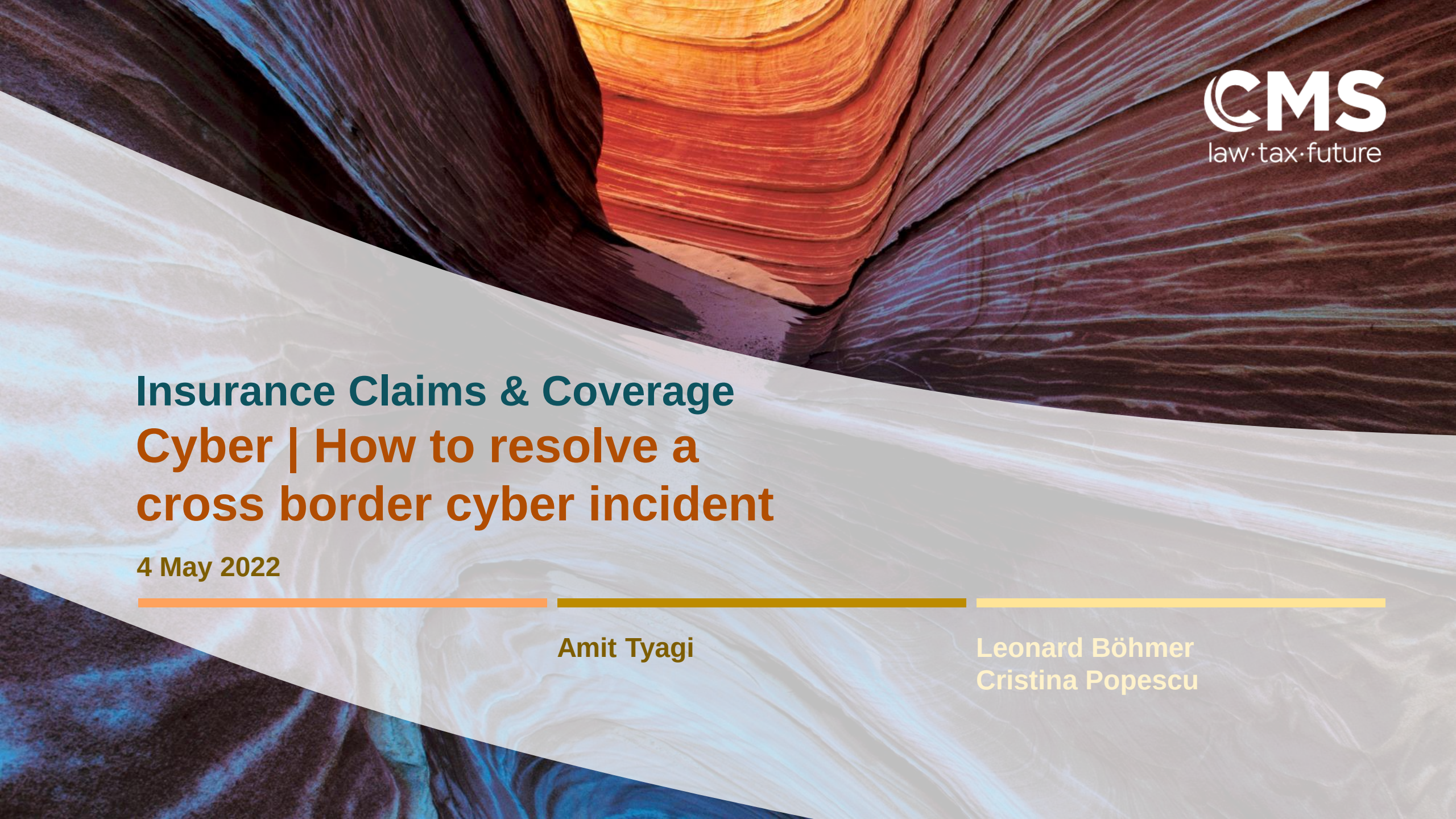


Insurance Claims & Coverage

Cyber | How to resolve a cross border cyber incident

4 May 2022

Amit Tyagi

Leonard Böhmer
Cristina Popescu

Your speakers today

Amit Tyagi | Partner
T: +44 20 7367 3578
E: amit.tyagi@cms-cmno.com

Leonard Böhmer | Partner
T: +31 30 2121 710
E: leonard.bohmer@cms-dsb.com

Cristina Popescu | Partner
T: +40 21 407 3811
E: cristina.popescu@cms-cmno.com

Introduction

- What is happening in the world of cyber?
- What does this mean in practice?
  - Increased frequency and scope of attacks
  - A rise in interconnection of incidents
  - Change in regulatory focus
  - Rise of data and other litigation
  - Hardening of the cyber insurance market

