



General Data Protection Regulation (GDPR) Checklist

LATHAM & WATKINS

Overview of the GDPR

- The General Data Protection Regulation (“**GDPR**”) comes into force on 25 May 2018 and has wide-reaching implications for businesses.
- Critically, **finances under the GDPR will be significant** – regulators may now fine companies up to **EUR 20 million or 4% of global turnover** for non-compliance.
- As a result, business data privacy compliance will raise issues similar to anti-corruption and antitrust compliance.
- The GDPR will **apply to companies based both inside and outside of Europe**, including:
 - companies processing personal data in the context of an EU establishment
 - companies offering goods or services to EU residents;
 - companies that monitor the behaviour of EU residents; and
 - companies providing services to the above.
- **Data is increasingly central to business operations, and data is obtained from many sources.** The changing nature of technology, in particular through the increased connectivity of the internet of things, means that companies are collecting, processing and exploiting data in new and evolving ways. Complex supply chains also mean that data is increasingly being collected by one party, but being used by others without appropriate assurances about the collection procedure. If not properly managed, this data can be a critical liability.

GDPR Compliance Checklist


- This GDPR Compliance Checklist seeks to provide a high level overview of the key requirements of the GDPR.
- The table summarises the nature of the provision, highlights the most important actions which organisations should take to prepare for compliance and provides reference to the relevant Article in the GDPR. It also identifies the functions that will be affected by the changes in law and notes the stakeholders which will need to be involved in each set of actions.




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




- This table **assumes a B2C environment** and therefore a company obtaining, processing and storing quantities of consumer data.
- If **your organisation has a B2B focus**, while there may be certain areas where your obligations are slightly less onerous (and are less likely to require marketing and customer relations involvement), many of the requirements will remain applicable.



What We Can Do for You



- We recommend that companies should implement a compliance project to review their structure, governance model, processes and procedures to avoid substantial sanctions.
- We can assist with this by preparing a comprehensive and tailored global data privacy programme to help you plan for, and implement, these changes within your organisation.
- We aim to help companies prepare for the GDPR with the following key objectives in mind:
 - to reduce **risk of enforcement action and fines**,
 - to reduce the **risk of adverse publicity** associated with any breach of data protection laws,
 - to reduce the financial exposure for breaches of confidentiality,
 - to implement rules on use of data, enabling companies to **exploit data more efficiently and in compliance with law**, and
 - to ensure, where possible, that consistent processes and procedures are adopted globally to reduce the administrative burden.

	Action(s) / Deliverable(s)	Obligation as a Controller (C), Processor (P) or both (CP)	Description of GDPR Requirement	Applicable GDPR Article(s)
Governance 	<input type="checkbox"/> Document your Privacy Governance Model e.g., with clear roles and responsibilities and reporting lines to embed privacy compliance into the organisation, and address situations where there may be conflicting objectives internally (e.g. between marketing and legal functions)	(CP)	<p>One of the underlying principles of the GDPR is to ensure that organisations 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 organisation, it is important to raise awareness of privacy issues and embed privacy compliance into decision makers and rank-and-file alike so that the business is proactive not reactive.</p>	5, 27, 37-39
	<input type="checkbox"/> Consider whether a statutory DPO is required	(CP)		
	<input type="checkbox"/> If no EU presence, appoint, a local representative	(CP)		
	<input type="checkbox"/> If carrying out cross-border processing across EU member states, consider which member state will be the lead data protection supervisory authority for your organisation (i.e., the location of your central EU administration or where the most significant decisions about data processing takes place)	(CP)		
	<input type="checkbox"/> Develop and roll-out training across all personnel to ensure understanding of data protection principles, responsibilities, risks, etc.	(CP)		
	<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	(CP)		

