WIPO | ADR
Arbitration and Mediation Center

ADR and Data Disputes Webinar

Ms. Margarita Kato
WIPO Arbitration and Mediation Center, Switzerland

Mr. Nicholas Oldham
Chief Privacy and Data Governance Officer, Equifax, USA

Mr. Flip Petillion
Arbitrator and Litigator, Petillion, Belgium

Mr. James Tumbridge
Partner and Barrister, Venner Shipley LLP, UK

Online Webinar
October 26, 2020

In this webinar

- Submit your questions
- Download handouts
- Receive webinar recording

In this webinar

- What we need to know about Data Protection issues
- Impact of GDPR and *Schrems II* on cross-border data transfers and contracts
- ADR for Data Disputes
- With perspectives from:
  - in-house counsel
  - external lawyers
  - Europe
  - UK, and
  - US

WIPO Arbitration and Mediation Center

- Part of the World Intellectual Property Organization (WIPO) which:
  - promotes innovation and creativity, through a balanced and effective international IP system
- WIPO Center is an ADR provider which facilitates resolution of commercial disputes between private parties through out-of-court procedures:
  - internationally neutral
  - specializes in IP and technology disputes
  - offices in **Geneva** and **Singapore**
  - users around the world

WIPO | ADR
Arbitration
and Mediation
Center

What is the WIPO Center's role?

- WIPO Center:
  - provides information and procedural advice, including assisting parties who are considering whether to refer their dispute to WIPO proceedings
  - assists parties in selecting specialized mediators, arbitrators and experts
  - arranges support services, including meeting rooms and videoconferencing facilities

WIPO and B2B Data Disputes

- "Neutrals" List
  - Arbitrators, mediators and experts with understanding of key issues in data processing
- WIPO Rules
  - Specific provisions on confidentiality and trade secrets
- International Neutrality
- Provides Standard Clauses in 9 languages

Contact: arbiter.mail@wipo.int

Further information: www.wipo.int/amc

WIPO | ADR
Arbitration and Mediation Center

WIPO – What can ADR offer Data Disputes?

October 26th 2020

Venner Shipley

The Panel

James Tumbridge

Venner Shipley LLP

Venner Shipley LLP is a Tier 1 full service European IP firm with offices in the UK and Germany.

James is an arbitrator, mediator & barrister, regularly advising corporate and government clients on all aspects of data protection, and disputes.

He is one of the authors of the UK Data Protection Act 2018, which implemented GDPR.

Nick Oldham

EQUIFAX

Nick is Global Chief Privacy and Data Governance Officer at Equifax.

He was previously a partner at King & Spalding in Washington, D.C., and a U.S. federal prosecutor focusing on cybercrime matters.

Flip Petillion

Petillion

Flip is the Managing Partner of Petillion law firm. He acts regularly in domestic and international litigations and arbitrations in matters related to Information Technology, Telecommunications, Intellectual Property, Construction and Energy.

Flip has acted as counsel and also served as chairman, sole arbitrator and party-appointed arbitrator in arbitration proceedings under WIPO and other international institutions.

Global Average Total Cost of a Breach

$3.8 Million

(Poneman Institute – “The 2018 Cost of a Data Breach Study”)

