LATHAM & WATKINS LLP

October 22, 2020

Privacy Developments in France, Germany and the UK

Fiona Maclean
Myria Saarinen
Tim Wybitul

Your Speakers

Fiona M. Maclean

Data & Technology Transactions
Partner, London

T +44.20.7710.1822
E fiona.maclean@lw.com

Myria Saarinen

Complex Commercial Litigation
Partner, Paris

T +33.1.40.62.28.43
E myria.saarinen@lw.com

Tim Wybitul

Connectivity, Privacy & Information
Partner, Frankfurt

T +49.69.6062.6560
E tim.wybitul@lw.com

Agenda

I. GDPR Fines and Investigations

II. Schrems II

III. Brexit

IV. Artificial Intelligence

LATHAM & WATKINS LLP

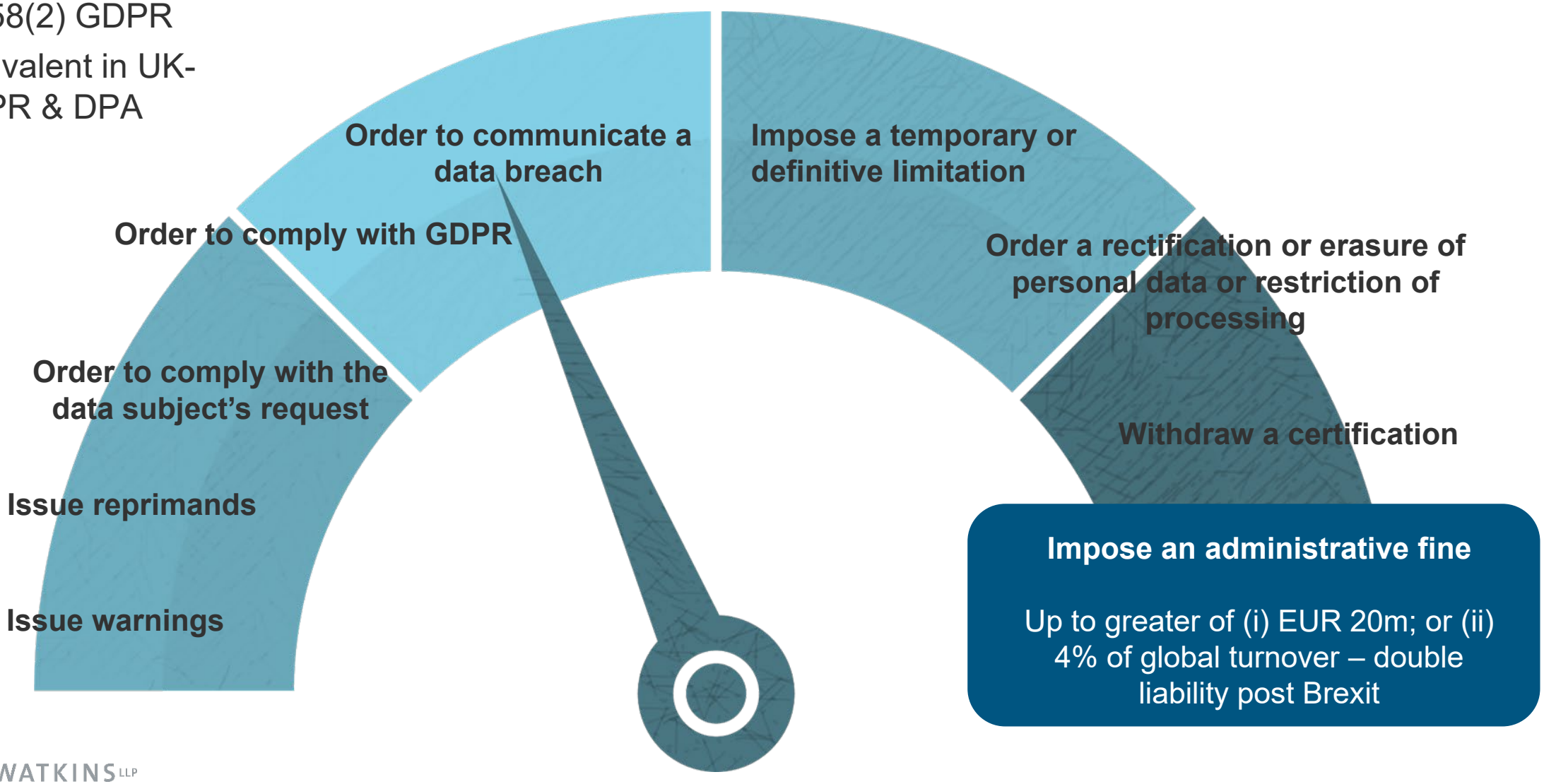
I. GDPR Fines & Investigations

Investigations – Key Risks

1. **Cybersecurity Incidents & Data breach** (mandatory notification requirements)
2. Complaints, civil litigation & **DSARs**
3. **Inadequate legal basis** (e.g. invalid consent/ inability to rely on legitimate interests/ sensitive person data)
4. Inadequate mechanisms for **cross-border transfer** – **Schrems II risks**
5. **Lack of transparency** on processing activities