	Action(s) / Deliverable(s)	Obligation as a Controller (C), Processor (P) or both (CP)	Description of GDPR Requirement	Applicable GDPR Article(s)
Record of Processing 	<input type="checkbox"/> Identify all data processed in a detailed Record of Processing, e.g., document what personal data is held by your organisation, where it came from, and who it is shared with <input type="checkbox"/> Implement and maintain processes for updating and maintaining Record of Processing	(CP) (CP)	The GDPR requires organisations 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
Accountability 	<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 above) <input type="checkbox"/> Integrate privacy compliance into your audit framework	(CP) (CP)	One of the threads which runs through the GDPR is the requirement for organisations 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.	5, 24, 25, 30
Fair Processing and Consent 	<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?) and ensure that the lawful basis for processing is explained in the privacy policy <input type="checkbox"/> Consider whether your organisation is processing any sensitive personal data and ensure the requirements for processing such data are satisfied	(C) (C)	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 must be freely given, specific, informed, and unambiguous. There must be positive opt-in (consent cannot be inferred from silence), consent must be separate from other terms and conditions, and simple options to withdraw consent must be available.	5, 6, 7, 9, 10, 85-91

Action(s) / Deliverable(s)	Obligation as a Controller (C), Processor (P) or both (CP)	Description of GDPR Requirement	Applicable GDPR Article(s)
<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 <input type="checkbox"/> Ensure systems can accommodate withdrawal of consent	(C) (P – through the contract with C)	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. This will be important as individuals’ rights will be different depending on the lawful basis for processing, e.g., there will be a stronger right to be forgotten where consent is used as the lawful basis. Consider whether the specific requirements relating to consent from children apply to your organisation (see <i>Children</i>).	
Notices / Vetting - HR  <input type="checkbox"/> Review and update, where necessary, employee and candidate notices to be GDPR compliant <input type="checkbox"/> If you currently conduct criminal records checks, review national laws to ensure you can continue to do so	(C) (C)	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 authorised by member state law.	10, 12-14
Notices - Customers  <input type="checkbox"/> Review and update, where necessary, customer privacy notices to be GDPR compliant <input type="checkbox"/> Consider whether your notices have to accommodate “child-friendly requirements” (see <i>Children</i>)	(C) (C)	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, e.g., the legal basis for the processing of personal data Notices must also be compliant with the new Consent requirements where relying on consent as your lawful ground of processing.	12-14
Children  <input type="checkbox"/> Identify whether you process personal data of children <input type="checkbox"/> Seek local counsel advice regarding applicable local law restrictions, codes and guidance	(C) (C)	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

Action(s) / Deliverable(s)	Obligation as a Controller (C), Processor (P) or both (CP)	Description of GDPR Requirement	Applicable GDPR Article(s)
<input type="checkbox"/> If data relating to a child will be processed, ensure that age-verification systems are in place, notices directed at that child are “child-friendly” and, if consent is relied upon, you have implemented a mechanism to seek parental consent	(C)		
<input type="checkbox"/> Consider alternative protections, e.g. age-gating	(C)		
Data Subject Rights and Procedures  <input type="checkbox"/> Identify which data subject rights are relevant given the legal basis on which you process each category of data (please see Data Subject Rights Table)	(C)	<p>Data subjects are given more extensive rights under the GDPR.</p> <p>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”). Organisations should consider how they would execute a request to delete all of the requestor’s personal data.</p> <p>A right to data portability is also new (a right not just to access your data but have it provided in a machine readable and commonly used format free of charge).</p> <p>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 decisions based on automated processing are also included and expressly refer to a right to object to profiling. These must be clearly communicated in the notices given to data subjects, e.g. privacy policy.</p>	16, 17, 18, 19, 20, 21, 22, 23
<input type="checkbox"/> Update data privacy policy and internal processes for dealing with requests	(CP - through the contract with C)		
<input type="checkbox"/> Ensure technical and operational processes are in place to ensure data subjects’ rights can be met, e.g. right to be forgotten, data portability, the right to object, and subject access requests (see Governance and Accountability)	(CP - through the contract with C)		
Privacy by Design and Default  <input type="checkbox"/> Ensure processes are in place to embed privacy by design into projects (e.g. technical and organisational measures are in place to ensure data minimisation, purpose limitation and security)	(C)	In keeping with the GDPR’s objective to bring privacy considerations to the forefront of organisation organisational decision making, the GDPR requires data protection requirements to be considered when new technologies are	25, 35, 36