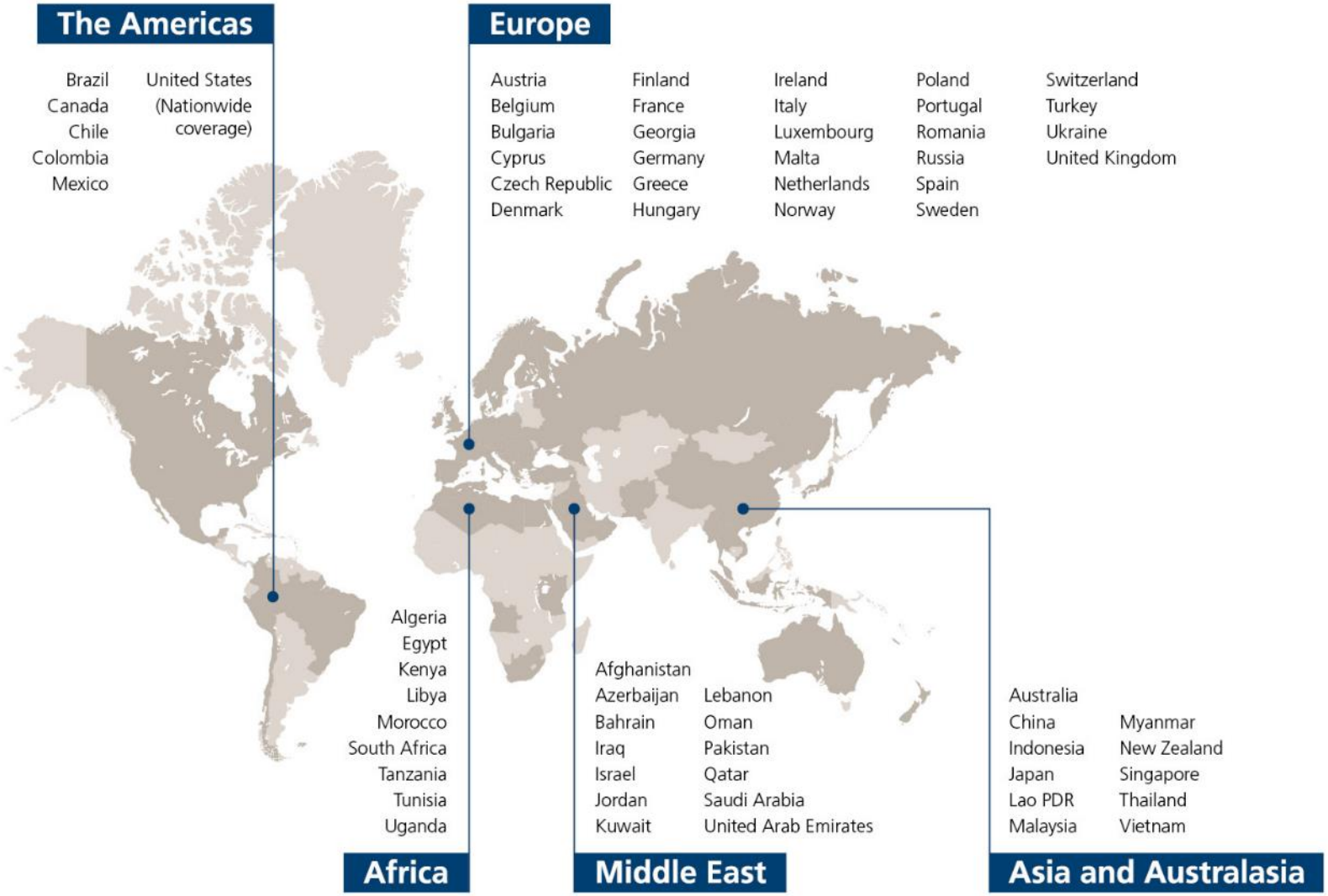
What we will cover

1. How to manage a cross border incident
2. Risks to insurers and regulatory trends
3. Managing civil claims
4. Future trends and questions

How to manage a cross border incident

Amit Tyagi

How to manage a cross border incident



24/7 365 Cyber coverage via the CMS Emergency Response Hotline and Data Breach Assistant