Identities Stolen 2016-17

1.1 Billion

IAPP, April 26, 2017

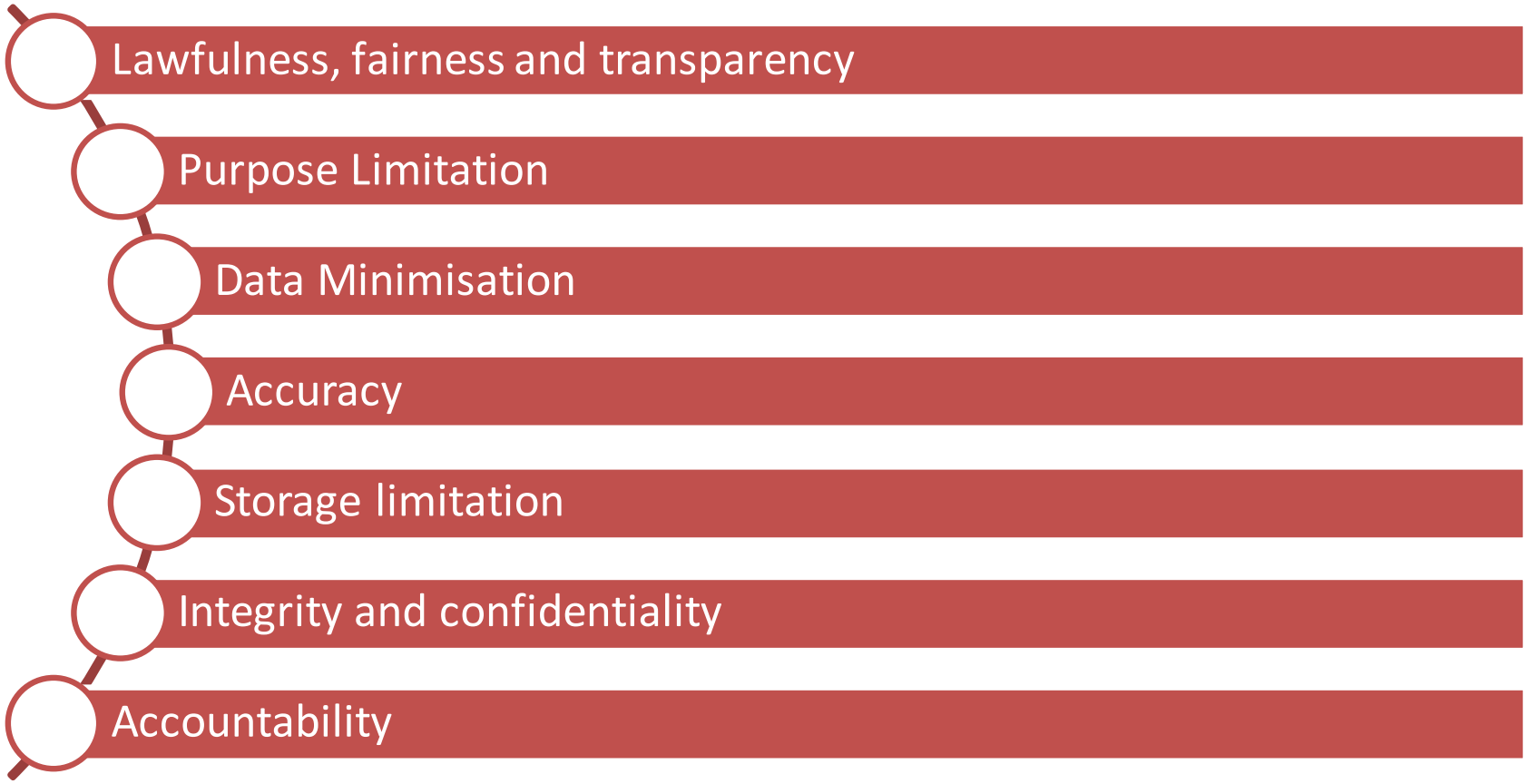
GDPR Requirements

- European Regulation – effective May 25th 2018 - applies uniform rules across the EU & UK.
  - Applies to anyone operating in the EU (including processing personal data of EU residents), even if they do not have a physical presence in the EU.
  - Technically duty to register as a Data Controller and pay an annual fee will be abolished (though a 'data protection fee' will continue to be payable), but new administrative duties are likely, including:
    - Expanded record keeping requirements
    - Security risk evaluations
    - Privacy impact assessments
    - Self auditing
    - Appointment of data protection officer for sign-off on privacy audits
    - Increased sanctions for non-compliance, including fines of up to €20 million or 4% of annual worldwide turnover

GDPR Requirements

- There will be a duty to notify the DPA and data subjects of data breaches
  - Having appropriate security measures in place (i.e. data encryption) will lessen the burden on controllers
- Data Controllers will be required to demonstrate compliance.
- More comprehensive privacy notices will need to be concise, transparent, intelligible and easy to access, setting out:
  - The purposes of data processing
  - The data retention terms
  - The right to lodge a complaint with the data protection authority
  - Transfers to third countries and the level of protection for the data
- Data subjects will have a right to request the erasure of their personal data, subject to certain exceptions.