	Action(s) / Deliverable(s)	Obligation as a Controller (C), Processor (P) or both (CP)	Description of GDPR Requirement	Applicable GDPR Article(s)
	<input type="checkbox"/> Put in place a privacy impact assessment protocol	(C)	<p>designed or on-boarded or new projects using data are being considered.</p> <p>Privacy impact assessments should be used to ensure compliance in any event, but these will be mandatory for projects where data processing is likely to result in a high risk to individuals, e.g., 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.</p> <p>Where data processing is high risk, and the risk cannot be sufficiently addressed, the regulator must be consulted as to whether the processing is in compliance with the GDPR.</p>	
Compliant Contracting and Procurement 	<input type="checkbox"/> Develop compliant contract wording for customer agreements and third party vendor agreements, e.g., as detailed in Article 28 <input type="checkbox"/> Identify all contracts that require relevant contract wording, prioritise and develop process for amending <input type="checkbox"/> Ensure procurement process has controls to ensure privacy by design (e.g., security diligence, data minimisation, visibility of onwards data flows)	(C and P – as P will need to enter into a compliant contract with C) (C and P – as P will need to enter into a compliant contract with C) (C)	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.	28
Data Breach Procedures 	<input type="checkbox"/> Ensure appropriate security has been implemented, including backups, encryption, and regular testing to ensure technical security	(CP)	The GDPR introduces a new data breach notification regime. The process requires organisations to act quickly, mitigate losses and, where mandatory notification	32-34

Action(s) / Deliverable(s)	Obligation as a Controller (C), Processor (P) or both (CP)	Description of GDPR Requirement	Applicable GDPR Article(s)
<input type="checkbox"/> Review and update (or develop where not in existence) Data Breach Response Plan	(CP)	thresholds are met, notify regulators (within 72 hours) and affected data subjects (if merited, without undue delay).	
<input type="checkbox"/> 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	(CP)		
<input type="checkbox"/> Review liability provisions in agreements for breaches caused by services provider and other partners	(CP)		
Data Export <input type="checkbox"/> Identify all cross-border data flows and review data export mechanisms <input type="checkbox"/> Update cross border mechanisms if necessary	(CP) (CP)	The GDPR only permits exports 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
Processors <input type="checkbox"/> Consider liability as a processor, and how to mitigate risk <input type="checkbox"/> Implement policies for appointment of sub-processors (these will be similar to those for processors) <input type="checkbox"/> Draft language to ensure sub-processing contracts are GDPR compliant and develop process for updating <input type="checkbox"/> Put in place a process for amending customer agreements to include language to reflect allocation of risk based on a change in processors liability under the GDPR	(P) (P) (P) (P)	The GDPR changes the liability regime for data processors, making them directly liable for compliance. It also increases the controls on appointing a data processor.	3, 28, 82

Latham & Watkins' Global Information Law, Data Privacy & Cybersecurity Practice

USA



Jennifer Archie
Partner, Washington, D.C.



Serrin Turner
Partner, New York



Ulrich Wuermeling
Counsel, Frankfurt, London



Gail Crawford
Partner, London



Danielle Van der Merwe
Senior Associate, London



Michael Rubin
Partner, San Francisco



Scott Jones
Associate, Washington, D.C.



Joachim Grittmann
Counsel, Frankfurt



Lore Leitner
Senior Associate, London



Fiona Maclean
Senior Associate, London



Heather Deixler
Associate, San Francisco



Marissa Boynton
Associate, Washington, D.C.



Michael J. Esser
Partner, Dusseldorf, Brussels



Esther Franks
Associate, London



Calum Docherty
Associate, London



Susan Ambler Ebersole
Associate, Washington, D.C.



Alex Stout
Associate, Washington, D.C.



Rita Motta
Counsel, Brussels



Ksenia Koroleva
Associate, Moscow



Brian Meenagh
Partner, Dubai

FRANCE



Myria Saarinen
Partner, Paris



Sandy Hendry
Associate, Singapore

CHINA & HONG KONG



Hui Xu
Partner, Shanghai



Lex Kuo
Counsel, Greater China



Kieran Donovan
Associate, Hong Kong

JAPAN



Hiroki Kobayashi
Partner, Tokyo



Nozomi Oda
Partner, Tokyo

GERMANY

UK

BELGIUM

RUSSIA

MIDDLE EAST

SINGAPORE

Languages spoken worldwide: English, Mandarin, Taiwanese, Arabic, French, German, Portuguese, Russian, Italian, Spanish, and Dutch

