MAYER·BROWN

GDPR: Lessons Learned from the First 100 Days

Today's Speakers

Dr. Ulrich Worm

Partner – Frankfurt
Uworm@mayerbrown.com

Charles-Albert Helleputte

Partner – Brussels
Chelleputte@mayerbrown.com

Diletta De Cicco

Associate – Brussels
Ddecicco@mayerbrown.com

Oliver Yaros

Partner – London
Oyaros@mayerbrown.com

Björn Vollmuth

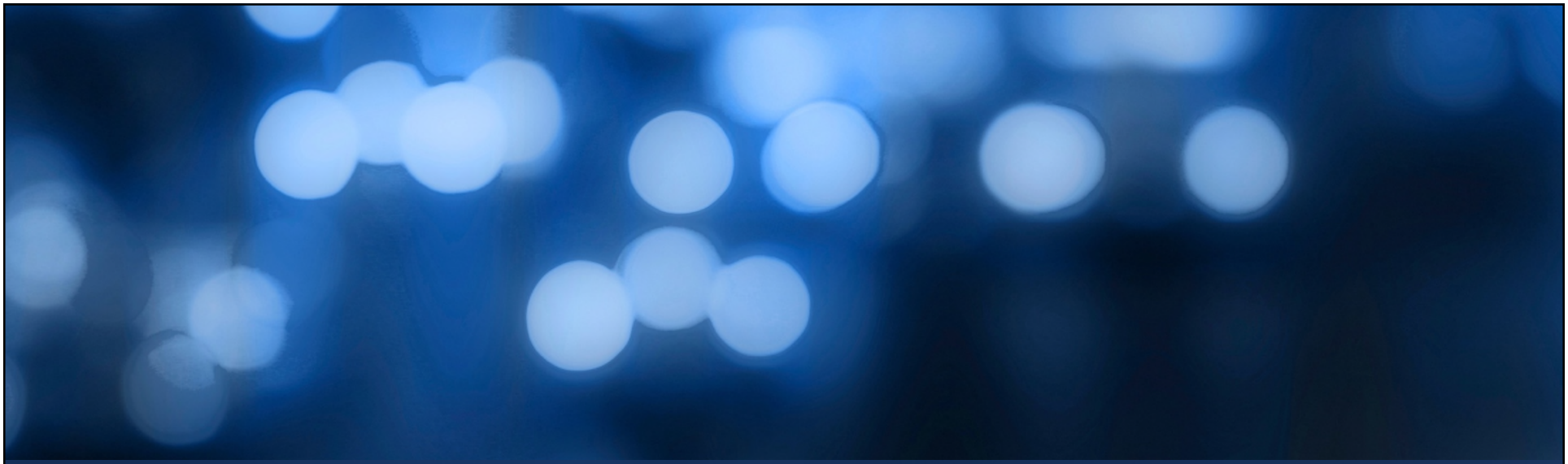
Counsel – Frankfurt
Bvollmuth@mayerbrown.com

Lei Shen

Partner – Chicago
Lshen@mayerbrown.com

Agenda

1. News, Development and First Enforcement Trends
2. Managing personal data breaches: 5 Lessons Learned
3. The (unintended) Effects of Negotiating a Data Protection Addendum
4. New Laws Inspired by GDPR; from California to Brazil



News, Developments and First Enforcement Trends of GDPR Since GDPR Day

Ulrich Worm

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

- "*We have got our teeth now, but we haven't shown our bite*"

  (as the head of a German data protection authority put it – "*Wir haben Zähne bekommen, sind aber nicht bissig geworden*")

- In fact, only limited number of reported fines since GDPR day, yet
  - UK data protection authority recently fined company for selling data for political campaigning, and another company for "nuisance" e-mails
- But: Fine proceedings take their time

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

- Data protection authorities seem overwhelmed by GDPR
- The number of
  - complaints filed by data subjects
  - requests for guidance and
  - notifications of personal data breaches

  with the data protection authorities have increased substantially

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

- The data protection authorities need to staff-up, and to prioritize, to tackle this
- Further, statements from some of the data protection authorities throughout Europe and the general political climate suggest that the authorities will:
  - Focus enforcement activities first on the "big fish"
  - Work with recommendations and warnings before imposing fines against smaller players
  - Continue to issue guidance documents to help companies navigate GDPR
  - But: Take enforcement actions against those that "*persistently ignore their obligations*"

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

- What else have we seen since G-Day?
- Data protection authorities have started to audit companies, for example:
  - a German data protection authority has started to audit 50 companies from various sectors
  - another German data protection authority has started to investigate several hospitals in relation to their handling of health data
  - the UK data protection authority investigated companies who provide data analytics for political purposes

