Bird & Bird LEXOLOGY

Mass Claims, Data Breaches and Fear of Data Subjects – Unpacking Recent Legal Milestones in Data Protection Case Law

21 February 2024

Speakers

Dr. Simon Assion

Partner

simon.assion@twobirds.com

James Moss

Partner

james.moss@twobirds.com

Evelyn Tjon-En-Fa

Partner

evelyn.tjon-en-fa@twobirds.com

Introduction – How does it all fit together?

Partner

James Moss
UK

Introduction – How does it all fit together?

Article 82 GDPR – Right to Compensation and Liability

*82(1) Any person who has suffered **material or non-material damage** as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*

82(3) A controller or processor shall be exempt from liability - if it proves that it is not in any way responsible for the event giving rise to the damage.

Case C-340/21 VB v Natsionalna agentsia za prihodite

What constitutes non-material damage

"Can the unlawful dissemination of personal data held by a public agency, as a result of a hacking attack, give rise to compensation for non-material damage in favour of a data subject ***merely because the latter fears a possible misuse of his or her data in the future?"***

Case C-687/21 BL v Media MarktSaturn Hagen-Iserlohn GmbH

"the concept of 'non-material damage' encompasses a situation in which the data subject experiences ***the well-founded fear,*** *which is for the national court to determine, that some of his or her personal data be subject to dissemination or misuse by third parties in the future"*

Hacking Attacks & Data Breaches

UK Government Data

- A third of businesses (32%) report having experienced some form of cyber security breach or attack in the last 12 months
- larger businesses are more likely to identify breaches or attacks than smaller ones
- Four percent of businesses reported outcomes that resulted in personal data being altered, destroyed or taken.
- Around 18,500 incidents involving personal data each year.

Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

What do data subjects know?

And when do they know it…

A.34(1) 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**

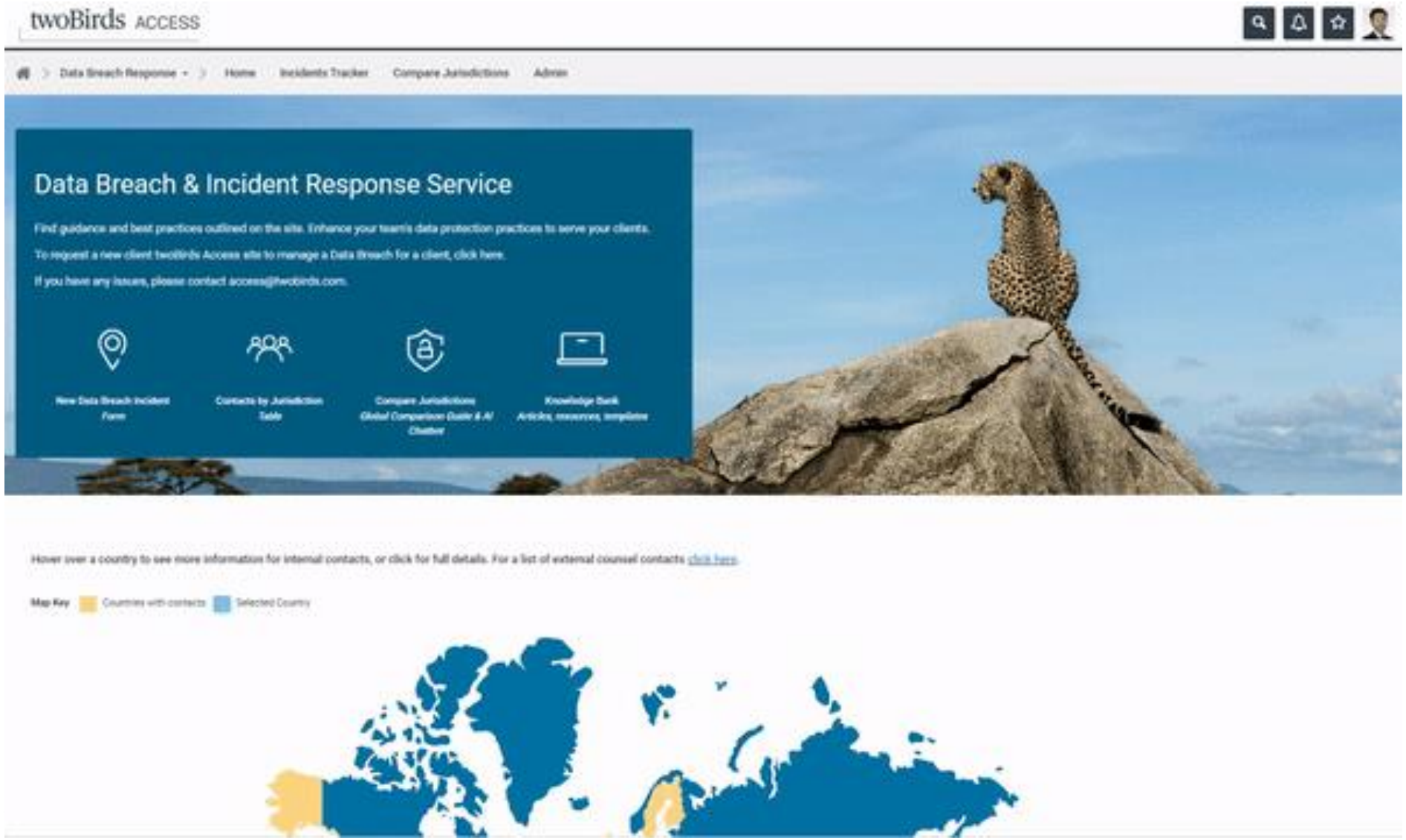
"The GDPR states that communication of a breach to individuals should be made "without undue delay,"