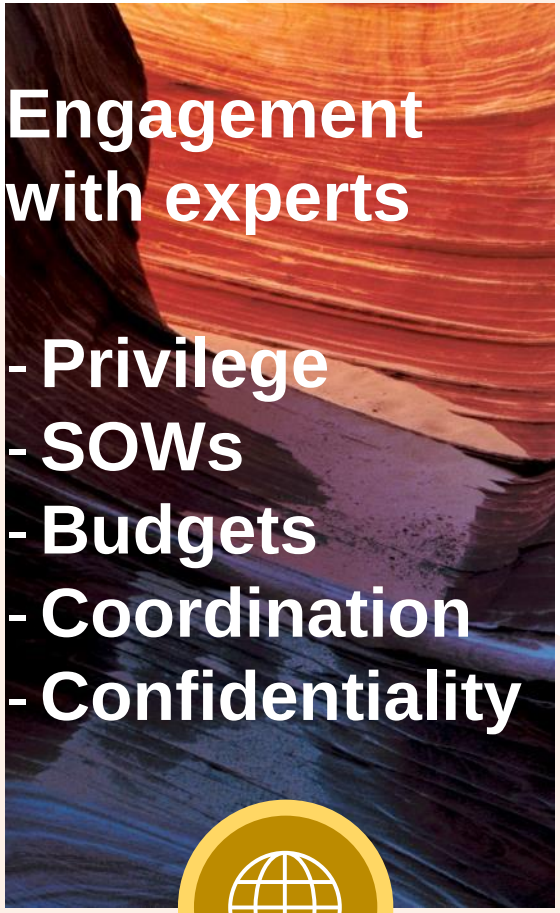
500+ Cyber incidents handled internationally to date

50+ Jurisdictions covered as part of our global cyber network

How to manage a cross border incident – Preparing

- Preparing for the worst
  - Understanding your business
  - Understanding your systems and data
  - Prioritise your risks
  - Engage with internal and external experts
  - Collaboration between Insured, Broker and Insurers

How to manage a cross border incident – Responding



Technical response

Containment

Remediation

Investigation

Ransomware negotiations?

Legal response

Assessment for notification to regulators

DPA, FCA/PRA, NCSC, Police, NIS and others

Notification to data subjects

Key commercial risks

PR and commercial response

Managing the message

Priority customers

Long tail reputation management

How to manage a cross border incident – Technical response

Containment	Protect the systems and stop further damage
Remediation	Prioritise key systems and resurrect in a safe way
Investigation	Important but not time critical for regulators, message can be managed
Reporting	Privileged? Disclosable to DPA?

How to manage a cross border incident – Legal response Personal data Notifications

Personal data breach	Notification to regulators	Notification to data subjects
• *means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*	• *"… the **controller** shall without undue delay and, where feasible, **not later than 72 hours after having become aware of it**, notify the personal data breach to the supervisory authority… unless the personal data breach is **unlikely** to result in a **risk** to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay"*	• *"When the personal data **breach is likely to result in a high risk** to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject **without undue delay**"*

How to manage a cross border incident – Legal response Notifications

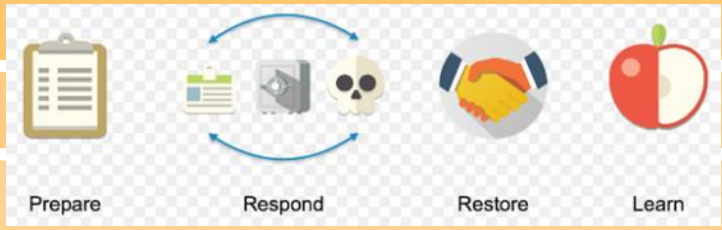
Notification to regulators	Other notifications
Coordinated approach	NIS for OES and RDSPs
Use of the “one stop shop” regime within EU	FCA/PRA for financial services companies
Position of “third countries” such as the UK	Industry specific notifications and customers
Always be consistent	