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

- The Italian data protection authority published its action plan for the second half year of 2018
- The authority plans to focus its activities on:
  - Processing activities carried out by public bodies that handle big databases
  - Data protection measures implemented by credit institutions (with a focus on data breaches)
  - Processing activities related to telephone marketing

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

- The Italian authority says that its investigations will in particular address the following aspects:
  - Information of data subjects
  - Requirements for valid consent and other legal bases for data processing
  - Data retention policies
  - Security measures
  - Data processing agreements
  - Appointment of data protection officers

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

- Conflicting guidance from authorities across Europe
- For example, in the context of study agreements concerning pharmaceuticals and medical devices:
  - The UK Health Research Authority took the position that hospitals are data processors of study sponsors
  - The German working group of the ethics commissions rather suggests that hospitals and study sponsors are typically joint controllers
- Conflicting guidance creates challenges to developing a joint GDPR compliance strategy for Europe

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

- Market participants have sent first cease and desist letters to competitors arguing that a violation of GDPR obligations amounts to a violation of the German Act Against Unfair Competition
  - No reported case law on the question whether GDPR violations are actionable by competitors on this basis
  - The German legal commentators appear split on this question
  - There are political initiatives to explicitly exclude GDPR violations from the German Act Against Unfair Competition

News, Developments and First Enforcement Trends of GDPR Since GDPR Day

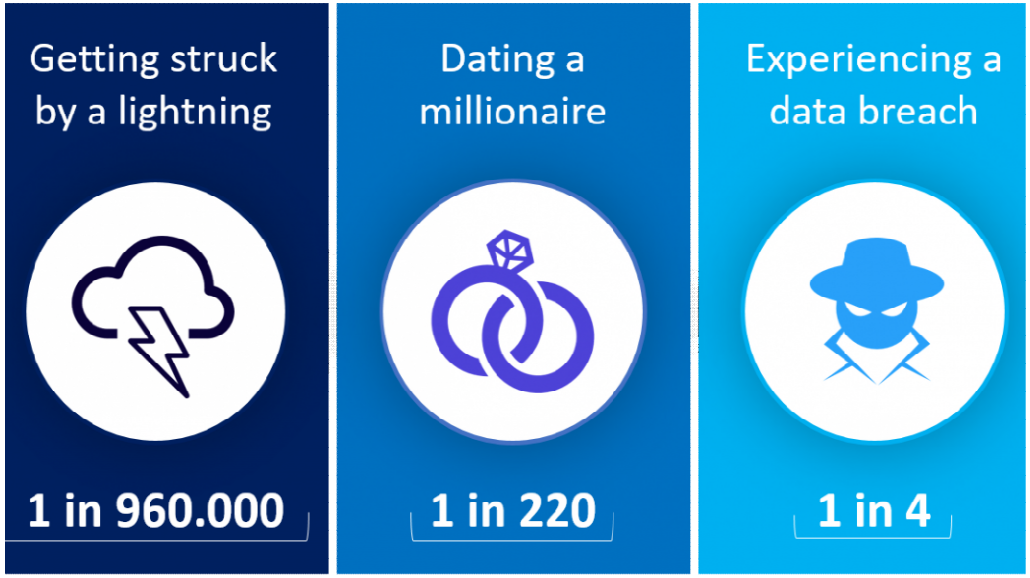
- The future of data transfers under the EU-U.S. Privacy Shield and the Standard Contractual Clauses
  - The EU parliament adopted a resolution on 5 July 2018 and asked the EU Commission to suspend the EU-U.S. Privacy Shield
  - Second annual review of the Privacy Shield is expected to take place in October 2018
  - Meanwhile, the ECJ has been asked to rule whether Standard Contractual Clauses and the Privacy Shield remain valid legal bases for data transfers under the GDPR (ECJ C-311/18)

Data Breaches: 5 lessons learned

Diletta De Cicco & Charles A. Helleputte

Data Breaches: 5 lessons learned

- Breaches happened, were notified to DPAs and communicated to data subjects since GDPR Day:



Source: Ponemon Institute's 2017 Cost of Data Breach Study

Data Breaches: 5 lessons learned

What have we learned from assisting our clients in this area?