which means as soon as possible. *The main objective of notification to individuals is to provide specific*

information about steps they should take to protect themselves"

edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf (europa.eu)

Dealing with Data Breaches



Recent case law and data breaches and (mass) claims

CJEU and German courts

Partner

Dr Simon Assion
Germany

A lot of new case law

CJEU, 4 May 2023, C-300/21, *Österreichische Post*

CJEU, 14 December 2023, C-340/21, *Natsionalna agentsia za prihodite*

CJEU, 14 December 2023, C-456/22, *Gemeinde Ummendorf*

CJEU, 25 January 2024, C-687/21, *MediaMarktSaturn*

CJEU, 21 December 2023, C-340/21, *Krankenversicherung Nordrhein*

Key take aways from the new CJEU case law (1)

1) **Is a data (security) breach also a breach of the GDPR?**

   - No, even organisations with appropriate security (Art. 32 GDPR) can become victims of a data breach.
   - But the burden of proof rests on the organisation.
   - Document the IT security measures of your organisation on an ongoing basis, and if possible, get clear proof

2) **What are the conditions for a damages claim under Art. 82 GDPR?**

   - (1) Breach of the GDPR; (2) Damage; (3) Causality; (4) Culpability

3) **What is a 'non-material damage' in the meaning of Article 82 GDPR?**

   - Infringement of the GDPR ≠ damage. There must be "negative consequences" - "however minimal"
   - Includes a "loss of control" (but what does that mean?)
   - "Fear" of a potential misuse of the data *can* be a damage (not: is a damage)

Key take aways from the new CJEU case law (2)

4) Who must prove that there was a damage?

- Burden of proof rests on the data subject
- In case of "fear" as damage, the national court must assess whether "fear can be regarded as well founded, in the specific circumstances at issue and with regard to the data subject"
- In other words: A "fear" is only a damage if it is, in the concrete case, well-founded
- A "purely hypothetical risk of misuse by an unauthorised third party" is not a well-founded fear
- Therefore, a data subject cannot just "invent" a fear, in the hope of making easy money

Key take aways from the new CJEU case law (3)

5) Culpability

- CJEU has now confirmed that culpability is a condition for a damages claim
- By 'culpability' the CJEU likely means intent and negligence
- Do not expect too much – exculpation will be very difficult (Art. 82(3) GDPR: "not in any way responsible")

6) Amount of the damage

- Clear since the *Österreichische Post* decision that national courts have discretion
- As a result, the same "damage" can lead to different amounts of compensation – depending on the jurisdiction
- Boundaries: EU principles of effectiveness and equivalence (meaning that CJEU reserves the right to stop outliers)
- Amount of compensation depends on the damages suffered.
- Not relevant: (1) Degree of culpability (except of maybe co-culpability of the data subject); (2) punitive damages

How high is the actual risk? (1)

- Risk is a function of damage and probability

Damage:

- Damage in this case is a multiplication of compensation + number of potential claimants
  - Very severe damage with one affected claimant: 10k EUR x 1 = 10k EUR
  - Small damage with 50 million claimants: 100 EUR x 50 million = 5 billion EUR
- This means that the real risk here applies in data processing activities that affect very large groups of data subjects
  - For example data breaches concerning the customer database
  - For example a data processing activity that affects every user/customer of a large business model (e.g. fraud prevention, CRM)
  - In such cases, the risk is higher than that of GDPR fines