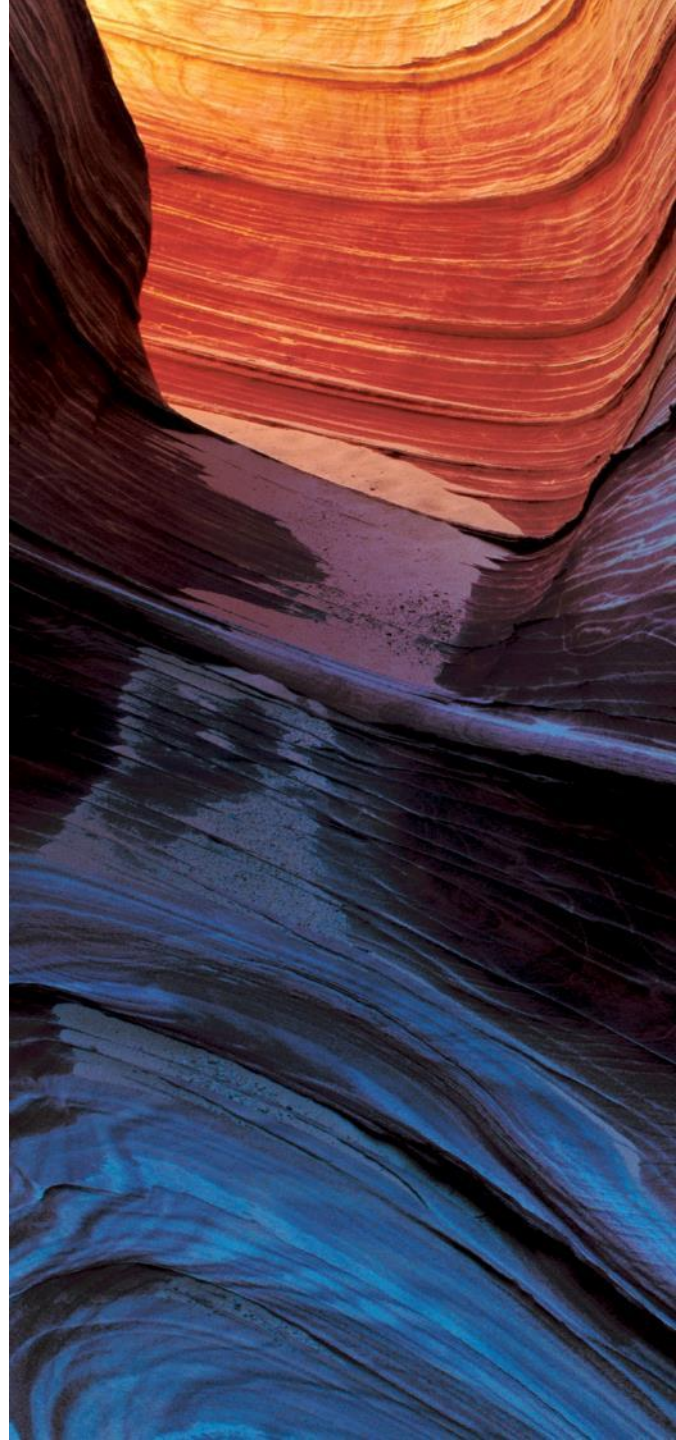
How to manage a cross border incident – Legal response Regulatory investigations and litigation

Investigations by DPA	Data litigation	Other civil litigation
• *"One stop shop regime" for investigations and enforcement action* • *Procedure governed by international and local law* • *Fines and penalties*	• *"Nuisance" claims by individual data subjects* • *Class action/group litigation claims* • *Don't forget about non cyber data breach claims*	• *Failure to comply with commercial terms* • *"Supply chain" litigation and multi-party disputes* • *Recovery claims vs. suppliers and MSPs*

Practical tips

- Stay calm
- Involve the right people (maintain privilege)
- What is the risk?
- How can we manage the risk? Be proactive - Identify a route map to resolution
- Record all decisions (Insured, insurer, broker, technical consultants)
- Consider action/claims against parties responsible for the incident
- Consistent messaging and contain the spread of information
- Conduct a lessons learned
- Produce a report for the board
- Update IT systems





Risks to insurers and regulatory trends

Cristina Popescu

Cyber risk and the insurance industry

– <u>Insurers are natural targets for cyber-attacks</u>
  - increasing frequency and sophistication of cyber-attacks
  - digital transformation
  - new technologies
  - Big data

» They possess substantial amounts of confidential policyholder information (including sensitive/special data)!

Yet, less than one-in-five CEOs of insurance groups believes that their organisation is fully prepared for a cyber-event!

What are the risks?

Identity theft	Policyholder information in the wrong hands
Business disruption	Systems affected impacting operations (both for existing policies and for underwriting new business)
Financial impact	Estimated between 0.002% and 10% of the own funds of the insurance undertakings
Reputational damage	Irreversible, a “label” difficult to get past

Regulatory approach to cyber risk

Regulations	EIOPA Guidance	In the making
•*Solvency II Directive* •*Delegated Regulation* •*General Data Protection Regulation* •*NIS Directive**	• *EIOPA Guidelines on information and communication technology security and governance* • *EIOPA Guidelines on outsourcing to cloud service providers*	• *Introducing…**DORA!*** • *DORA – the EU's Digital Operational Resilience Act for the financial services* • *Expected to be finalised by end of 2022* • *Compliance required 12-18 months later*

