MAYER·BROWN

GDPR and the Privacy Shield

Mark Prinsley
Partner

+44 20 3130 3900
mprinsley@mayerbrown.com

Kendall Burman
Counsel

+ 202 263 3210
kburman@mayerbrown.com

Speakers

Kendall Burman
Counsel – Washington DC

Mark Prinsley
Partner - London

MAYER·BROWN

LATEST GUIDANCE ON NEW OBLIGATIONS IN THE GDPR

The General Data Protection Regulation

- "Go live" in May 2018
- Harmonised position across the member states
- Guidance on interpretation of the regulation emerging from advisory bodies
- Key areas:
  - additional compliance obligations on data controllers
  - additional rights of data subjects

The General Data Protection Regulation

- Specific topics:
  - Data Protection Officers (DPOs)
  - Data Privacy Impact Assessments (DPIAs)
  - Data Portability Right
  - Consent

Do We Need to Appoint a Data Protection Officer?

- Applies to both controllers and processors
  - Public authorities required to appoint DPOs
  - For private-sector entities, the test is:
    - Does the core activity of the entity involve regular and systematic monitoring of data subjects on a large scale?
    - Does the core activity consist of large-scale processing of "sensitive personal data?"
  - Article 29 Working Party Guidance on meaning of:
    - "core activities"
    - "large-scale"
  - Possibility of voluntarily appointing a DPO

Location and Qualifications of the DPO

- Location:
  - Guidance that the DPO should be located within the EU, even if the controller or processor is located outside the EU
- Qualifications:
  - No minimum standard of qualifications required – related to the nature of the processing operations being carried out, **but** must have a deep understanding of the regulatory framework (the GDPR)
  - Other duties must not give rise to a conflict of interest

The Role of the DPO

- Involvement in all issues relating to data privacy in the business and monitor compliance with the GDPR
- Part of “privacy by design”
- “The opinions of the DPO must be given due weight”
- Involvement in all data breach incidents
- Responsible for liaising with the Supervisory Authority

Data Privacy Impact Assessments

- Where processing involves “high risk” to the rights and freedoms of individuals, the data controller should conduct an assessment of the impact of the processing operations on the protection of personal data (Article 35 GDPR)
- National Supervisory Authorities required to publish lists of types of processing activities that are subject to requirement for DPIA, GDPR targets:
  - systematic and extensive evaluation of personal data
  - large-scale processing of special-category personal data
  - systematic monitoring of a publicly accessible area on a large scale
- Fines of up to €10 million / 2 percent of revenue for not carrying out a DPIA where appropriate
- If the DPIA indicates a high risk in the absence of steps to mitigate risks by the data controller, the National Supervisory Authority must be consulted

Article 29 Working Party Guidance on "High Risk" Processing

Factors for National Supervisory Authorities to consider:

Evaluation or scoring/processing	Automated decision-making with legal significant effect
Systematic monitoring	Use of sensitive data
Data processed on a large scale	Datasets that are matched
Data concerning vulnerable data subjects	Innovative use or applying technological or organisational solutions
Data transfers out of the EU	Processing that prevents individuals from exercising a right or using a service or a contract

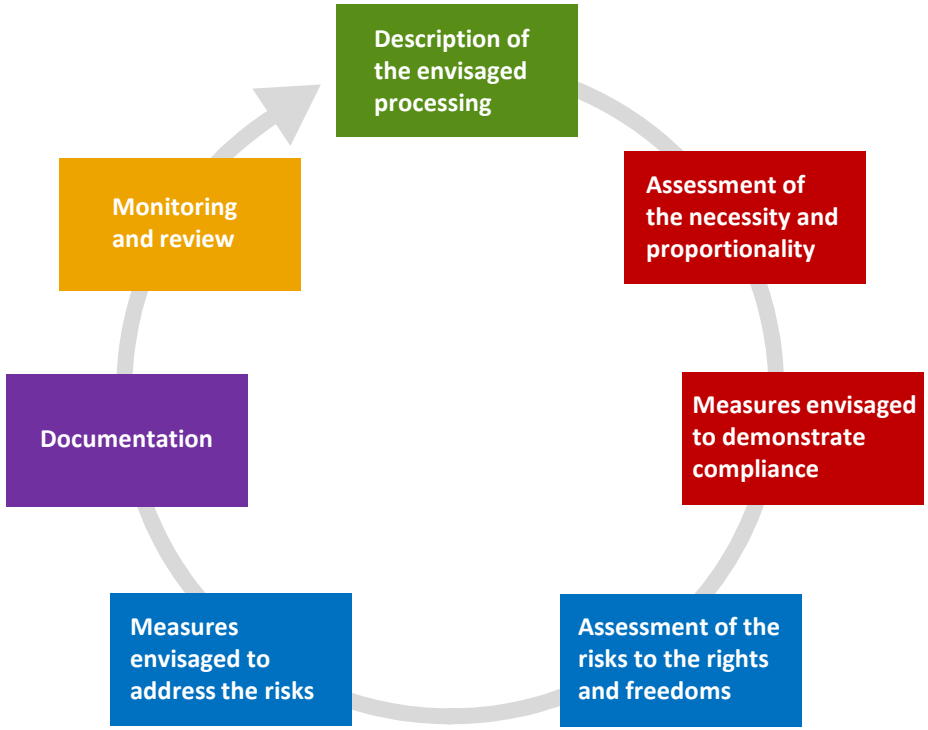
"Rule of thumb" – if two or more of the above factors are present, a DPIA should be conducted