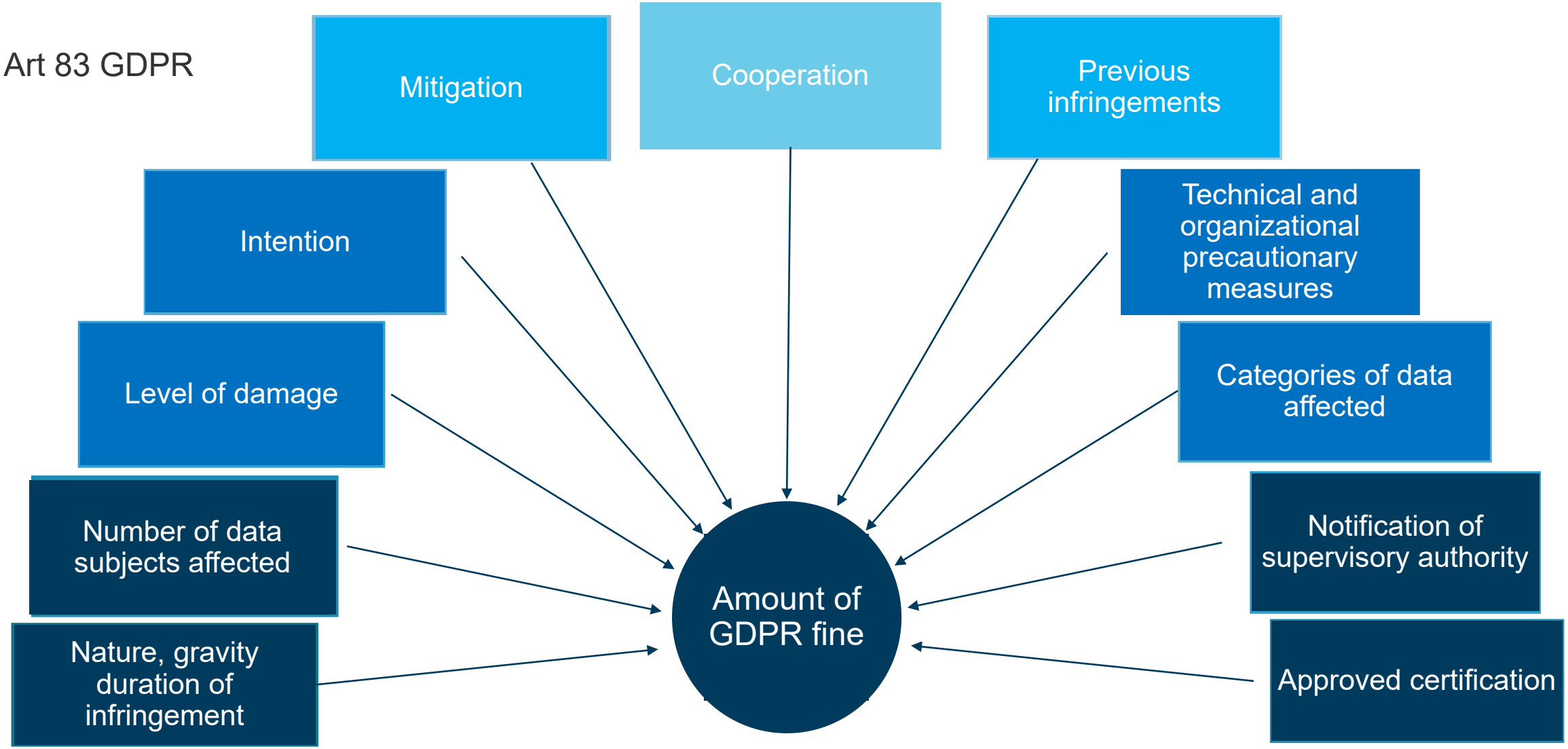
Powers of DPAs

- Art 58(2) GDPR
- Equivalent in UK-GDPR & DPA



Determination of Fines

- Art 83 GDPR



Scope of GDPR fines: the "undertaking"

Recital 150 of the GDPR:

"*Where administrative fines are imposed on an