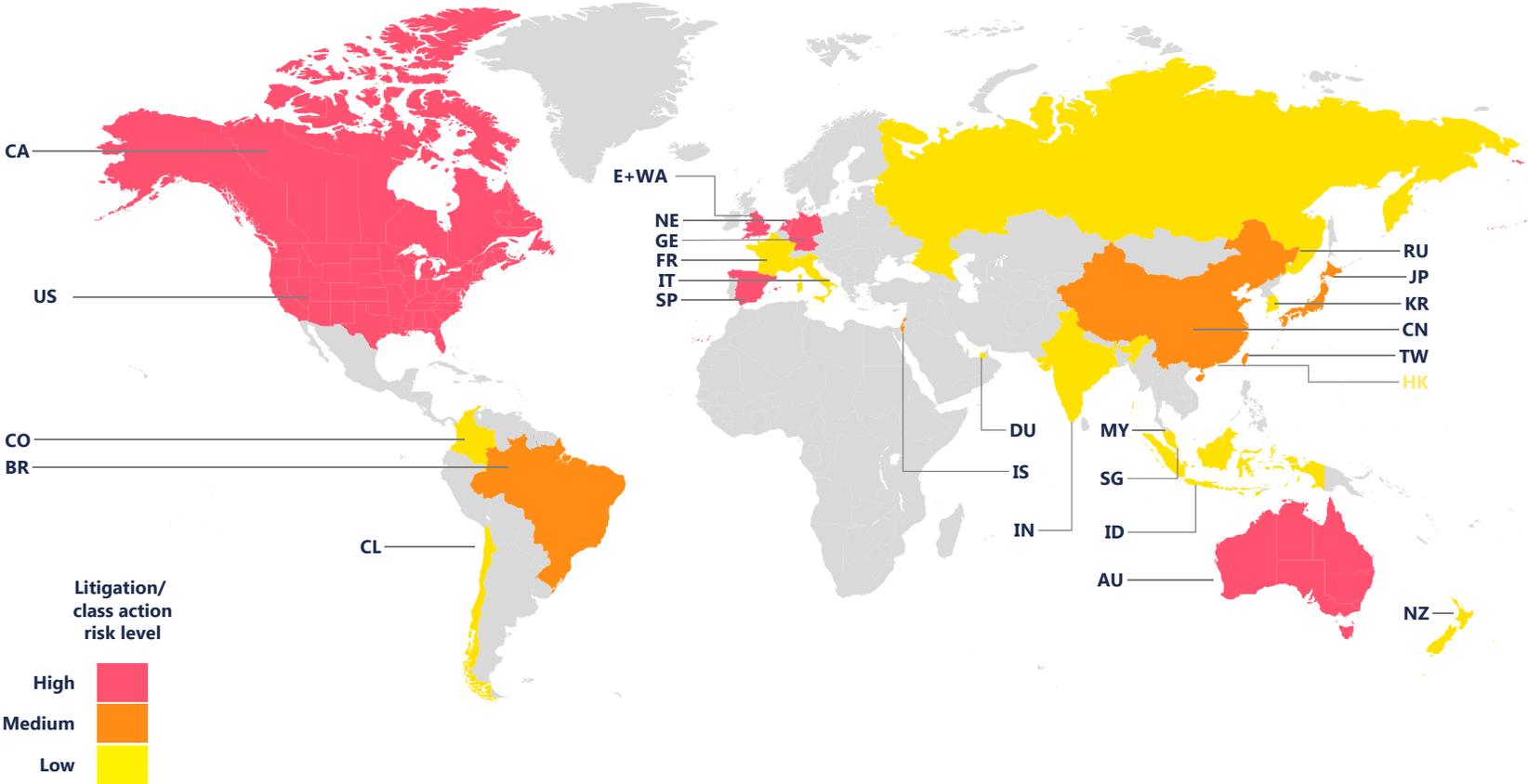
- Reputation
- Investigations
- Fines
- Litigation
- Compensation
- Resignations
- Management time
- Share / equity value



Data privacy – most active regulators



Litigation/class action risk



**Data security –
What are the controller's obligations?**

Technical security goes beyond the GDPR

GDPR

Art. 32 GDPR: Obligation to implement **appropriate (i.e. risk-based) technical and organizational measures** having regard to **state of the art technology**

- Pseudonymisation and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

NIS Directive

Art. 14 NIS Directive: Obligation of member states to ensure that operators of 'essential services' (critical infrastructures and certain digital service providers) take **appropriate (i.e. risk-based) technical and organizational measures** having regard to the **state of the art**