1. GDPR is important but … there is more than GDPR
2. Interaction with DPAs requires caution
3. Data breach notification is a test for your LSA's election
4. Notifying DPAs might be (un)easy
5. The When, How and Why of communication to data subjects

\+ bonuses we are prepared to share

Lesson 1: GDPR is *not* the only thing that matters

- Reminder:
  - GDPR imposes strict compliance / requirements on organizations having to deal with personal data breaches BUT many other breach / security frameworks (might) come into play (prudential, non-EU ones, etc.)
  - How communication to data subjects and cooperation with enforcement authorities can smoothly play out?
- Lessons learned:
  - Preparation and readiness of global team to coordinate and work alongside is necessary to protect the interest of the organization and mitigating exposures

Lesson 2: Interact with DPAs with caution

- Reminder:
  - Transparency and accountability are important data protection principles but in dealing with DPAs, especially in the breach context, controllers should remind themselves that they are the ones to assess whether or not they are facing a reportable breach (and that they might have to defend their choices later on)
  - There are no “off the record” conversations with DPAs. What you tell them is on their file

Lesson 2: Interact with DPAs with caution

- Lessons learned:
  - There is a timing and a way for interactions with DPAs to run as best as possible
    - Interact with DPAs following your initial notification: (i) on timing and expectation on notification in phases or (ii) to test your communication' strategy with data subjects
  - Some DPAs promoted hot lines for data breaches reporting (over forms)
    - Whom will you be sending to take that call and be faced with (tough) questions?
    - Whenever you can (unless portals are unavailable), use forms

Lesson 2: Interact with DPAs with caution

- Lessons learned:
  - There is an uneven responsiveness rate among the DPA (and some are taking steps that are not even anticipated under GDPR such as DPA on site with processors)

Lesson 3: Data Breach is a test for your LSA election

- Reminder:
  - In a cross-border processing context, EU-based controllers designate a Lead Supervisory Authority
  - This requires proper documentation to be in place, supported by ad hoc assessment
  - LSA is not available to all controllers (i.e., only to “EU-based”)
  - Very relevant in a breach notification context, as controller only needs to notify their LSA (using and gathering information on a single form)

Lesson 3: Data Breach is a test for your LSA election

- Lessons learned:
  - Controllers tend to stand behind the choice they made (or they think they made)
  - Caution is necessary in case of doubts as to whom is your LSA (see WP29 breach guidelines). Multiple notifications might be necessary / prudent
  - Not yet challenged by DPAs (even if they may do so under Article 56 GDPR) or no occasion where multiple DPAs stepped in and launched their own investigations even when a LSA was designated

Lesson 4: Notifying DPAs is (un)easy

- Reminder:
  - Notification of a reportable data breach should take place within a tight timeframe
  - Breach notification forms are not harmonized across the EU Member States
  - Information to provide differs (significantly) from one DPA to another

Lesson 4: Notifying DPAs is (un)easy

- Lessons learned:
  - Providing the required information in a timely manner may prove to be difficult. This is even more the case in a processor-breach context (what does your DPA with them provide and can you enforce your right to receive ad hoc information?)
  - Don’t get caught by processor-driven communications in relation to the data breaches they encounter; controllers retain the overall responsibility in the notification process (e.g., review templates provided by processors and some of their line of arguments and don’t copy paste what are presented as ready to use materials)

Lesson 4: Notifying DPAs is (un)easy

- Lessons learned:
  - Example: recent hospitality software breach we worked on showed that processor encountering a breach might try bargaining with controller (to avoid communication to data subjects for example or to limit the information disclosed) in a way to mitigate their own exposure
  - Communication to data subjects should be drafted keeping in mind the objective and not used as a defense / shifting responsibilities

Lesson 5: Communicating to data subjects

- Reminder:
  - When a data breach is likely to result in a high risk to the rights and freedoms of data subjects, the controller shall communicate to the data subjects
  - What is high risk (and how to assess it)?
    - This requires a methodology that needs to be part of your incident response plan (building it at the same time of managing the breach is unpleasant)

Lesson 5: Communicating to data subjects

- Lessons learned:
  - Using pre-GDPR tools to objectify risk is a reasonable approach BUT:
    - One needs to keep in mind the rationale of the communication to data subjects ("allow them to take steps to protect themselves from any negative consequences of the breach")
  - How easy is it to substantiate that, confronted with a breach involving EU and non-EU located data subjects that are likely to cause a high risk to their rights or freedoms, you will only communicate to EU-located ones?
    - (Not very easy) ☺
  - PR-related aspects of communicating (even more about processor-located breaches) and some of the feedback

Bonuses:

- Watch out for GDPR-related tools that might be breach trigger (non substantiate SARs)
- Breaches are a Friday's things (and we are Thursday)

Negotiating Data Protection Addenda with Third Parties

Oliver Yaros & Björn Vollmuth

Negotiating DPAs with Third Parties

- Requirements controllers must impose on processors under Article 28. E.g.:
  - Only act on controller's documented instructions
  - Ensuring security
  - Commitments re confidentiality, deletion / return of personal data
  - Audit rights, appointment of subprocessors, etc.
- Direct obligations that a recipient may have under GDPR. E.g.:
  - Controller obligations: Keeping a record, appointing a DPO, conducting DPIAs, providing fair processing notices / obtaining consents, liaising with supervisory authorities, data subjects, etc.
  - Processor obligations: Keeping a record, appointing a DPO, notifying a controller of personal data breach / that instructions infringe law, etc.