undertaking, an* ***undertaking should be understood*** *to be an undertaking* ***in accordance with Articles 101 and 102 TFEU*** *for those purposes*".

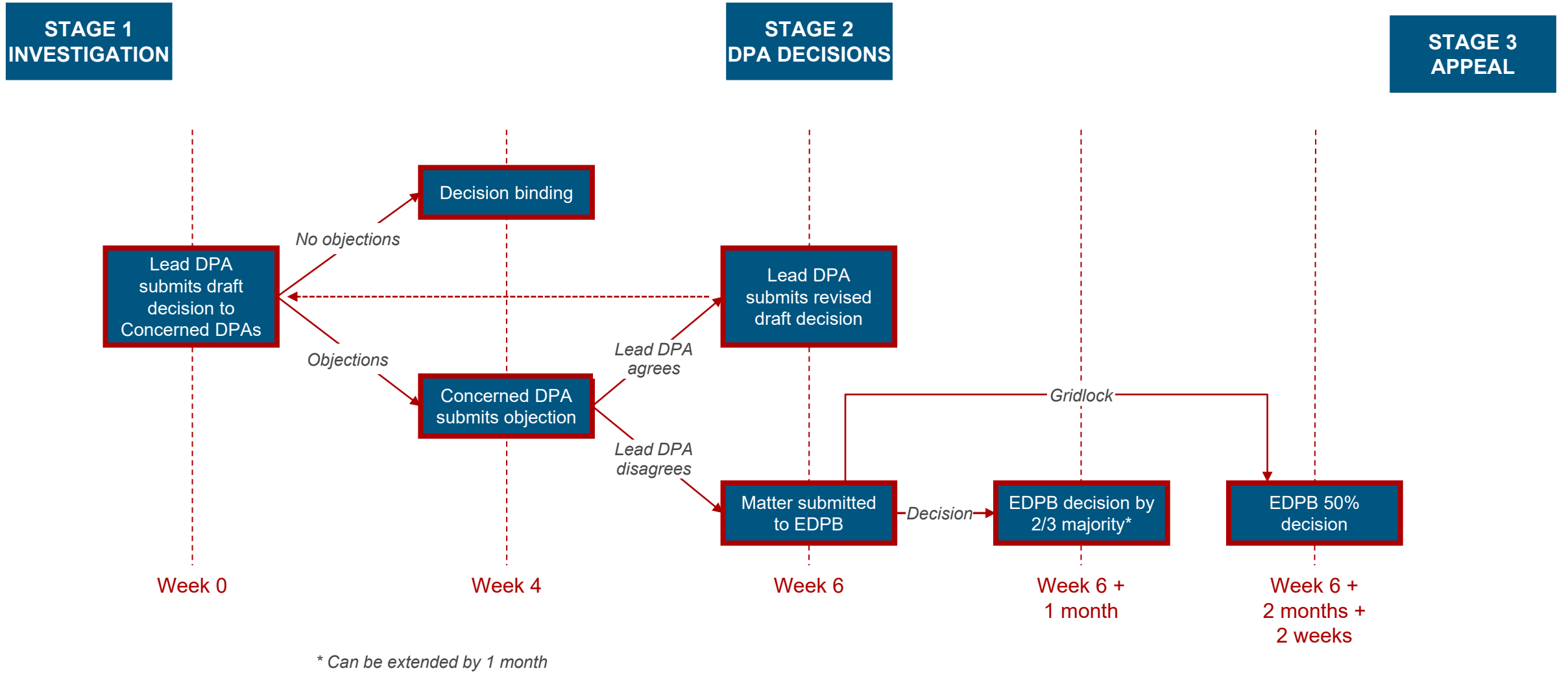
EDPB Guidelines on the application and setting of administrative fines (WP 253)

