Morgan Lewis

GDPR COMPLIANCE CHECKLIST

PROTECTING EU AND UK PERSONAL DATA

PRACTICAL CONSIDERATIONS

The EU and UK General Data Protection Regulation (GDPR) significantly impacts how organisations, whether or not established in Europe, may collect and use personal data relating to individuals in Europe or European business operations. GDPR violations may result in significant regulatory fines (including direct liability for group parent companies) and private litigation (including collective litigation).

Consider these steps to point your organisation in the direction of compliance and consult Morgan Lewis lawyers (including a former senior enforcement lawyer at a European data protection regulator) for more tailored analysis and advice.

1 GDPR AND EPRIVACY LAW APPLICATION

- Map how personal data is collected, used, and otherwise processed, notably, if involving:
  - "Special" and sensitive categories of data[1]
  - Healthcare, clinical trial, biometric, or genetic data
  - Criminal offences and law enforcement data
  - Social media and telecom-related data
  - Banking, payment, and financial data
  - Children and vulnerable individuals
  - CCTV, surveillance, and facial recognition data
  - Artificial intelligence and machine learning technologies
  - Automated decision-making and profiling
  - Employee and workplace monitoring
  - Connected consumer devices and IoT
  - AdTech, cookies, and tracking technologies
  - Electronic and telephone marketing
  - Transfers of personal data to other organisations
  - Transfers of personal data outside Europe
- Determine whether the organisation is subject to the GDPR, European ePrivacy laws, and/or additional sector-specific data protection laws.
- Determine whether the organisation is a "controller" or "processor" with regard to specific data processing activities.
- Determine whether the data processing is lawful, and if so, identify the lawful basis (e.g., data subject consent, legal obligation, or legitimate interest).
- Determine which GDPR supervisory authority will regulate and whether the organisation may designate a lead supervisory authority.

2 DATA PROTECTION AND COOKIE NOTICES

- Controller should promptly provide a GDPR-compliant data protection notice to individuals. The GDPR is prescriptive as to what information is required in such notices.
- If an organisation uses cookies or other tracking technologies or conducts electronic marketing, it may need to provide notices and obtain opt-in consents.

[1] Special categories of data include 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.

3 KEY POLICIES AND DOCUMENTATION

Develop relevant GDPR and related policies and implement procedures to effect such policies, e.g.:

- Record of Processing Activities (ROPA)
- Template data subject consents
- Legitimate Interest Assessment (LIA)
- Data Protection Policy
- Information Security Policy
- Incident Response Plan (IRP)
- Business Continuity and Disaster Recovery Plan (BCDRP)
- GDPR staff training materials and records
- Data subjects rights policies, e.g., requests seeking:
  - Access to data (within 30 days)
  - Data deletion and rectification
  - Data porting to third parties
- Data retention and deletion policies
- Template "data processing agreement"
- Records of consents granted by data subjects
- EU representative appointment
- Personal data breach log

4 PRIVACY IMPACT ASSESSMENT (PIA)

Controller should conduct a PIA if processing could result in a "high risk" to data subjects or systematic monitoring or profiling.

5 DATA TRANSFERS OUTSIDE EUROPE

Consider necessary steps for data transfers to countries outside Europe (whether to affiliates, vendors, or business partners) if (1) the country is on an approved list (e.g., Canada, New Zealand, or South Korea) *or* (2) if not, any of the following legal mechanisms applies to such transfer:

- Use of model/standard contractual clauses approved by the European Commission and/or the UK Information Commissioner's Office (ICO)
- Certification to the EU-US Data Privacy Framework (DPF) and UK-US Data Bridge
- Reliance on binding corporate rules (supervisory authority–approved data transfer arrangements)
- Supervisory authority–approved codes of conduct
- Reliance on specific exceptions (derogations), e.g., obtaining data subject consent, in limited circumstances

Organisations should undertake transfer risk assessments when relying on one of the above legal transfer mechanisms to demonstrate that they are satisfied that the relevant GDPR protections are not undermined. Importantly, Brazil, India, the People's Republic of China, Russia, South Africa, and the United States are *not* on the list of approved countries.

6 DATA PROCESSING CHAINS

The GDPR imposes obligations on controllers where data will be processed by other organisations (whether controllers or processors) in a data processing chain.

- Conduct GDPR diligence on vendors and subcontractors (processors) *and* enter into data processing agreements prescribed by the GDPR.
- Consider whether a data sharing agreement is needed relative to other controllers (e.g., data sharing in relation to clinical trials).

7 DATA PROTECTION OFFICER (DPO)

Appoint a DPO if, for example, core business activities include regular and systematic monitoring on a large scale or processing of special categories of data on a large scale. The DPO should have a key role in the organisation's information governance.

8 DATA BREACH RESPONSE PROCESS

- Regularly test the IRP and BCDRP.
- If a personal data breach occurs, controller must "without undue delay" notify (i) relevant supervisory authority(ies) and (ii) impacted data subjects, to the extent required by the GDPR.
- Processor must notify controller "without undue delay."
- Perform other necessary or appropriate incident remediation tasks

Morgan Lewis

At Morgan Lewis, we're always ready to respond to the needs of our clients and craft powerful solutions for them.

PRIMARY CONTACTS

Vishnu Shankar
London | Brussels
vishnu.shankar@morganlewis.com
+44.20.3201.5558 | +32.2.507.7500

Scott A. Milner
Philadelphia
scott.milner@morganlewis.com
+1.215.963.5016

Dr. 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

Megan A. Suehiro
Los Angeles
megan.suehiro@morganlewis.com
+1.213.612.7324

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

Ezra D. Church
Philadelphia
ezra.church@morganlewis.com
+1.215.963.5710

Kristin M. Hadgis
Philadelphia
kristin.hadgis@morganlewis.com
+1.215.963.5563

Dr. Axel Spies
Washington, DC | Frankfurt
axel.spies@morganlewis.com
+1.202.373.6145 | +49.69.714.00.777

Connect with us

www.morganlewis.com

04092024_240842_A4