Negotiating DPAs: The service provider's perspective

- Typical points of concern for service providers in negotiations
  - Responsibility for ensuring processing complies with law
  - Responsibility for ensuring appropriateness of security
  - Retaining control and consistency of terms over supply chain and audits
  - Personal data breach notification
  - Liability
- Trends in the negotiating stance of service providers:
  - Disclaimer of liability / suspension rights where processing does not comply with law
  - Responsibility for ensuring security to a defined level only, not appropriateness
  - Offer of visibility not control over supply chain, limited rights to object. Pre-defined audit rights
  - Resistance to specific time limits to inform of personal data breaches
  - Narrowing of liabilities, particularly for personal data breaches

Negotiating DPAs: The customer's perspective

- Typical points of concern for customers in negotiations and trends in the negotiating stance of customers:
  - Right to object to sub-processors limited to specific or important reasons:
    - Objection must not be random but based on objective reasons
    - Further limitation to be verified carefully
  - Consequences of valid objection to use of certain sub-processor:
    - Preferred consequence of objection: processing to be continued without use of the relevant sub-processor
    - In practice (partial) termination of contract more likely/feasible
  - Limitation on the right to issue instructions:
    - Controller is responsible for whole processing operation and must hence be able to issue processing-related instructions beyond the statement(s) of work
    - Provider could suggest a fee for complying with instructions that go beyond agreed services

Negotiating DPAs: The customer's perspective

- TOMs - Reference to provider's website:
  - A "moving target" is not acceptable
  - Current status of TOMs needs to be agreed and documented in an attachment to the DPA
- Deadline for personal data breach notification:
  - Deadline for data breach notification should not be unreasonably short to avoid false positives
  - Controller's deadline for notifying data subjects and/or the supervisory authority commences upon receipt of notification from processor, not upon occurrence of the incident
- Backup/deletion concept of provider:
  - Personal data is to be deleted or returned at the end of the service contract
  - But technical impediments cannot be ignored in practice
- Liability cap:
  - Tendency to renegotiate liability caps in light of the increased fines under the GDPR

New Laws Inspired by the GDPR, from California to Brazil

Lei Shen

New Laws Inspired by the GDPR

- The GDPR has inspired a number of similar laws in other countries, including Brazil and the State of California in the United States
- While there is a lot of overlap among these laws, there are some key differences
  - Compliance with the GDPR will not be enough to comply with these laws, but companies can leverage work done to comply with the GDPR to reach compliance with these laws

California Consumer Privacy Act (CCPA)

- Signed into law on June 28th
- Considered to be the strongest, most aggressive privacy law in the U.S.
- Applies to for-profit companies doing business in California that either:
  - (1) have annual gross revenues of USD $25 million or more
  - (2) obtain personal information of 50,000 or more California residents, households or devices annually, or
  - (3) derive 50% or more of their annual revenue from selling the personal information of California residents

California Consumer Privacy Act (CCPA)

- Broad definition of personal information
- New individual rights, including:
  - The right to request certain disclosures from a company (e.g., regarding the types of personal information collected and what the company is doing with that information)
  - The right to request deletion of personal information, with certain exceptions
  - The right to opt-out of the sale of personal information
- Enforcement by California Attorney General (with potential fines) and limited private right of action
- Recent amendment contains several substantive changes, including extension of enforcement timeframe

Brazil Data Protection Law

- Enacted in August 2018 and comes into force in February 2020
- Has rights and obligations similar to the GDPR:
  - Applies to all processing of personal data
  - Extraterritorial application
  - Requires legal basis for processing
  - Significant fines (although not as high as those under the GDPR)
  - Data subject rights
  - Security requirements
  - Data breach notification requirements
  - Cross-border data transfer restrictions

Notice

The material in this presentation is provided for informational purposes only and does not constitute legal or other professional advice. You should not and may not rely upon any information in this presentation without seeking the advice of a suitably qualified attorney who is familiar with your particular circumstances. Mayer Brown Practices assumes no responsibility for information provided in this presentation or its accuracy or completeness and disclaims all liability in respect of such information.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the "Mayer Brown Practices") and non-legal service providers, which provide consultancy services (the "Mayer Brown Consultancies"). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website.

MAYER·BROWN