Wilsons
Solicitors

GDPR Compliance Checklist

GDPR Compliance Checklist

1 Accountability and Governance

1.1 Awareness

Ensure decision-makers and key people are aware of the GDPR and its accountability requirement.

1.2 Accountability

Implement, review and update technical and organisational measures to ensure and demonstrate that you are GDPR-compliant (including staff, IT security, policies, procedures, monitoring, review, training and record-keeping).

1.3 Information you hold

Conduct a data audit to establish and record what personal data and special categories of personal data you hold, where, when it was obtained, its source, who it is shared with, the purposes for which it is (and will be) processed and applicable security measures.

1.4 Data Protection Officer

Check if you need a DPO; even if you don't, ensure someone has data protection responsibility.

2 Key issues regarding data subjects

2.1 Lawful basis for processing

Establish and record the lawful bases for processing your data on which you intend to rely.

2.2 Consent

Review how you seek, record and manage consents and ensure you meet the GDPR requirements for any new consents. If necessary, refresh your existing consents or find another lawful basis for processing.

2.3 Children

If providing digital services directly to children, put in place systems for verifying children's consent or obtaining parental consent and ensure communication is especially clear.

2.4 Privacy notices

Update your privacy notices to ensure GDPR compliance (transparency and specific requirements including lawful basis for processing and rights notification). Note that different requirements apply when the data has been obtained from a source other than the data subject.

3 Individuals' Rights

3.1 Right to rectify, erase, restrict and object to processing of, and move data

Update procedures, letter templates and training to allow you to comply with and respond to requests to exercise individual rights.

3.2 Subject access requests

Update procedures and training to reflect new requirements of GDPR on charging, time limits and scope of accessible information.

3.3 Automated processing

If you rely on automated processing (including profiling), which affects data subjects, either put in place procedures to comply with their right to object or ensure the right does not apply.

4 Relationships with Third Parties

4.1 Joint controllers

Determine respective responsibilities and obligations of joint controllers.

4.2 Processors

If you delegate processing (or you are a processor), you must conclude a contract containing the provisions required by the GDPR and meet its other requirements including on record-keeping.

4.3 Commercial contracts

Update data-sharing agreements and data protection clauses in existing contracts.

4.4 Insurance

Check that your insurance is adequate to protect you from increased fines and civil actions.

5 Internal operations

5.1 Demonstrate compliance

Update your policies, procedures, training and records to meet GDPR requirements.

5.2 Record-keeping

Implement the GDPR's extensive record-keeping requirements unless you are exempt.

5.3 Privacy by design and default

Consider technical and organisational measures and integrate safeguards (such as encryption and pseudonymisation) designed to implement data protection principles, and only process data that is strictly necessary for each specified purpose.

5.4 Data privacy impact assessments

If you carry out high risk processing, introduce procedures to ensure DPIAs are made.

6 Security

6.1 Security of processing

Consider the appropriate level of security required to address your risk.

6.2 Anonymisation

If you already anonymise data, check you meet the stricter GDPR requirements to stay outside the scope of the GDPR.

6.3 Data breaches

Be aware of the new requirements and time limits for controllers and processors to report data breaches to the Information Commissioner's Office and data subjects. Update your procedures for detecting, reporting and investigating data breaches and test them to ensure GDPR compliance.

7 International

7.1 Designated representative

If you are an overseas controller or processor to which the GDPR applies, designate a representative in the EU.

7.2 Lead supervisor

If you operate in more than one EU member state, establish who your lead supervisory authority is.

7.3 Overseas transfers

Ensure you have met the requirements for overseas transfers of data on the basis of adequacy, appropriate safeguards, binding corporate rules or a specific derogation.

www.wilsonsllp.com