How high is the actual risk? (2)

Probability:

- In which situations can it come to large-scale claims for damages?
- Currently two potential avenues for such mass claims:
  1) Legal tech-based law firms trying to use technology to file mass claims;
  2) Legal framework for 'class-actions' based on the EU Representative Actions Directive or other laws
- **'Legal tech' mass claims** have the problem that fears must be "well-founded" in the specific circumstances and demonstrated by the data subjects.
- German Higher Regional Courts have dismissed multiple damage claims after the Meta data scraping incident, stating that automated "boilerplate" descriptions of fears were not sufficient
- **'Class actions'** under the Representative Actions Directive are different, because they allow a mechanism for "standardised" calculation of damages (via settlements or through a court order)

The Growth in Consumer Class Actions

From an EU-centric perspective

Partner

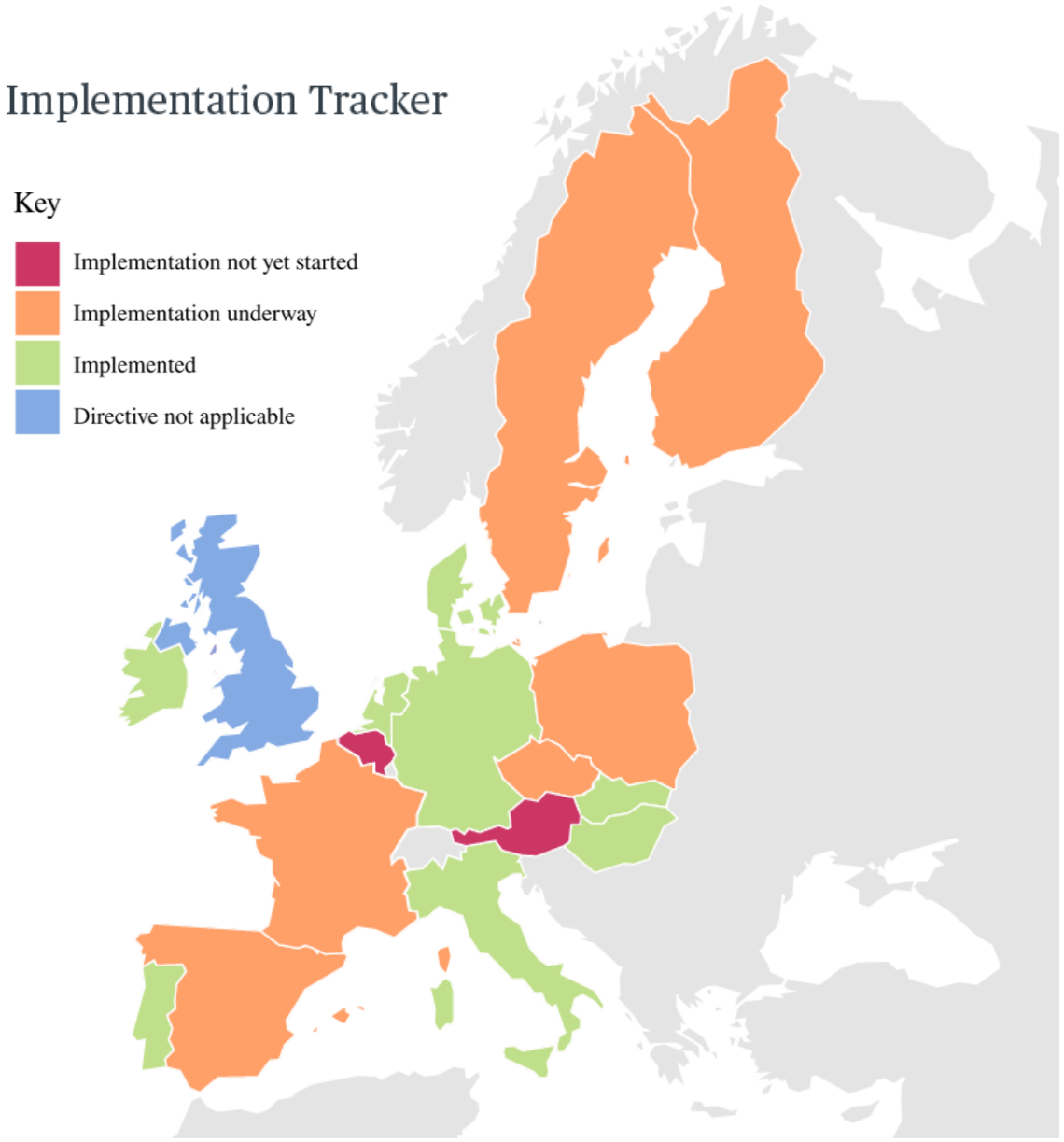
Evelyn Tjon-En-Fa
The Netherlands

Mass Claims on the Rise

- New consumer rights at national and European level
- Recent court cases and progressive legislation
- Well-developed mass claims regimes:
  - The Netherlands: Act on the Settlement of Mass Damages in Collective Action
  - Portugal: lawsuits against big tech companies
- Less developed regimes:
  - Safer havens for businesses