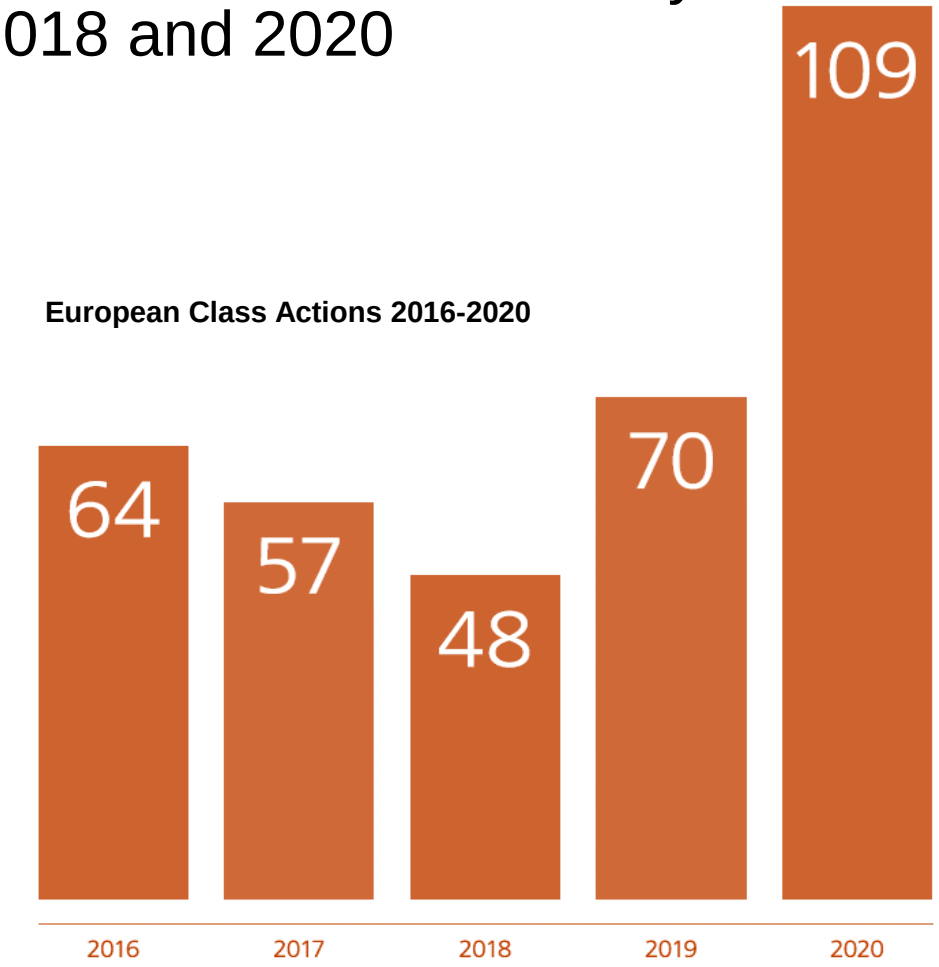
But….is it enough to address cyber risk?