Principles of personal data processing



Basic definitions and scope

Personal data	• Any information relating to an identified or identifiable natural person
Processing	• Any operation or set of operations which is performed on personal data – just hosting is enough

Geographic scope	• Establishment in the EU or
	• Processing activities related to:
	  • The offering of goods or services to data subjects in the EU; or
	  • Monitoring/processing of EU data subjects.

GDPR

- **Article 6 – Lawful processing can be by:**
  - **Consent;**
  - **Contract;**
  - **Legal Obligation**;
  - Protection of interests vital to a person;
  - Performance of a task of an official authority; or
  - Necessary for legitimate interests (the last does not apply to public authorities).

‘Personal Data’ and ‘Sensitive Personal Data’

- **Personal Data**
  - Data relating to an individual who can be identified from the data or from the data and other information in the possession of, or is likely to come into the possession of the Data Controller
  - Includes any expression of opinion about the individual and any indication of the intentions of the data controller or any person in respect of the individual
- **‘Sensitive’ Personal Data**
  - Racial or ethnic origin
  - Political opinions
  - Religious or similar beliefs
  - Physical or mental health
  - Sexual orientation
  - Trade union membership
  - Criminal offences/proceedings and/or accusations

GDPR

- Article 9 – Processing of special categories of data:
  - Racial or ethnic origin;
  - Political opinions;
  - Religious opinion;
  - Philosophical belief;
  - Trade union membership;
  - Genetic data;
  - Biometric data;
  - Sexual orientation –
  - All prohibited from process or revealing unless… explicit consent

Sensitive Personal Data

- If the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle.
- Key Conditions:
  - The individual whom the sensitive personal data is about has given explicit consent to the processing.
  - The individual has manifestly made the information public.
  - The processing is necessary for administering justice, or for exercising statutory or governmental functions.

Security

- Data Processing Principle 7 requires that:

  '*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*'

- In practice – there is a need to:
  - Design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach
  - Be clear about who in your organisation is responsible for ensuring information security
  - Be sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff
  - Be prepared to respond to any breach of security swiftly and effectively

Security (cont)

- The security measures you put in place should seek to ensure that:
  - Only authorised people can access, alter, disclose or destroy personal data
  - Those people only act within the scope of their authority
  - If personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned
- There is no 'one size fits all' solution to data security, and the level of security you choose should depend on the risks to your organisation
- ISO 27001 security online may be used as a guide

Breach, consequences and fines

- **Breaches:**
  - You must have a policy in place and the ability to report within 72 hours to the ICO.
- **Fines:**
  - The new regime has significantly increased the fines available to the ICO.
- For the most serious violations of the law, fines up to twenty million Euros or four per cent of a company's total annual worldwide turnover for the preceding year.

Transfers of personal data outside the European Economic Area (EEA)

- Personal data are not to be transferred outside the EEA unless there is an ‘adequate level of protection’
- Some countries are deemed to have an ‘adequate’ level or protection; the United States does not unquestionably have an adequate level of protection
- Transfer of data to the US - The Court of Justice of the European Union held that the Safe Harbour did not offer an adequate level of protection, and Privacy Shield is now also invalid following Schrems II.

Transfers of personal data outside the European Economic Area (EEA) *(contd)*

- Other options include the use of Model Contract Clauses or Binding Corporate Rules
  - These can be onerous and expensive to implement
  - It is uncertain how effective these options will be for transfers to the US as they have not been GDPR reviewed
- Certain exemptions are available but are narrowly construed and it is not recommended that these be relied upon

Contractual Solution?