- Implementation by member states
e.g. Germany: sector-specific standards to be approved by BSI
- Trend: focus from collaboration between BSI and companies to enforcement (GDPR-type fines planned)

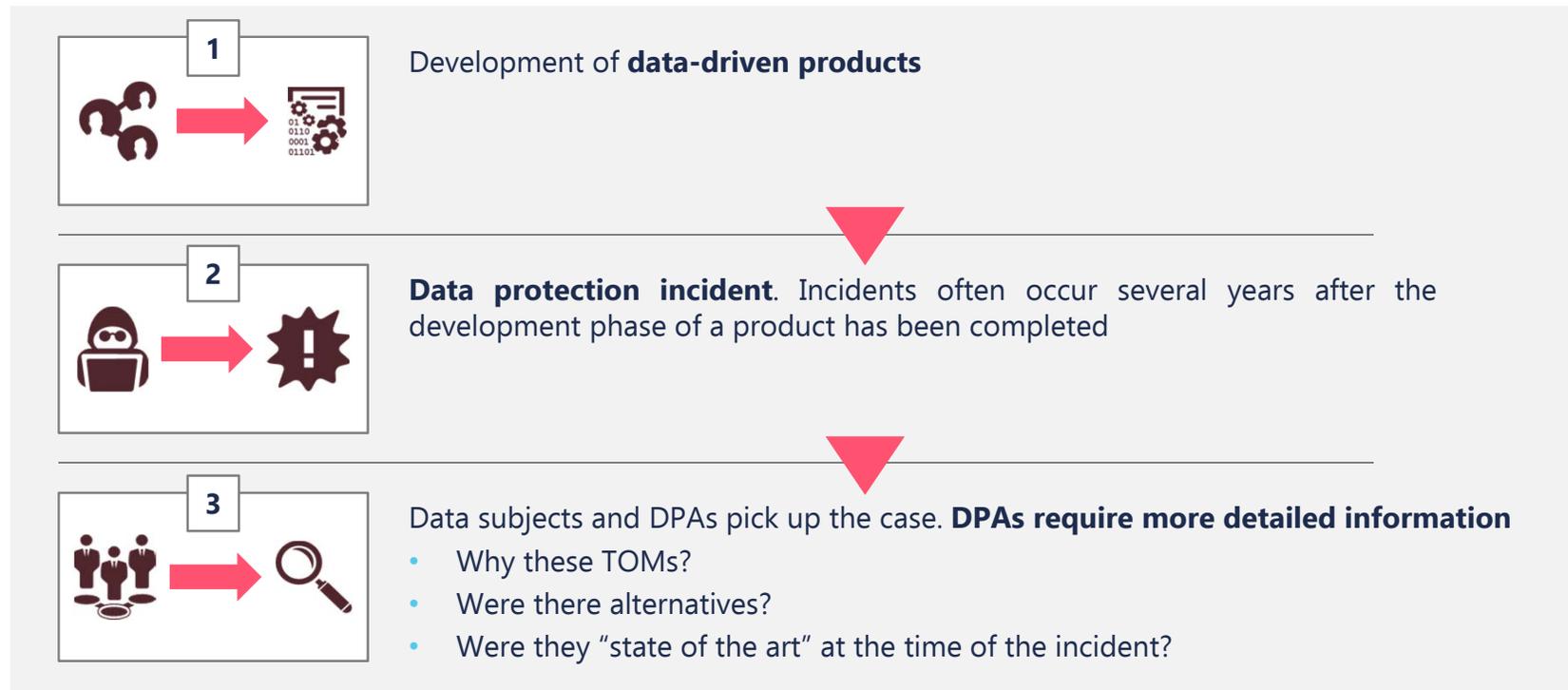
Technical and organisational measures (TOMs)

What does the GDPR say about TOMs?

What are TOMs	Technical and organisational measures to ensure a level of security appropriate to the risk (see for example Art. 32 (1) GDPR)
What should Controllers and Processors take into account when deciding what measures to implement?	<ul style="list-style-type: none">• Costs of implementation• Nature, scope, context and purposes of processing• Risks of likelihood and severity for the rights and freedoms of natural persons
What measures should be considered?	<ul style="list-style-type: none">• Pseudonymisation and encryption• Ensure confidentiality, integrity, availability and resilience• Availability and access after physical or technical incident• Regular testing, assessing and evaluating• Emergency Planning• Due Diligence

Technical and organizational measures

Adequacy & documentation of TOMs in light of practical challenges



Analysis of processing activities

Controllers have to implement technical and organizational measures to

...