Litigation trends and risks

Leonard Böhmer

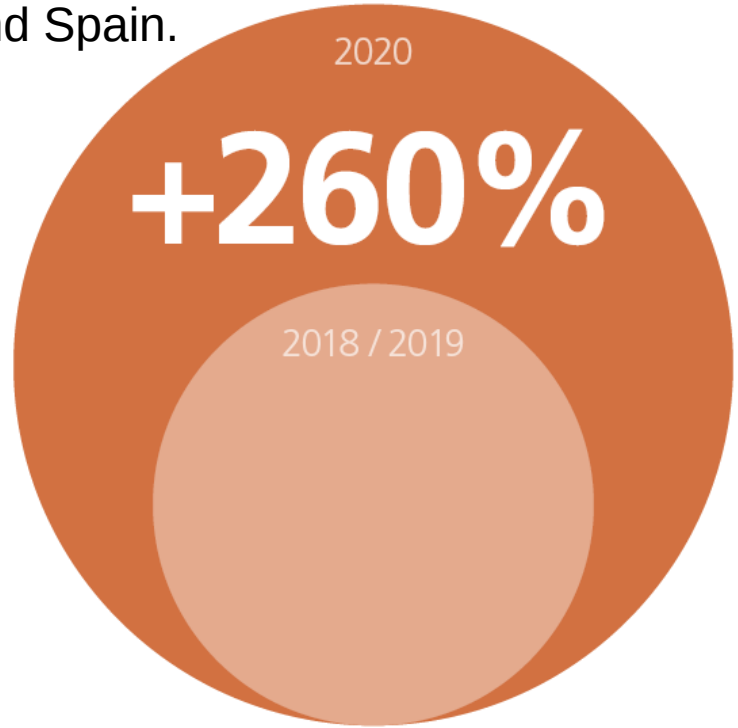
Increasing in class actions in Europe

– The number of class actions filed increased by over 120% between 2018 and 2020

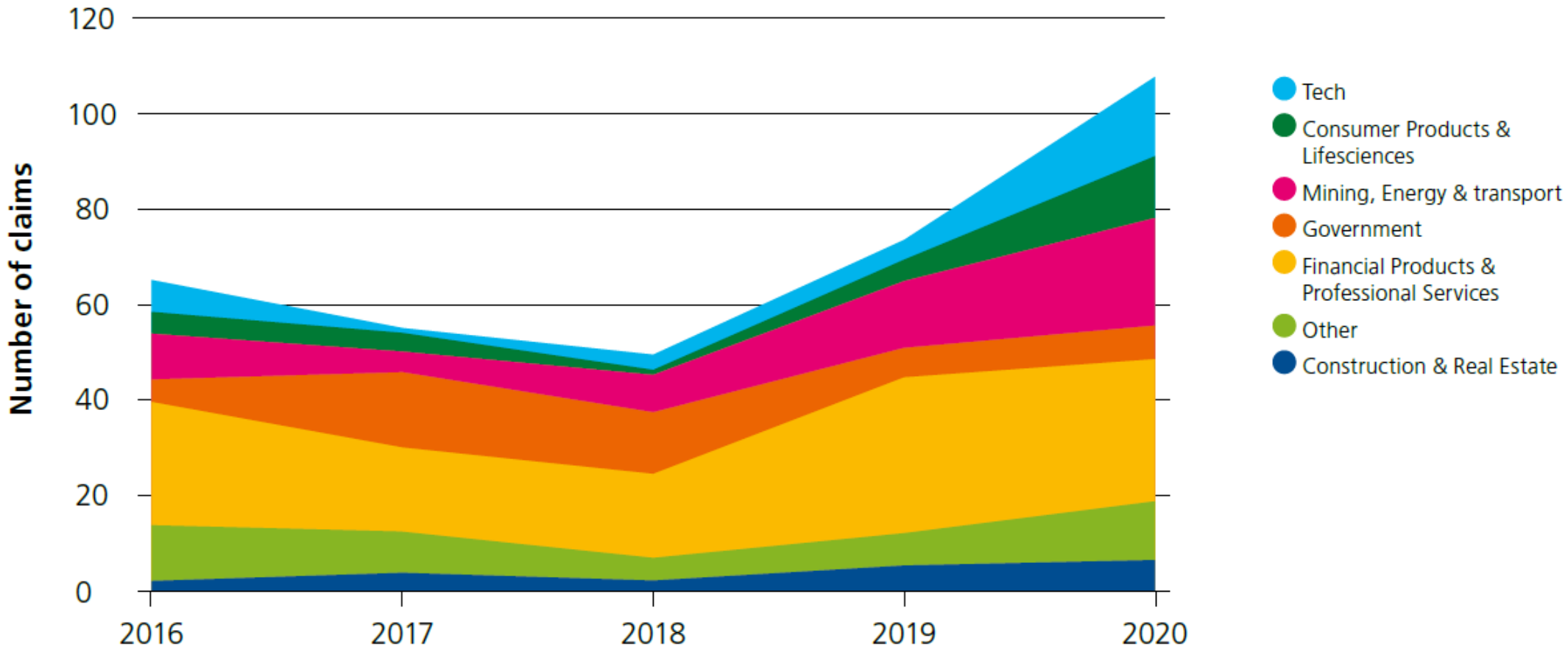


Class actions against the consumer sector (Europe)