- SCCs can be relied upon for data transfers to countries which do not benefit from an Adequacy Decision, but post-Schrems II the data exporter and the recipient each have duties to satisfy themselves that data will be adequately protected in the foreign jurisdiction.
- BCRs remain valid, though the commentary from the CJEU in Schrems II concerning SCCs is likely also to be relevant to BCRs, i.e. whether the corporate group relying on its approved BCRs is satisfied that the foreign domestic law where group companies reside provide adequate protection for personal data.
- The EDPB has created two task forces following Schrems II, one of which will consider appropriate supplementary measures for the transfer of personal data to third countries; the EDPB's recommendations may apply to BCRs as well as SCCs

ADR Can Help

Many businesses contract with others who in their services process data.

If something goes wrong how do you want to resolve disputes with your contractors?

Tensions

Personal rights of the Data Subject v. Contractual Sphere v. Public Authorities & DPA's

- ADR is possible in all of these relationships, taken separately
- More complicated when they interfere with one another
- ADR may be difficult or even impossible if certain administrative or Court procedures have been initiated.

Roles & Responsibilities

- Controller
- Joint Controller
- Processor

Three types of relationships

- Data processing agreement (between controller and processor)
- Data exchange agreement (between controller and controller)
- Data sharing agreement (between joint controllers)

Tendency: Case Law and EPDB see parties rapidly as joint controller

- Joint liability (*in solidum*)
- Requalification of data processing agreement to data sharing agreement
- Requalification of data exchange agreement to data sharing agreement

Joint controller: Option to shift liabilities?

Likely. Parties can agree on limitation of liability *inter partes*

Caveat: Art. 26(3) and 82(4) GDPR

- Art. 26(3) Data subject may exercise his or her rights under the GDPR in respect of and against each of the controllers
- Art. 82(4): Each controller shall be held liable for the entire damage in order to ensure effective compensation of the data subject

Authorities can sanction each of the joint controllers

(See Art 83 GDPR & 29 WP Guidelines on administrative fines)

- Actions taken to mitigate damage
- Degree of responsibility
- Degree of cooperation with supervisory authority
- History of infringements
- …

ADR is useful for resolving disputes :

- Obtain conservative measures (freeze information)
- Contractual determination of roles and responsibilities
- Cooperation in resolving data breaches
- Damage recovery
- Consequences of requalification of data processing/exchange agreement by DPA
- Finding alternatives for Privacy Shield with the help of an expert (expert determination)
- …

ADR Mechanisms

- Mediation
- Mediation organised by the DPA
- Emergency arbitrator
- Expert determinator
- Arbitrator
- Expedited arbitration

Stimulus for out of Court settlements with Data Subjects

- Codes of conduct.
- Art. 40 GDPR: "Associations and other bodies representing categories of controllers or processors may prepare codes of conduct [...] such as with regard to [...] out-of-Court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79"
- Public nature of Court proceedings may be incompatible with the relief the data subject is looking for
- DPAs provide for mediation

Challenges

- Obtaining Data Subject's consent to out of Court dispute resolution
- What about ADR between controllers, joint controllers & processors?
  - Not provided for in GDPR
  - Not to be used to escape from duties under the GDPR

Challenges for ADR in the context of data protection

- Jurisdictional scope
- Use of personal data in ADR proceedings itself
  - International Council for Commercial Arbitration (ICCA) and International Bar Association (IBA) created a 'roadmap' for arbitration (https://www.arbitration-icca.org/media/14/18191123957287/roadmap_28.02.20.pdf)
  - How to handle objections to disclosure based on data protection?

Challenges for ADR in the context of data protection

- No possibility for preliminary rulings
  - Uniform application of EU Law?
  - Public order ground to annul legal instrument resulting from ADR?
- Data protection v. removing trade barriers
- Investor State Dispute Settlement

Venner Shipley LLP
200 Aldersgate
London EC1A 4HD

Tel: +44 (0) 207600 4212
Fax: +44 (0) 2076004188
Email: jtumbridge@vennershipley.co.uk

For more information about our firm please visit www.vennershipley.co.uk

End

Venner Shipley