- comply with, and to demonstrate compliance with, GDPR – **General Accountability** (Art. 5 (2), 24 GDPR)
- develop processes and products in a data protection compliant way, i.e. take data protection in consideration already during the development phase – **Privacy by Design** (Art. 25 GDPR)
- ensure an adequate level of data protection – **Data Security** (Art. 32 GDPR)

Analysis of processing activities

Analysis of processing activities



TOMs must be „**process-specific**“, i.e. related to the relevant processing operation. Relevant considerations for the determination of adequate TOMs include

- **Categories of data** processed (e.g. health data or only pseudonymized data from website visitors)
- **Potential risks** for data subjects (e.g. financial damages due to the loss of credit card data, reputational damages due to the loss of very private data)
- **Likelihood of damages** (probability that a risk materializes, in case of new technologies, a comprehensible, substantiated forecast is required)

 Detailed data processing registers facilitate the analysis of adequate TOMs

Determination of adequate TOMs

Determination
of TOMs
corresponding
to processing
activities



Risk-based approach, i.e. TOMs must correspond to the respective processing activity (taking into account the costs of implementation)

- If **sensitive** (like health) **data** is processed, one firewall might not be enough; in case of address lists, the second best and less expensive malware detection maybe sufficient taking into account lower risks and costs of implementation
- If personal data is **instantly deleted or anonymized**, a sophisticated process for responding to data subject access requests might not be necessary
- If personal data is processed for **marketing purposes**, a functioning consent management system might be required



Definition of TOMs corresponding to the nature and risks of the processing activity is the basis for each data protection impact assessment

Implementation of TOMs during the development phase – “Privacy by Design”

Determination of TOMs corresponding to processing activities

- **Internal guidelines and processes** for the determination and implementation of TOMs during the development phase
- Data protection compliance as a **product feature**
- Establishment of "**Privacy Gates**" in the development process

Determination of TOMs corresponding to processing activities

- **Data protection** as a **part of the product requirements**
- When **choosing between several suppliers**: Decision to purchase the “second best” product must be comprehensibly justified (i.e. by weighing risks for data subjects and costs of implementation)



Implementing TOMs in the development phase ensures marketability of products and services

Updating of TOMs

Triggers for a re-assessment



Following the implementation of appropriate TOMs, GDPR explicitly provides for an obligation to regularly review and update TOMs (Art. 24 GDPR; Art. 32 (1) d) GDPR).

- **Data breaches** revealing weaknesses of IT-security
- **Technological development**
- **Changes in the processing activity** require a new assessment of risks (e.g. processing is extended to sensitive data)
- **Cyclical review** of TOMs is considered best practice. Intervals depend on process/product life cycle



Review and update your TOMs regularly to be compliant at any time

Documentation of TOMs

Compliance with GDPR



GDPR requires data controllers to be able to demonstrate that processing is performed in compliance with GDPR principles (Art. 24 GDPR)

- Determination of TOMs is a risk-based prognosis
- Data protection authorities tend to take the view that, if a data breach occurs, TOMs – by default – were not sufficient
- This puts data controllers in a defensive position having to prove TOMs' adequacy at the time of the incident
- Documentation of TOMs and the underlying risk assessment is the basis for each data protection impact assessment



**While you cannot always prevent a breach,
you can still be prepared for it**

Documentation of TOMs

Scope	Reflect the process leading to the definition and implementation of the TOMs
Perspective	Include the assessment and the decision-making perspective to prove risk- adequacy of the TOMs
Traceability	Document decision transparently and reconstructably for lawyers and technicians
Level of detail	Include as many details as necessary to ensure traceability – even several years later