"*In order to impose fines that are effective, proportionate and dissuasive, the supervisory authority shall use for the definition of the notion of an undertaking as provided for by the* ***CJEU*** *for the purposes of the application of Article 101 and 102 TFEU, namely that* ***the concept of an undertaking is understood to mean an economic unit, which may be formed by the parent company and all involved subsidiaries****. In accordance with EU law and case-law, an undertaking must be understood to be the economic unit, which engages in commercial/economic activities,* ***regardless of the legal person involved***".

CJEU definition

- *"Any entity engaged in an economic activity,* ***irrespective of its legal status and the way in which it is financed***" (judgement of 11 December 2007, *ETI and Others*, C-280/06, paragraph 38);
- *"An economic unit even if in law that economic unit* ***consists of several persons, natural or legal*** " (judgement of 27 April 2017, *Akzo Nobel and others v. Commission*, C-516/15 P, paragraph 48).

Lead DPA & Decision-Making Process



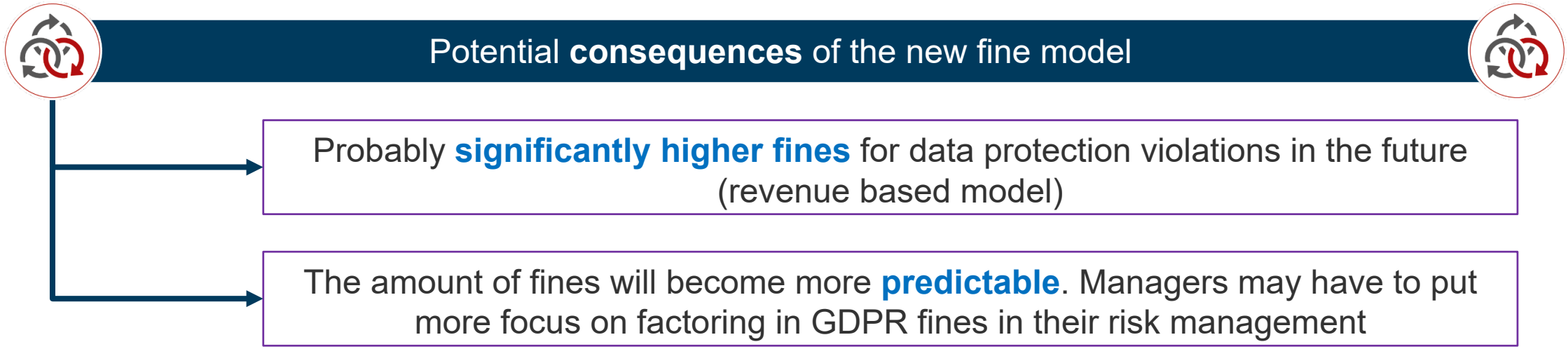
** Can be extended by 1 month*

GDPR – Largest Fines

1. **€ 110 m** (UK)	Controller: Hotel Chain (Jul 2019) Violation: Insufficient technical/organizational measures to ensure information security – **DPA has already announced to reduce this amount – Final decision expected 30 Oct 2020**
2. **€ 50 m** (France)	Controller: Search Engine (Jan 2019, upheld by the French State Council on Jun 2020) Violation: Insufficient legal basis for data processing (invalid consent for targeted advertising) and non-compliance with transparency obligations
3. **€ 35 m** (German)	Controller: Online Retailer (Oct 2020) Violation: Insufficient legal basis for data processing
4. **€ 27 m** (Italy)	Controller: Telecommunications Operator (Jan 2020) Violation: Insufficient legal basis for data processing
5. **€ 22 m** (UK)	Controller: Airline (Oct 2020) Violation: Insufficient technical/organizational measures to ensure information security – **Final fine reduced from proposal of € 204 m**
6. **€ 18 m** (Austria)	Controller: Postal Service (Oct 2019) Violation: Insufficient legal basis for data processing
7. **€ 16 m** (Italy)	Controller: Telecommunications Operator (July 2020) Violation: Non-compliance with general data processing principles

