

# GDPR Compliance Checklist

---



This GDPR Compliance Checklist sets out the key requirements that the General Data Protection Regulation will introduce into EU Privacy law on 25 May 2018. The table summarizes the nature of the provision, highlights the most important actions which organizations should take to prepare for compliance, and provides reference to the relevant Article in the GDPR (these can be cross referred to in *Latham & Watkins' General Data Protection Regulation at a Glance*).

The GDPR will apply to companies processing personal data in the context of an EU establishment, companies offering goods or services to EU residents and companies that monitor the behavior of EU residents.

The changes brought in by the GDPR are wide-reaching and a number of functions within many organizations will be affected by the changes, from marketing to security and, of course, legal and compliance. This checklist aims to identify, below, the stakeholders which will need to be involved in each set of actions.

- Legal
- Compliance
- HR
- IT & Information Services
- Insurance
- Security
- Procurement
- Marketing and Customer Relations
- PR & Comms

This table has been created with a B2C company in mind, *i.e.* a company obtaining, processing and storing quantities of consumer data. If an organization is B2B, while there may be certain areas where the obligations are slightly less onerous (and are less likely to require marketing and customer relations involvement), many of the requirements will still stand.

## Contacts



**Gail Crawford**

*Partner*  
+44.20.7710.3001  
gail.crawford@lw.com







**Fiona Maclean**

*Senior Associate*  
+44.20.7710.1822  
fiona.maclean@lw.com



**Lore Leitner**

*Senior Associate*  
+44.20.7710.4785  
lore.leitner@lw.com

	Action(s) / Deliverable(s)	Description of GDPR Requirement	Applicable GDPR Article(s)
<b>Governance</b> 	<ul style="list-style-type: none"> <li><input type="checkbox"/> Document your Privacy Governance Model e.g. with clear roles and responsibilities and reporting lines to embed privacy compliance into the organization</li> <li><input type="checkbox"/> Consider whether a statutory DPO is required</li> <li><input type="checkbox"/> If no EU presence, appoint a local representative</li> <li><input type="checkbox"/> Develop and roll out training across all personnel</li> <li><input type="checkbox"/> Review insurance coverage and consider whether it needs to be updated in light of the higher fines and penalties under the GDPR</li> </ul>	<p>One of the underlying principles of the GDPR is to ensure that organizations place data governance at the heart of what they do. As a result, the GDPR introduces a number of requirements to ensure that compliance is a serious focus for companies.</p> <p>Within the organization, it is important to raise awareness of privacy issues to embed privacy compliance into the mind-set of employees so that the business is proactive not reactive.</p>	5, 27, 37-39
<b>Accountability</b> 	<ul style="list-style-type: none"> <li><input type="checkbox"/> Implement a global overarching data protection policy, which brings together all underlying related policies including processes for privacy by design and the creation and maintenance of a record of processing activities (see below)</li> <li><input type="checkbox"/> Integrate privacy compliance into the audit framework</li> </ul>	<p>One of the threads which runs through the GDPR is the requirement for organizations to have documentation to be able to demonstrate how they comply with the GDPR. Compliance should be integrated within the audit framework to ensure policies, processes and controls are working.</p>	5, 24, 25, 30
<b>Fair Processing and Consent</b> 	<ul style="list-style-type: none"> <li><input type="checkbox"/> Review your existing grounds for lawful processing and confirm that these will still be sufficient under the GDPR e.g. can you still rely on consent given the new requirements?</li> <li><input type="checkbox"/> Consider whether your organization is processing any sensitive personal data and ensure the requirements for processing such data are satisfied</li> <li><input type="checkbox"/> Where consent is relied upon as the ground for processing personal data, review existing consents to ensure they meet the GDPR requirements, and if not implement a process to seek new consents</li> <li><input type="checkbox"/> Ensure systems can accommodate withdrawal of consent</li> </ul>	<p>In order to lawfully process personal data, one of the conditions of processing, as set forth in the GDPR, must be satisfied. While the grounds for processing are broadly the same as those set out in the current Data Privacy Directive, the GDPR imposes new requirements to gain valid consent. Consent can be withdrawn at any time and systems must be able to handle withdrawal requests. Under the GDPR, privacy notices must state the processing ground relied upon, and if relying on legitimate interests, state the nature of the legitimate interest.</p> <p>Consider whether the specific requirements relating to consent from children apply to your organization (see <i>Children</i>).</p>	5, 6, 7, 9, 10, 85- 91
<b>Notices / Vetting - HR</b> 	<ul style="list-style-type: none"> <li><input type="checkbox"/> Review and update, where necessary, employee notices to be GDPR compliant</li> <li><input type="checkbox"/> If you currently conduct criminal records checks, review national laws to ensure you can continue to do so</li> </ul>	<p>There is an emphasis on transparency in the GDPR. Notices must be clear, concise and informative. Employees must be adequately informed of all data processing activities and data transfers and the information set out in Articles 13 to 14 must be provided. Criminal records can no longer be processed unless authorized by member state law.</p>	10, 12-14