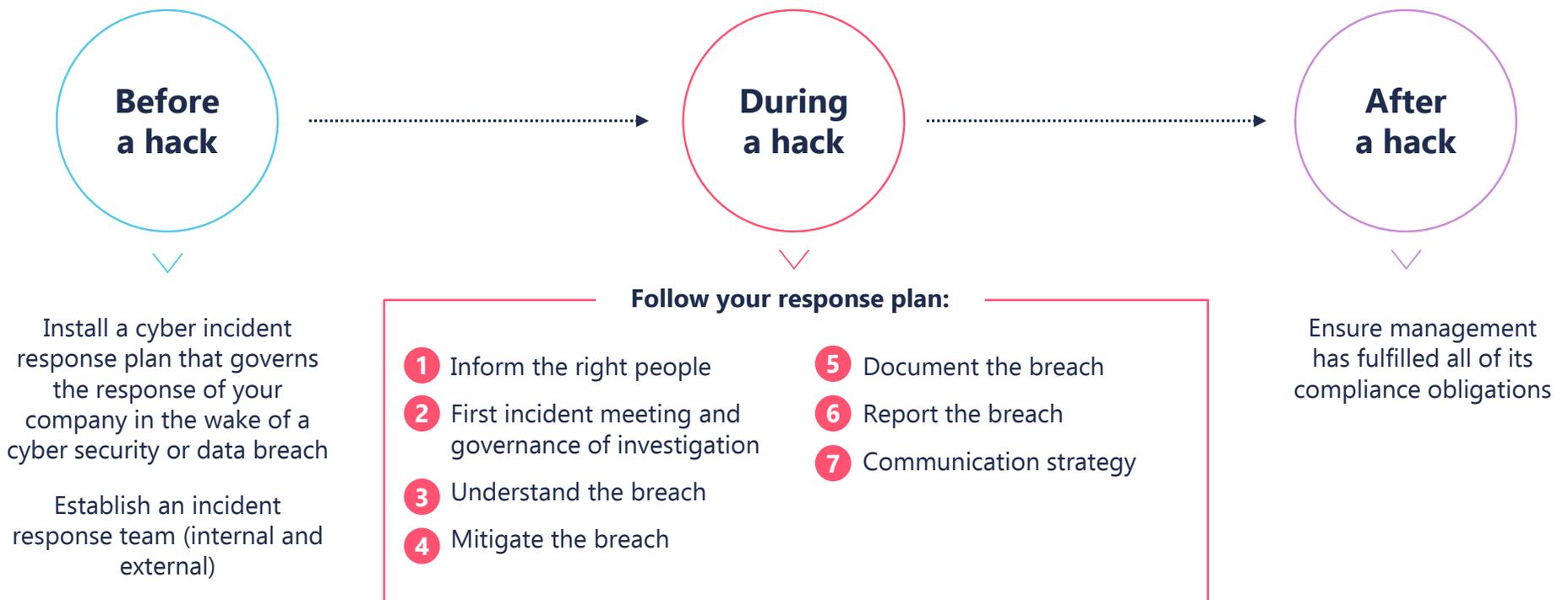
- Failure to provide necessary documentaton is an independent infringement which may lead to **fines**
- **Risks** of product recall in case TOMs are not sufficient
- **Shifting the burden of proof** to the detriment of the controller (Art. 82 (3) GDPR)
- **Reputational damages and loss of revenue**

 **Do good and document it**

What to do in case it goes wrong?