DSK Fine Model

- German DPA Coordination Board (DSK) published a comprehensive model for calculating GDPR fines, in October 2019
- DSK has announced it will further discuss the German model with other member states (**Co-ordination on a European level**), with potential for this to become a blueprint for an EU-wide model



ICO Fine Guidance

- The UK DPA (ICO) published draft guidance on actions and enforcement in October 2020 (open for public consultation)
- On fines (penalty notices), the guidance states these are for "**the most serious breaches**" and "typically involve **intentional or negligent acts**, or **repeated breaches of information rights** obligations, **causing damage to individuals**".
- Organisations are first given a 'notice of intent', and will have 21 days to respond.
- Nine-step mechanism to determine fine amount:
  1. Assessment of seriousness considering relevant factors under DPA 2018.
  2. Assessment of degree of culpability, taking into account the intentional/negligent nature of the processing.
  3. Determination of turnover.
  4. Calculation of an appropriate starting point:
  5. Consideration of relevant aggravating and mitigating features (e.g. financial benefits gained, or losses avoided etc.).
  6. Consideration of financial means.
  7. Assessment of economic impact.
  8. Assessment of effectiveness, proportionality and dissuasiveness.
  9. Early payment reduction - 20% if paid in 28 days, but not available if decision appealed.

Penalty starting point Standard Maximum Amount (SMA) (max of 2% or 10 Million Euro) Higher Maximum Amount (HMA) (max of 4% or 20 million Euro)				
Seriousness: / Degree of Culpability:	Low	Medium	High	Very High
Low / No	**SMA** 0.125% **HMA** 0.25%	**SMA** 0.25% **HMA** 0.5%	**SMA** 0.375% **HMA** 0.75%	**SMA** 0.5% **HMA** 1%
Negligent	**SMA** 0.25% **HMA** 0.5%	**SMA** 0.5% **HMA** 1%	**SMA** 0.75% **HMA** 1.5%	**SMA** 1% **HMA** 2%
Intentional	**SMA** 0.375% **HMA** 0.75%	**SMA** 0.75% **HMA** 1.5%	**SMA** 1.125% **HMA** 2.25%	**SMA** 1.5% **HMA** 3%

CNIL Fining Policy

No clear methodology emerges from the recent CNIL decisions **but several criteria** taken into account

- Criteria based on the infringement at stake
  - the categories of data involved in the infringement
  - the nature of the infringement (infringements appear of particular gravity when in relation to data subjects' rights, collection of consent, obligation of transparency…)
  - the number of infringements
  - the ongoing nature of the infringement (not an occasional one)
  - the basic nature of the measures which should have been taken to avoid the infringement

- Criteria based on the data subjects
  - the number of data subjects concerned by the infringement
  - the existence / the number of complaints filed by data subjects
  - the existence of damages suffered by the data subjects

CNIL Fining Policy

- Criteria based on the company itself
  - the size of the company
  - the financial results of the company (including their evolution)
  - the company's business model

- Other aggravating / mitigating factors in the calculation of the fine
  - the fact that the infringement is in relation with an obligation which was already existing before GDPR
  - the rapidity of the corrective measures implemented by the company to achieve compliance
  - the cooperation of the infringing company with the CNIL

- The French State Council (Appeal court) **controls the proportionality** of the fine imposed by the CNIL
- It made clear that the amount of the fine should take into account "*the **nature**, the **gravity**, the **duration** of the infringements, as well as the **behavior** of the infringing company following the CNIL's observations*".
- It decided that the CNIL is **not obliged** to include an explanation of the amount of the fine, to refer to each of the Article 83 criteria and to give a method of calculation justifying the amount of the fine.

