Morgan Lewis

GDPR CHECKLIST

PROTECTING PERSONAL DATA

PRACTICAL CONSIDERATIONS

The General Data Protection Regulation (GDPR) significantly changes how companies may collect and use the personal data of individuals in the European Union. Penalties for violating GDPR are steep. Consider these steps to point you in the direction of compliance and let Morgan Lewis lawyers provide more detailed analysis and advice.

1. DETERMINE AUTHORITY

- Determine lead supervisory authority—where is the main establishment for processing

2. PRIVACY IMPACT ASSESSMENT (PIA)

- Required if processing likely to result in high risk to rights and freedoms of subjects or systematic monitoring or profiling
- Consider if PIA is recommended given compliance profile of organisation

3. KEY DATA PRIVACY DOCUMENTS

- Consents in employment contracts
- Consents in commercial contracts
- Employee and customer privacy policies
- Cybersecurity policy
- Website user policy
- Privacy Notice/Information Notice
- Subject access procedure
- Rectification, blocking, and deletion of data procedure
- Data portability procedure

4. PRIVACY NOTICE

Data controller must provide the Privacy Notice in advance or at the time of processing or, if it was collected via a third party, within a reasonable period of being collected. The Privacy Notice should include the following:

- The identity and contact details of the data controller and where applicable, the data controller's representative) and the data protection officer
- The purpose of the processing and the legal basis for the processing
- The legitimate interests of the controller or third party, where applicable
- The categories of personal data
- Any recipient or categories of recipients of the personal data
- The details of transfers to a third country (e.g. US) and method of transfer such as model clauses or other data transfer agreements
- The retention period
- The data subject's rights relating to the processing such as the right of access and rectification
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority
- The source of the personal data and whether it came from a publicly accessible source
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
- The existence of any automated decisionmaking, including profiling and information about how decisions are made, and the significance and consequences of such decisions

The Privacy Notice must be concise, transparent, intelligible, and easily accessible; written in clear and plain language; and provided free of charge.

5. CONSENTS

Retain records of consent where relied on for processing

6. DATA TRANSFERS

Data transfers from European affiliates to affiliates outside the EEA in countries with "inadequate"[1] data protection laws:

- Notice or consent
- Model clauses (controller-controller; controller-processor[2])
- Binding Corporate Rules
- Approved Code of Conduct
- Privacy seal/certificate

7. RECORDS OF DATA PROTECTION COMPLIANCE

- Training of staff
- Policies and procedures
- Information security and data breach procedures
- Privacy by design and privacy by default processes or systems
- PIAs

8. DATA TRANSFERS TO VENDORS/ SUBCONTRACTORS

- Minimum data protection obligations:
  - Process the personal data only on their instructions
  - Keep the personal data confidential
  - Comply with the data controller's data security obligations under Article 32 of the GDPR
  - Take appropriate technical and organisational measures to allow the data controller to comply with data subjects' rights under the GDPR
  - Restrict the engagement of sub-processors
  - Assist the data controller in complying with its obligations relating to data security, notification of a data breach, and conducting a data protection impact assessment and any obligations to consult a supervisory authority before high-risk processing
  - Comply with the data controller's request to delete or return the personal data at the end of the provision of the services
  - Notify the data controller of any breach of the above obligations
  - Allow the data controller to have access to the data processor's systems or facilities and otherwise provide information to demonstrate compliance with the above obligations
- Data transfers from European affiliates to third parties based outside EEA in countries with "inadequate"[3] data protection laws:
  - Notice or consent
  - Model clauses (controller-processor; processor-processor if approved)

9. DPO OR APPOINTMENT OF EU REPRESENTATIVE (for non-EU organisations)

- DPO if core activities of business include regular and systematic monitoring on a large scale or processing of special categories[4] of data on a large scale; DPO must implement training on data protection
- Appoint EU representative if not based in EU (consider indemnifying the representative)

10. DATA RETENTION PERIOD

- Notice of retention period
- Internal process to administer deletion of personal data

11. DATA SUBJECT RIGHTS

- Procedure for responding to subject access requests within 30 days
- Procedure for deleting/rectifying/restricting access to data and to implement right to be forgotten
- Procedure to give a copy of data to subject or another controller in a commonly used machine readable format

12. RECORDS

Controllers and processors (unless less than 250 employees, provided processing does not carry a risk to rights and freedoms of data subjects and no special categories of data or criminal record data is stored) to keep records of processing activities, details of any joint controllers, categories of personal data and of data subjects, recipients where data is transferred, retention periods, technical and organisational security measures to secure data, and any DPO or appointed representative

13. DATA BREACH PROCESS

- Process to manage data breach and investigate without undue delay and within 72 hours unless no risk to rights and freedoms of subjects for serious incidents
- Controllers to notify:
  - Data protection authority
  - Individuals affected by breach if high risk to their rights and freedoms
  - Third parties e.g. clients
- Processor to notify controller without undue delay

---

[1] Countries deemed to be "adequate" by the European Commission other than the EEA are: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay. Countries under consideration are South Korea and India.

[2] Processor-processor clauses may be approved by European Commission.

[3] See footnote 2 above.

[4] Special categories of data are racial or ethnic data, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, sex life data and/or sexual orientation data.

Morgan Lewis

At Morgan Lewis, we're always on and always ready to respond to the needs of our clients.

PRIMARY CONTACTS

Pulina Whitaker | London
pulina.whitaker@morganlewis.com
+44.20.3201.5550

Tess Blair | Philadelphia
tess.blair@morganlewis.com
+1.215.963.5161

Walter Ahrens | Frankfurt
walter.ahrens@morganlewis.com
+49.69.714.00.766

Charles Dauthier | Paris
charles.dauthier@morganlewis.com
+33.1.53.30.44.74

Mark Krotoski | Silicon Valley
mark.krotoski@morganlewis.com
+1.650.843.7212

Gregory Parks | Philadelphia
gregory.parks@morganlewis.com
+1.215.963.5170

Dr. Axel Spies | Washington, DC
gaxel.spies@morganlewis.com
+1.202.373.6145

Ronald Del Sesto, Jr. | Washington, DC
ronald.delsesto@morganlewis.com
+1.202.373.6023

Connect with us

www.morganlewis.com

101618_181967_A4