## Notices - Customers



- Review and update, where necessary, customer notices to be GDPR compliant
- Consider whether your notices have to accommodate “child-friendly requirements” (see *Children*)

There is an emphasis on transparency in the GDPR. Notices must be clear, concise and informative. Customers must be adequately informed of all data processing activities and data transfers and the information set out in Articles 13 to 14 must be provided. Notices must also be compliant with the new Consent requirements where relying on consent as your lawful ground of processing.

12-14

## Children



- Identify whether you process personal data of children
- Seek local counsel advice regarding applicable local law restrictions, codes and guidance
- If data relating to a child will be processed, ensure that notices directed at that child are “child-friendly” and if consent is relied upon, you have implemented a mechanism to seek parental consent
- Consider alternative protections, e.g. age-gating

The GDPR requires parental consent for the processing of data related to information society services offered to a “child” (ranging from 13 to 16 years old depending on member state). The GDPR leaves a lot to the discretion of the member states as to how children must be treated under this provision.

8, 12

## Data Subject Rights and Procedures



- Update data privacy policy and internal processes for dealing with requests.
- Ensure technical and operational processes are in place to ensure data subjects’ rights can be met, e.g. right to be forgotten, data portability and the right to object (see *Governance and Accountability*)

Data subjects are given more extensive rights under the GDPR. The current rights to request access to data or require it to be rectified or deleted have been expanded to include a much broader right to require deletion (“the right to be forgotten”), a right not just to access your data but have it provided to you in a machine readable format (“data portability”). Versions of the existing right to object to any processing undertaken on the basis of legitimate interests or for direct marketing and the right not to be subject to decision based on automated processing are also included and expressly refer a right to object to profiling. These must be clearly communicated in the notices given to data subjects, e.g. privacy policy.

16, 17, 18,  
19, 20, 21,  
22, 23

## Record of Processing



- Identify all data processed in a detailed Record of Processing
- Implement and maintain processes for updating and maintaining Record of Processing

The GDPR requires organizations to maintain a detailed record of all processing activities, including purposes of processing, a description of categories of data, security measures, comprehensive data flow map, etc. A number of stakeholders will need to be involved in creating and maintaining this data record.

30

## Privacy by Design and Default



- Ensure processes are in place to embed privacy by design into projects (e.g. technical and organizational measures are in place to ensure data minimization, purpose limitation and security)

In keeping with the GDPR’s objective of bringing privacy considerations to the forefront of organizations’ decision making, the GDPR requires data protection requirements to be considered when new technologies are designed or on boarded

25, 35, 36

- Put in place a privacy impact assessment protocol

or new projects using data are being considered. Privacy impact assessments should be used to ensure compliance; these are required for projects that involve processing, on a large scale, of sensitive personal data or criminal convictions, monitoring of a public area or systematic and extensive evaluation by automated means including profiling.

**Compliant Contracting and Procurement**



- Develop compliant contract wording for customer agreements and third-party vendor agreements
- Identify all contracts that require relevant contract wording, prioritize and develop process for amending
- Ensure procurement process has controls to ensure privacy by design (e.g. security diligence, data minimization, visibility of onwards data flows)

Procurement processes and vendor contracts will need to be updated to ensure they reflect the new GDPR requirements and flow down obligations which must be complied with by parties processing European personal data on your behalf.

N/A

**Data Breach Procedures**



- Review and update (or develop where not in existence) Data Breach Response Plan
- Review insurance coverage for data breaches and consider whether it needs to be updated in light of the higher fines and penalties under the GDPR
- Review liability provisions in agreements for breaches caused by service providers and other partners

The GDPR introduces a new data breach notification regime. The process requires organizations to act quickly, mitigate losses and, where mandatory notification thresholds are met, notify regulators and affected data subjects.

32-34

**Data Export**



- Identify all cross-border data flows and review data export mechanisms
- Update cross border mechanisms if necessary

The GDPR only permits exports of data to entities of its group and third-party vendors outside the European Economic Area if the country in which the recipient of such data is established offers an adequate level of protection.

44-50