Mitigating the Risk

Preparedness for crisis management

Determine and maintain processes and policies

Monitor and be responsive to activities of SAs

Internal coordination

Effective communications strategy

Self-disclosure or notification

Be reactive to complaints / DSARs from employees, customers, etc.

Determine roles and responsibilities

Response documentation prepared (draft communications, litigation documentation, compliance documentation)

DPO involvement

Mitigating Risk – Response

Evidence & Privilege

- Document creation and organisation
- Local and international laws – conflicts?

Parallel proceedings & litigation

- Different privilege issues?
- Government committees elsewhere
- Regulators investigate when others do

Time including appeals

- Managing investigations is a full-time job

Lessons learnt

Mitigating the Risk - Fines

Fundamental Question – Strategic Landmark Decision
Full cooperation with DPA in fine proceedings or conflict defence?

Cooperation

- Often to be recommended when negotiating the amount of a possible fine
- Cooperation of company that exceeds the requirements of Art. 31 GDPR has to be taken into account as mitigating effect when determining the fine

(Art. 83(1), (2): Should a supervisory authority not take into account cooperation sufficiently, the fine violates the principle of proportionality)

Conflict defence

- If, contrary to the opinion of the DPA, the company does not believe that a fine is justified in a specific case, it may be advisable to engage in conflict defence
- Company may decide to provide minimal cooperation with the DPA and prepare for fine proceedings in court

Litigation & Damages Claims – Strategy

Receipt of a claim

- **Civil litigation & damages claims:** Class actions/ representative actions for damages are increasingly common.
- Typically following DPA investigations and fines, or public reporting of actual/ suspected cybersecurity incidents and data breaches.

Review & Strategy

- Review of the claims and relevant case law
- Development of a strategy (helpful to have a defence strategy prepared in advance)

Meeting the demand?

- In general it is not recommended to meet the demands in the first instance
- This may set a precedent and invite further claims

Thorough examination of the claims made

- It might be advisable to reject the claims as a first step
- Consider procedural steps to mitigate the risks of interim injunctions/ other interim measures

Litigation & Damages claims – Defence

Damage claims

- Claimant must prove the claim and evidence the specific damage
- German perspective: No general reversal of the burden of proof in favor of the claimant (according to Art. 5 Abs. 2 und 24 Abs. 1 DSGVO)

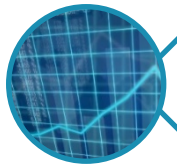
Cease and desist claims

- German perspective: Potential defence to show no risk of recurrence
- Unique non-recurring situation (especially when data breaches are due to criminal behaviour by third parties, e.g. hacking)

Litigation & Damages Claims - Litigation Funding

- Published fine proceedings and data breaches increasingly attract the attention of **commercial litigation funding**
- Commercial litigation funders **actively advertise** by the means of different media channels to obtain engagements
- Commonly, the commercial litigation funders will bear the costs and risks of litigation, and will receive a percentage of any damages awarded (**no expense risks** for data subjects)
- In other areas, the commercial enforcement of consumer rights has already been established (e.g. the enforcement of compensation claims against airlines)

Lessons Learned



Higher GDPR fines are to be expected in future. As a result, effective defence strategies are becoming increasingly important

In the event of an investigation, companies should decide at an early stage whether they want to cooperate with the supervisory authority or prepare to defend

After data breaches, data subjects increasingly demand damages and injunctive relief. Companies should develop strategic procedures for dealing with such claims.

The emergence of commercial litigation financiers could lead to companies having to defend themselves much more frequently against damage claims in the future.

By effectively designing internal defense processes (and documentation), companies can proactively counter the risk of fines and damage claims.

Internal processes should also be designed from the outset to create an effective defence in potential fine proceedings or in case of damage claims (defensibility).