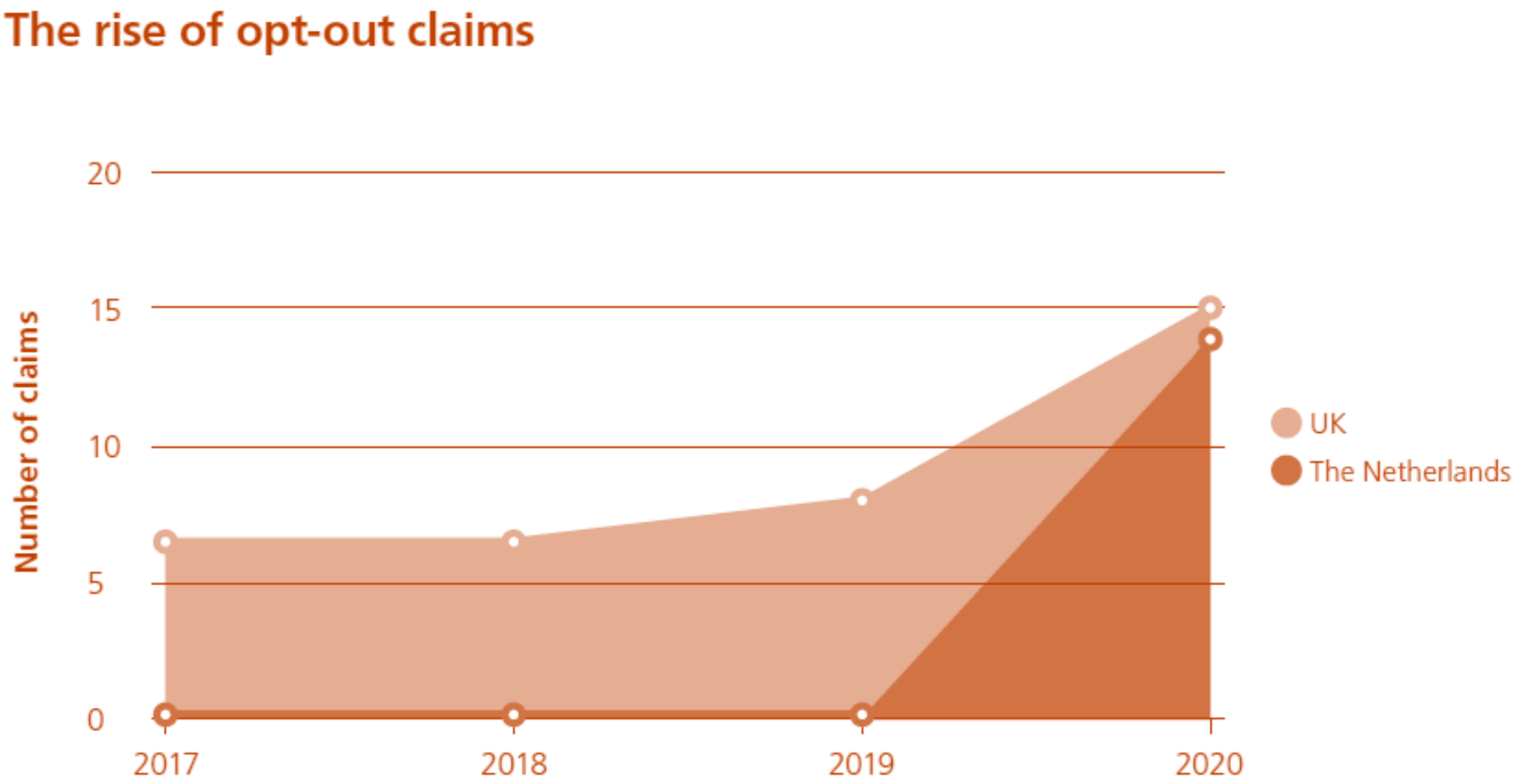
- Class actions against the consumer sector across Europe have increased with almost 3 times the number of claims filed in 2020 as in 2018 (i.e. growth of 260%). This is being driven by claims in the UK, Germany, the Netherlands and Spain.



