GDPR Compliance Checklist

☐ **Am I subject to GDPR?**

The GDPR applies to you if you answer yes to any of the following questions:
1. Do you have operations in the EU?
2. Do you offer goods and services to individuals in the EU (even free goods or services)?
3. Do you monitor behavior of individuals that takes place within the EU?

☐ **Inventory Your Personal Data Processing Activities**

Assess the kinds of data you have and how it has been used. You should understand:
1. The category of data (employment, consumer, Art. 9 data, Art. 10 criminal data);
2. The specific data elements involved;
3. How the data is collected;
4. How the data is processed;
5. The purpose of the processing;
6. Who has access to the personal data internally;
7. Who the data is shared with externally;
8. How long the data is retained.

☐ **Determine Whether to Appoint a Data Protection Officer ("DPO")**

Appoint a DPO if any of the following are true:
1. Processing is carried out by a public authority or body (except for courts);
2. Your core activities consist of processing that requires regular and systematic monitoring of data subjects on a large scale; or
3. Your core activities consist of processing on a large scale of special data under Art. 9 or criminal data under Art. 10.

☐ **Determine Whether to Appoint an EU Representative**

You need to appoint an EU representative if you are subject to the GDRP under Art. 3(2) unless processing is occasional, does not include on a large scale Art. 9 or 10 data, and is unlikely to result in a risk to the rights and freedoms of people. The appointment of the EU representative must be in writing. The representative must be in a Member State where data subjects are.

☐ **Identify a Legal Justification for Each Specific Use of Personal Data**

For processing to be lawful and compliant with GDPR, processing must have one of the justifications laid out in Art. 6 (consent, contract performance, legal obligation, vital interest, legitimate interest, etc.).

☐ **Ensure Security of Processing**

Conduct a risk assessment to determine the appropriate technical and organizational measures you should implement to ensure a level of security of personal data appropriate to the risk. Examples of these measures are listed in Art. 32(1).

☐ **Determine Whether Consent is Required for Processing Activities**

If processing is being done on personal data of someone below the age of 16, you will need to get the consent from the parent.

If you are processing special data pursuant to Art. 9 or Art. 10, you will likely need consent from the data subject.

If processing is based on consent, you must follow the requirements listed in Art. 7. If you have obtained consent before the GDPR went into effect, evaluate whether that consent is valid under GDPR requirements.

☐ **Develop Disclosure Notices Regarding the Collection and Processing of Data**

If data is collected from a data subject, a controller must provide the subject with the specific information listed in Art. 13 at the time data is obtained. If the data has not been obtained from the data subject directly, the controller must provide the data subject with the specific information listed in Art. 14. Also consider whether "child-friendly" notices are necessary.

Warner Norcross + Judd

☐ **Document and Record Data Processing Activities**

A controller must maintain a record of processing activities under their responsibility that includes the requirements in Art. 30(1).

A processor must maintain a record of processing activities that includes the requirements listed in Art. 30(2).

Records do not need to be maintained if your organization has fewer than 250 people unless the processing you carry out is likely to result in a high risk to rights and freedoms of people, processing is not occasional, or processing includes Art. 9 or 10 data.

☐ **Establish Procedures for Responding to Rights of Data Subjects**

Develop procedures for responding to the following rights of data subjects:

1. Right of Access (Art. 15)
2. Right to Rectification (Art. 16)
3. Right to Be Forgotten (Art. 17)
4. Right to Restriction of Processing (Art. 18)
5. Right to Data Portability (Art. 20)
6. Right to Object (Art. 21)
7. Rights Related to Automated Processing (Art. 22)

☐ **Create a GDPR Compliant Privacy Policy**

Create a policy documenting your privacy practices. Practices must include measures designed to implement data-protection principles and measures that ensure by default that only data which is necessary for the purpose of processing is processed. Integrate primary compliance into your audit framework.

☐ **Develop Breach Notification Procedures**

Develop an incident response procedure. If a data breach is discovered, the controller must notify the supervisory authority of the breach within 72 hours of discovery. If a processor discovers a data breach, it must notify the controller of the breach without undue delay. When the breach is likely to result in a high risk to the rights and freedoms of people, the controller must notify data subjects unless an exception applies. Consider whether cybersecurity insurance coverage is adequate.

☐ **Create GDPR Compliant Data Processing Agreements**

Anytime processing is carried out by a processor, on behalf of a controller, the processing must be governed by a written agreement between a controller and processor. Agreements must include the specific requirements listed in Art. 28.

Identify vendors who process personal data and amend contracts as necessary. Processors must consider GDPR-compliant policies for appointing sub-processors.

☐ **Have a Cross-Border Mechanism in Place for Cross-Border Transfers**

If you transfer data from the EU to a non-EU country, you must have a cross-border transfer mechanism in place. Transfers can be authorized through an adequacy decision, the Privacy Shield, binding corporate rules, or standard contractual clauses. In the absence of the foregoing, cross-border transfers may only occur if any of the Art. 49(1) conditions are met.

☐ **Train Employees on Requirements for Personal Data Protection**

Train all staff involved with processing and those with access to data on the GDPR and requirements for data protection.

☐ **Implement Privacy by Design**

Put in place a process to ensure privacy is embedded in all projects involving personal data. If you hope to process data using new technologies likely to result in a high risk to rights and freedoms of people, put in place a protocol for conducting data protection impact assessments.

☐ **Conduct Prior Consultations with Supervisory Authorities**

If a data impact assessment indicates processing would result in a high risk, absent mitigation, the controller must consult with the relevant supervisory authority prior to processing.