Article 29 Working Party Examples

Examples of Processing	Possible Relevant Criteria	DPIA Required?
A hospital processing its patients' genetic and health data (hospital information system).	- Sensitive data - Data concerning vulnerable data subjects	Yes
The use of a camera system to monitor driving behaviour on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognise licence plates.	- Systematic monitoring - Innovative use or applying technological or organisational solutions	
A company monitoring its employees' activities, including the monitoring of the employees' work station, Internet activity, etc.	- Systematic monitoring - Data concerning vulnerable data subjects	
The gathering of public social media profile data to be used by private companies generating profiles for contact directories.	- Evaluation or scoring - Data processed on a large scale	
An online magazine using a mailing list to send a generic daily digest to its subscribers.	- (none)	Not necessarily
An e-commerce website displaying adverts for vintage car parts that involve limiting profiling based on past purchasing behaviour on certain parts of its website.	- Evaluation or scoring, but not systematic or extensive	

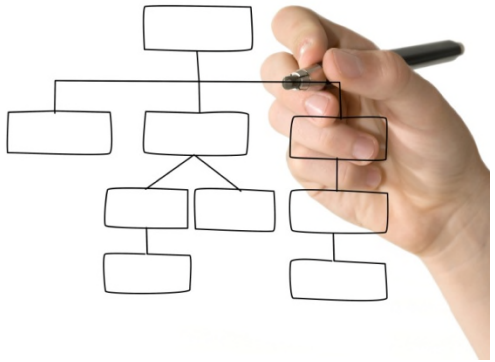
Article 29 Working Party Guidance on Generic Steps in a DPIA

It should be underlined that the process depicted here is *iterative*: in practice, it is likely that each of the stages is revisited multiple times before the DPIA can be completed.



What Should You Do Now?

- Article 29 Working Party's strong recommendation to start conducting DPIAs prior to May 2018
- Consider common processing activities for which one DPIA may be sufficient
- Producers of new technologies should consider producing generic DPIAs for the technology to provide to users of their technology/products



Data Subject's Right to Data Portability

- The data subject has the right to receive personal data concerning him or her that he or she has provided to the data controller in a structured, commonly used format and shall have the right to transmit the data to another controller where the processing is based on consent or a contract and is automated means (Article 20 GDPR)
- Article 29 Working Party guidance on:
  - Scope of data "provided to the data controller"
    - Data provided includes "observed data"
    - Status of "derived data" and "inferred data"
  - Importance of the basis on which the data is being processed (e.g., collection of KYC data)

What Should data controllers be Doing about the Data Portability Right?