What to do before, during and after a hack

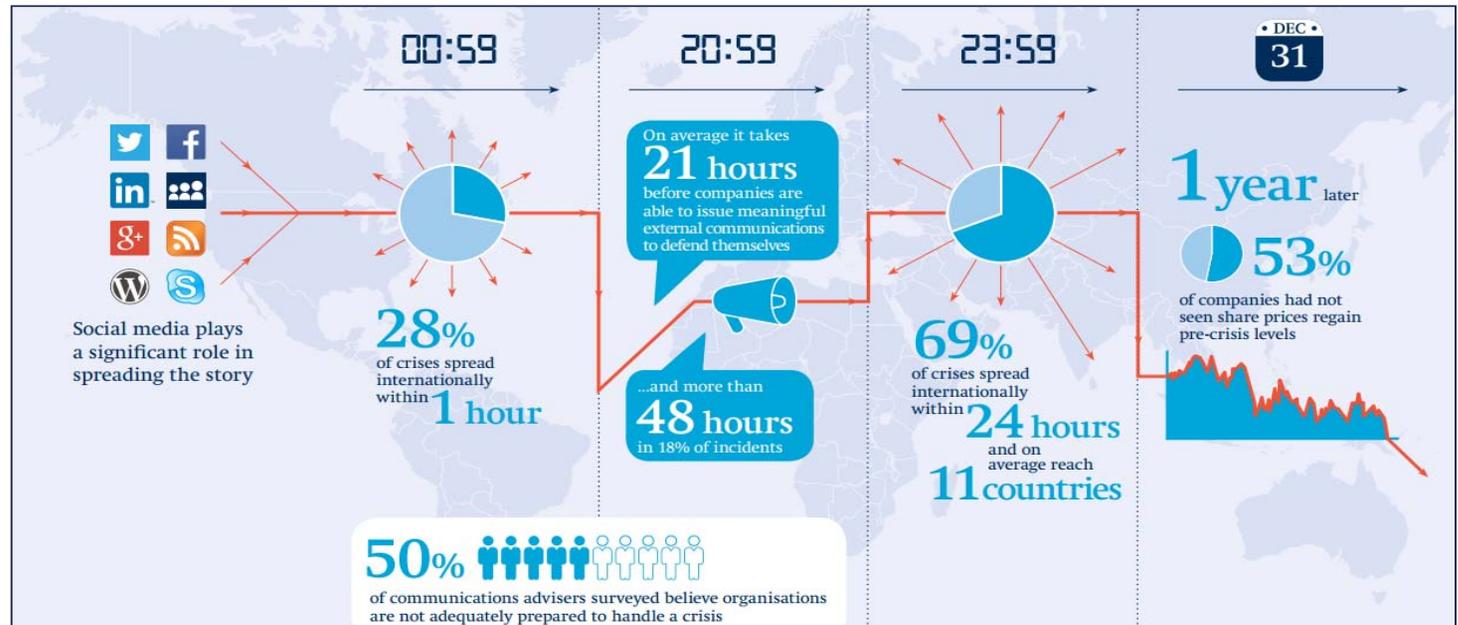
Cyber incident response planning



Responding to an incident

Why is the first 24 hours so important?

More than one-quarter of crises spread to international media within an hour and over two-thirds within **24 hours**. It still takes an average of 21 hours for companies to respond, leaving them open to 'trial by twitter'



Responding to an incident



Notification to regulators

'Without undue delay' and in any case within 72 hours of becoming aware

...unless the breach is unlikely to result in a **risk** to individuals' rights and freedoms

If later, reasoned justification required



Notification to data subjects

'Without undue delay' if likely to result in a **high risk** to them

Regulator can require notification



Notification by processors

Notification to data controllers 'without undue delay'

Notification of the data subject (Art. 34 GDPR)

Condition: likely to result in a high risk to rights and freedoms of data subject

Exceptions:

- Appropriate TOMs
- Measures to reduce risk
- Disproportionate effort (public communication instead)

Communication:

- Without undue delay
- Clear and plain language
- Details: DPO, consequences, measures

Lessons learned from recent data breaches

Cooperating with authorities in Europe

Identifying a lead supervisory authority under GDPR



Judgement Calls

- Which supervisory authorities have to be notified?
- Which supervisory authorities will receive status reports?



Preliminary considerations

- Is there a main establishment in the EU?
- Where are the affected controllers established?
- Which processes are affected by the data breach?
- Which entity has decision-making powers over the affected process?



Multiple affected authorities assert jurisdiction

- Local authorities tend to find a local angle to the breaches to establish their jurisdiction, e.g. if controller is communicating with the affected data subjects in different countries in their respective languages



Lines of defense that worked

- Decision-making powers over all affected processes are concentrated in one country, where the chosen lead authority sits
- Importance to communicate personally with authorities

Cooperating with authorities in Europe

Key documentation requirements



Authorities request documentation in great detail

Data retention concept

In most cases, hackers have had access to the system for a long time without notice. For this reason, authorities usually request the data retention concept when a breach is notified.

Technical and Organisational Measures (TOMs)

- Authorities require a high level of detail regarding the description of TOMs
- Detailed documentation of regular controls