Defendant sector trends



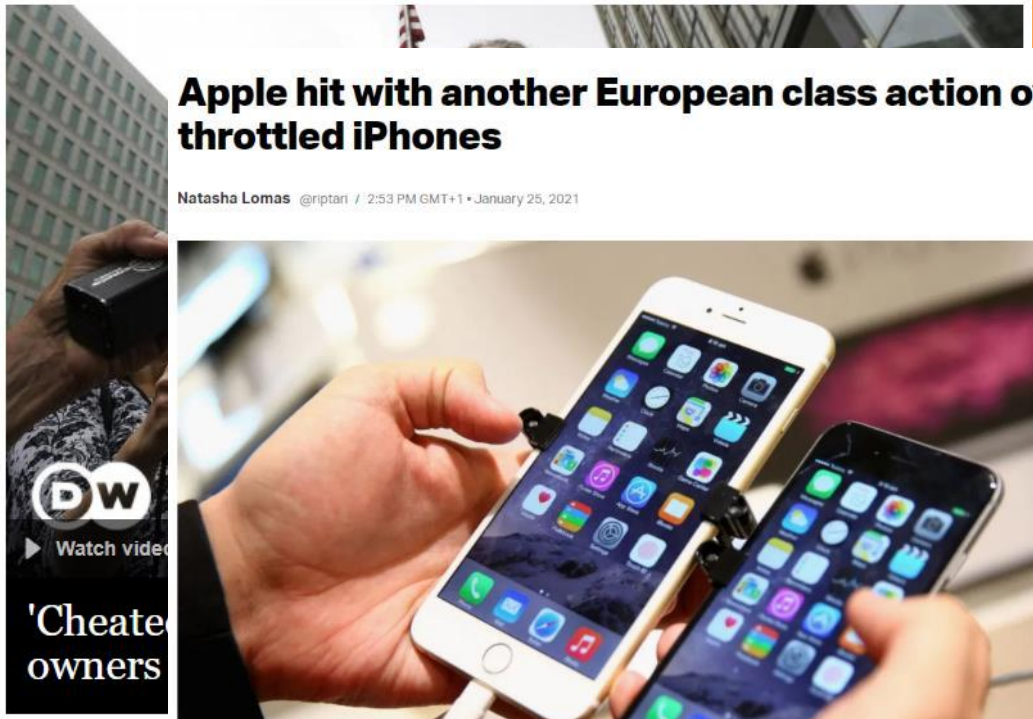
The rise of opt-out claims in 2121: 31 recorded



BUSINESS

German class action lawsuit over VW emissions begins

Four years after Volkswagen's Dieselgate scandal broke, more than 400,000 Germans are part of fresh legal action against the carmaker. But some lawyers warn against joining Germany's first-ever class action lawsuit.



Apple hit with another European class action over throttled iPhones

Natasha Lomas @riptari / 2:53 PM GMT+1 • January 25, 2021

Comment

Banks face fresh collective action over forex manipulation

Specialist litigation firm Hausfeld latest to launch suit on behalf of investors

BT faces £600m lawsuit over 'overcharging'

By Mary-Ann Russon
Business reporter, BBC News

18 January

Why is risk increasing?

Drivers for increased risk

New procedures

- Representative Actions Directive
- National procedures

- New claimant law firms
- More litigation funders

Collective Redress across Europe

UK

- Highly developed claimant market
- Opt-out devices available for antitrust and data protection claims (subject to appeal)
- Sophisticated opt-in devices
- Large claims are advertised

Netherlands

- New law (Jan 2020) allowing representative actions.
- Opt-out available for Dutch claimants.
- Contingency fees prohibited.
- Courts will scrutinise funding arrangements.

Germany

- 2018 law extended regime to allow QE actions on declaratory judgments.
- Consumers can seek damages on basis of judgment.
- Also: multi-party actions, representative actions, assignment of claims.
- No regulation of funders.

France

- 2016 law extended regime scope to include data protection, environmental liability and discrimination.
- Third-party funding is rare.
- Only licensed associations can bring claims.

Spain

- CR Directive would require significant modifications to law.
- No collective redress mechanism, but specific procedural rules.
- No certification process.
- Third party funding uncommon.

Representative Actions Directive

- Came into force in December 2020
- Requires MSs to have “minimum procedural standards” for collective redress for consumer claims
- Opt-in device must be available; MSs can permit opt-out device
- Claims will be brought by Qualified Entities
- Categories of available claims include:
  - Unfair terms in consumer contracts (93/13/EEC)
  - Product liability directive (85/374/EEC)
  - GDPR (2016/679)
- MSs have 24 months to adjust domestic law; then 6 months to bring into force

Measures to consider – data protection
Be aware of local issues and peculiarities

Type of prophylactic measure	Action	Comment
Scoping risk	High level mapping on shape and nature of risk	Consider: • Types of potential GDPR claims beyond data breaches • Higher risk jurisdictions
	Update risk assessment on data processing	Does class action risk require re-evaluation
Reducing risk	Ensure supply chain (controller/processer) arrangements minimise risk	Controller can be liable for failings of processors – unless “not in any way” responsible
	Internal awareness/training	Behavioural change reduces risk
	Review insurance coverage	Is class action exposure covered?
Readiness	Holistic data breach response plan	Litigation readiness should be part of response plan • Risk mapping more accurate (geography and class action device) • Narrative is important
	Ensure consistent messaging with regulators and in litigation	Driven by risk mapping
Macro measures	Lobbying/shaping detail of mechanisms	

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Beirut, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sheffield, Singapore, Skopje, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

cms.law