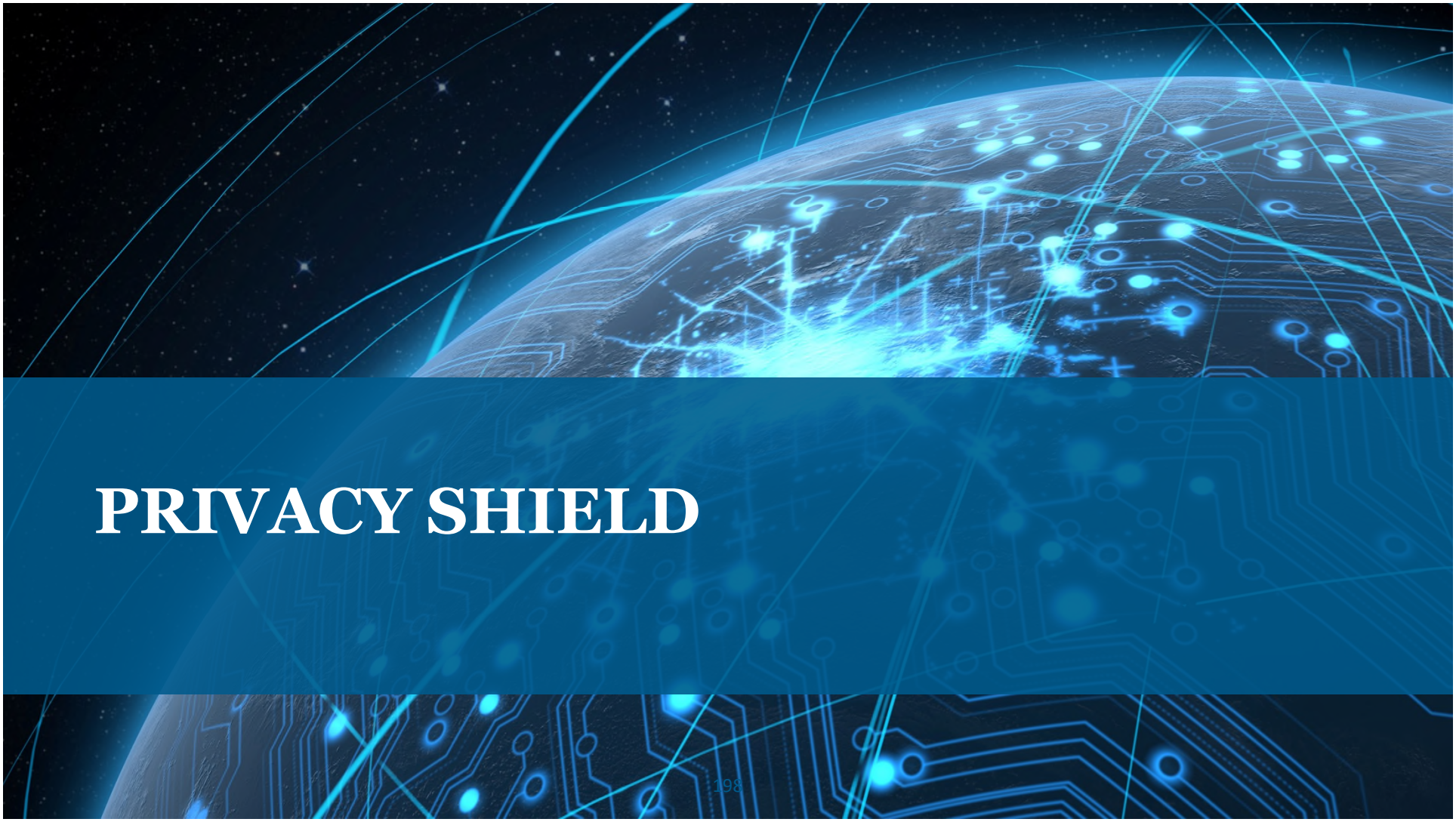
- The "Disclosing" Data Controller
  - Review terms of business to ensure clarity as to the scope of personal data subject to the data portability right
  - Establish technical measures for providing the data in an appropriate form
  - Be clear about the basis upon which personal data will be processed
  - Establish procedures for dealing with requests to port data within one month of the request
- The "Recipient" Data Controller
  - Clarity as to whether the data is received as a controller or as a processer
  - Establish appropriate controls on how the data is used – take care not to enrich other data without first obtaining consent

Consent as a Basis for Processing

- "Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 4 GDPR)
- New features to "consent"
  - must be "unambiguous"
  - requires "statement or clear affirmative acti

What should Data Controllers be Doing Now?

- Guidance from the UK Information Commissioner's Office:
  - no need to repaper existing consents (provided the existing consent meets the GDPR standards)
  - consents should be unbundled from other terms and conditions relating to the service or offering
  - use active opt ins, not opt outs
  - make the withdrawal of consent process straightforward
- Balance the benefits of relying on consent as the basis for processing
  - relying on consent means the data subject definitely has rights to erasure and data portability



PRIVACY SHIELD

What to Expect for Privacy Shield and Model Clauses

- GDPR, like the EU directive, permits data transfers to countries with adequate protection OR use of approved means:
  - EU Model Clauses
  - Privacy Shield Certification
  - Binding Corporate Rules
  - Derogations
- Being Privacy Shield certified and entering into EU Model Clauses with the data controller are the two most common mechanisms used to transfer personal data from the EU to the US

What are Privacy Shield and Model Clauses?

Privacy Shield

- Self-certification of US companies to the Department of Commerce
- Must be subject to jurisdiction of FTC or DOT who enforces commitments
- Privacy Shield Principles: Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse Enforcement and Liability
- Requires policy and operational changes

Model Clauses

- Different contractual clauses to be used by EU companies for transfers of data to non-EU companies (data controller to data controller/data controller to data processor)
- Clauses cannot be revised or changed
- Creates liability giving data subject the direct right of action

Privacy Shield "Onward Transfer" Principle

- The onward transfer principle addresses how Privacy Shield certified companies must protect personal information that they transfer onto other data controllers or to third-party agents. How does the onward transfer principle function under Privacy Shield?
  - Different requirements for data processors and agents (No recourse mechanism for processors)
  - Transfers must be pursuant to contract and must offer "equivalent" protections to Privacy Shield

Crystal Ball: What Does the Future Hold for Privacy Shield and Model Clauses?

- Various forms of EU review:
  - Litigation in the EU around Privacy Shield and Model Clauses
  - Annual review of Privacy Shield framework
- Status of US privacy protections:
  - Acting ombudsperson within State Department
  - Changes in Privacy Act protections for EU citizens
  - Presidential Policy Directive 28 limiting surveillance on non-US persons

QUESTIONS?

Mark Prinsley
Partner

+44 20 3130 3900
mprinsley@mayerbrown.com

Kendall Burman
Counsel

+ 202 263 3210
kburman@mayerbrown.com