Agreements and Contracts

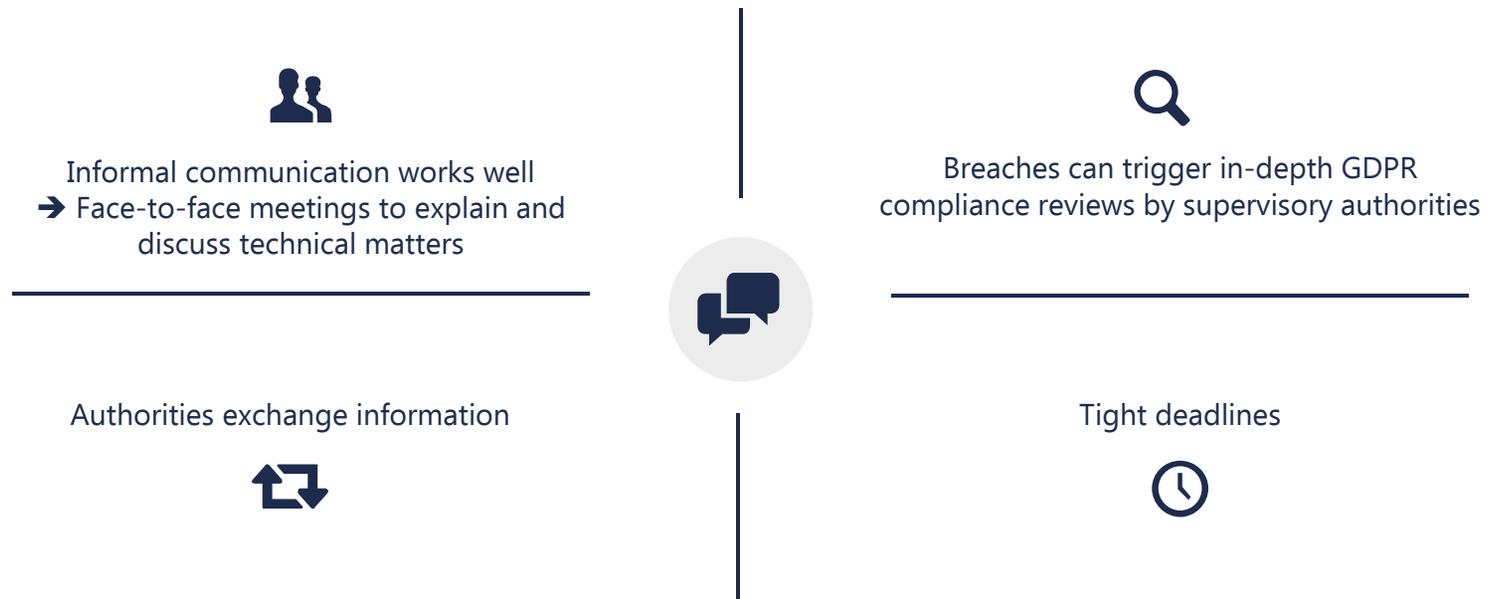
- Contracts with suppliers
 - Intra-group agreements
- Specific complexity in case of Joint Control and Data Processing agreements

Documentation of remediation

- Remediation roadmap
- Notifications (global vs local) to consumers, employees
 - Call centre bandwidth in local languages
 - Local point of contacts
 - Web monitoring
 - Credit checking
 - Data subject rights requests
 - Outsourced services (Reputation of third party vendors; Quality, incl languages; Geographical coverage; Cost; Insured?)
 - Compensation (and impact on litigation strategy)

Communicating with authorities in Europe

General lessons learned on communicating with authorities on data breaches



Communicating with authorities in Europe

Notifications and status updates



Problem

- Usually, not all facts known

Considerations

- Who has to be notified?
- Which information do we include?
- When do we have to notify?

Considerations/Judgement Calls

- Who receives status updates?
- How often do we send status updates?

Communicating with authorities in Europe

Confidentiality and privilege



Legal privilege and confidentiality

- Varying levels of legal privilege around the world
- Level of legal privilege and confidentiality dependent on context



Exchange between different authorities

- Exchange between different types of authorities, incl. law enforcement, financial supervision, cyber security supervision
- Exchange between DPAs from different countries in the EU



Strong divergence between different authority's conduct

- Regarding the type of requested documentation/information
- Regarding the level of detail requested

Judgement Call



Consistency of information given to different authorities

- Obligation to inform all authorities about every aspect or only about the points the specific authorities have requested?
- Is there a risk of follow-on investigation or will the information become publicly known anyway?

Contact



Prof. Dr. Norbert Nolte
Partner

E: norbert.nolte@freshfields.com

T: +49 211 49 79 185

Thank you

This material is provided by the international law firm Freshfields Bruckhaus Deringer LLP (a limited liability partnership organised under the law of England and Wales authorised and regulated by the Solicitors Regulation Authority) (the UK LLP) and the offices and associated entities of the UK LLP practising under the Freshfields Bruckhaus Deringer name in a number of jurisdictions, and Freshfields Bruckhaus Deringer US LLP, together referred to in the material as 'Freshfields'. For regulatory information please refer to www.freshfields.com/support/legalnotice.

The UK LLP has offices or associated entities in Austria, Bahrain, Belgium, China, England, France, Germany, Hong Kong, Italy, Japan, the Netherlands, Russia, Singapore, Spain, the United Arab Emirates and Vietnam. Freshfields Bruckhaus Deringer US LLP has offices in New York City and Washington DC.

This material is for general information only and is not intended to provide legal advice.

© **Freshfields Bruckhaus Deringer LLP 2019**