LATHAM & WATKINS LLP

II. Schrems II

Schrems II

Privacy Shield

- CJEU invalidated the EU-US Privacy Shield – Immediate effect; enforcement grace period unclear
- Swiss-US Privacy Shield also deemed inadequate for data transfer, by Swiss DPA

Standard Contractual Clauses

- SCCs remain valid, but imposed caveats – SCCs are not necessarily sufficient; additional safeguards may be required
- CJEU held that reliance on SCCs (and BCRs) requires assessment of whether the destination country ensures adequate protection – case-by-case basis
- CJEU focussed on access rights to data by public authorities for national security purposes, and individual rights and remedies
- The CJEU's new standards for the SCCs apply to all data transfers outside the EU/ UK (not just the US)
- The decision applies to data transfers from the UK during the transition period
- Long term implications unclear – New SCCs expected before the end of the year

LATHAM & WATKINS LLP

III. Brexit

Brexit

- UK has enacted GDPR into its domestic law (Data Protection Act 2018; UK-GDPR)
- Similar extra-territorial test for application of UK-GDPR
- Post Brexit, **data processing activities could potentially be subject to both GDPR and UK-GDPR - Doubles potential exposure to fines**
- Representatives may be required in both EU and UK
- LSA/One-stop shop mechanism will not apply
- **Data exports from EU to UK are not considered adequate – Unless (until) UK gets adequacy ruling**
- Policies and agreements should address UK to ROW exports

LATHAM & WATKINS LLP

IV. Artificial Intelligence

Increasing Regulatory Focus

EU Guidelines on Ethics in AI & Assessment List for Trustworthy AI

- Privacy and Data Governance
- Transparency
- Diversity and Fairness
- Human Agency and Oversight
- Robustness and Safety
- Societal/Environmental Well-Being
- Accountability

EU High-Level Expert Group on AI

EU Commission White Paper on AI

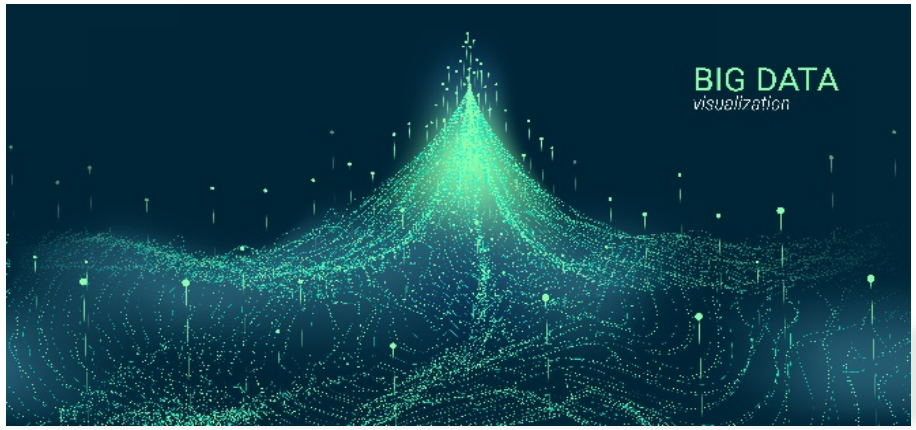
EU Commission Report on Safety & Liability Aspects of AI

UK ICO Guidance on AI & Data Protection

Challenges under GDPR

Key privacy considerations

- Knowing what is ‘personal’ data and ‘sensitive’ personal data
- Fair processing – Lawful? Ethical? Reliable? Fair – e.g. not biased and discriminatory
- Transparency: Difficulties providing notice to data subjects/ explaining meaningful logic of decision
- Controller/Processor: blurred lines v joint controller: lack of clarity
- Requirements for obtaining valid “consent” / legal basis
- Article 22 – decision that have legal / significant effect required consent / contractual necessity
- Data retention
- Managing data subject rights
- Subcontracting
- Cross-border transfers of data
- Mandatory data breach reporting
- Cybersecurity implications



LATHAM & WATKINS LLP

Questions

Disclaimer

Although this presentation may provide information concerning potential legal issues, it is not a substitute for legal advice from qualified counsel. Any opinions or conclusions provided in this presentation shall not be ascribed to Latham & Watkins or any clients of the firm.

The presentation is not created or designed to address the unique facts or circumstances that may arise in any specific instance, and you should not and are not authorized to rely on this content as a source of legal advice and this seminar material does not create any attorney-client relationship between you and Latham & Watkins.