EU: Representative Actions Directive

- Entered into force 24 December 2020
- Prescribes minimum requirement of implementing an opt-in class action mechanism
- Actions can be brought domestically and cross-border
- Claimant groups can seek redress measures
- Member States are now in the process of evolving their national mass claims mechanisms
- Directive sets out first standardised framework for collective suits – encourages more class actions



Forum Shopping

Distribution of consumer class actions

- Litigating parties will bring their proceedings to favourable jurisdictions
  - Few States receiving the majority of consumer class actions
- Third-party litigation funding
  - European Parliament urged to regulate risks by:
  1. Introducing a new licensing system, and
  2. Curtailing maximum proportion of compensation allocated to the litigation funder
  - European Parliamentary Research Service: litigation funders demand disproportionate shares (20-50% of the proceeds)

Mass Claims and Data Protection

Digital regulations which will shape consumer litigation

What is shaping consumer claims today?

General Data Protection Regulation

- Ongoing consumer class actions on data protection claims rest upon obligations set under the GDPR
- As of 2023: 10 pending GDPR-related lawsuits against Big Tech companies, 9 in the Netherlands.
  - 15 March 2023: *Data Privacy Foundation v Facebook Ireland*
    - Ruling by Amsterdam District Court cemented obligation of data controllers to demonstrate compliance with GDPR
- UK and Dutch courts experiencing upsurge of opt-out lawsuits

What will shape consumer claims in the future?

Artificial Intelligence Act

- Status: in last stages of legislative process
- Governs different types of AI across all sectors
- New procedural and quality rules for those distributing and developing AI systems
- Note: Artificial Intelligence Liability Directive also in the works

Digital Services Act

- Status: in force, rules will apply February 2024
- Aims to heighten safety online and regulate digital spaces
  - Safeguards to protect consumer rights
- Rules for all online services providers (in and outside the EU)
  - Proportionate to their role, size, and impact
- Sanctions: up to 6% of global turnover

Digital Markets Act

- Status: in force rules will apply March 2024
- Aims to make markets in the digital sector fairer and more contestable
- New obligations and prohibitions for 'gatekeepers'
  - Gatekeeper: large digital platform providing core platform services
- Sanctions: up to 10% of global turnover and beyond up to 20% that for repeat offenders

Omnibus Directive

- Status: in force
- Modernises 4 significant EU consumer directives
- Rules for 'traders'
  - Trader: B2C stores in EU, B2C e-commerce companies with EU consumers, and B2C companies offering free services to EU consumers
- Consumer rights will apply to digital services in exchange for personal data instead of money

What new consumer rights will arise?

Artificial Intelligence Act

- Creates new consumer rights, for example:
  - right to be informed when subjected to an AI-produced decision
  - right to submit complaints of AI system
  - right to bring supervisory authority to court if complaint is not addressed
- Creates the right to invoke **collective redress**

Digital Services Act

- Establishes collective redress mechanisms
- Reduces costs of legal proceedings for claimants
  - Litigation and alternative dispute resolution (ADR)
- Option to choose between platform's complaint system, court, or arbitration and fees must be reasonable

Digital Markets Act

- Establishes right to collective redress
- Protections for businesses and entrepreneurs
  - More competition in digital markets

Omnibus Directive

- Closely linked to the Representative Actions Directive
- Provides the right to redress for consumers harmed from unfair commercial practices

Questions

Thank you

twobirds.com

Abu Dhabi ● Amsterdam ● Beijing ● Bratislava ● Brussels ● Budapest ● Casablanca ● Copenhagen ● Dubai ● Dublin ● Dusseldorf ● Frankfurt ● The Hague ● Hamburg ● Helsinki ● Hong Kong ● London ● Luxembourg ● Lyon ● Madrid ● Milan ● Munich ● Paris ● Prague ● Rome ● San Francisco ● Shanghai ● Shenzhen ● Singapore ● Stockholm ● Sydney ● Warsaw