Understanding GDPR and Data Protection

A Guide to Data Protection Laws, Including GDPR Compliance for Businesses and Individuals' Rights

360 LAWGROUP

Table of Contents

Introduction to GDPR

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect on May 25, 2018. It aims to protect the personal data of individuals within the European Union (EU) and the European Economic Area (EEA), ensuring their privacy and control over their information

This regulation also addresses the export of personal data outside the EU and EEA. The GDPR replaces the 1995 Data Protection Directive and strengthens data protection rights, introducing new requirements and higher penalties for non-compliance.

Key Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person, such as names, email addresses, identification numbers, location data, or online identifiers.
- **Data Subject:** The individual whose personal data is being processed, who has specific rights regarding their data under the GDPR.
- **Data Controller:** The entity that determines the purposes and means of processing personal data. Controllers are responsible for ensuring compliance with GDPR requirements.
- **Data Processor:** The entity that processes personal data on behalf of the controller. Processors must adhere to the controller's instructions and implement adequate security measures.

Principles of Data Protection

The GDPR outlines several key principles that organizations must adhere to when processing personal data:

- **Lawfulness, Fairness, and Transparency:** Data must be processed lawfully, fairly, and in a transparent manner. Organizations must inform individuals about how their data is being used.
- **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization:** Data should be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- **Accuracy:** Data must be accurate and, where necessary, kept up to date. Inaccurate data should be corrected or deleted.
- **Storage Limitation:** Data should be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data is processed.
- **Integrity and Confidentiality:** Data must be processed securely to prevent unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Rights of Data Subjects

Under the GDPR, data subjects have several rights regarding their personal data:

- **Right to Access:** Individuals can request access to their data to understand how it is being used and verify the lawfulness of the processing.
- **Right to Rectification:** Individuals can request corrections to inaccurate or incomplete data.
- **Right to Erasure ("Right to be Forgotten"):** Individuals can request the deletion of their data when it is no longer necessary for the purposes for which it was collected or if they withdraw their consent.
- **Right to Restrict Processing:** Individuals can request the restriction of their data processing under certain conditions, such as when they contest the accuracy of the data.
- **Right to Data Portability:** Individuals can request their data in a structured, commonly used, and machine-readable format to transfer it to another controller.
- **Right to Object:** Individuals can object to data processing based on legitimate interests or direct marketing purposes.
- **Rights Related to Automated Decision-Making:** Individuals have rights concerning automated decision-making and profiling, including the right to obtain human intervention and contest decisions.

Obligations of Data Controllers and Processors

Data controllers and processors have several obligations to ensure GDPR compliance:

- **Accountability:** Demonstrate compliance with GDPR principles by maintaining records and implementing appropriate measures.
- **Data Protection by Design and by Default:** Implement appropriate technical and organizational measures, such as data minimization and pseudonymization, to protect data privacy.
- **Record Keeping:** Maintain records of processing activities, especially if processing is not occasional, includes special categories of data, or could result in a risk to the rights and freedoms of individuals.
- **Data Protection Officer (DPO):** Appoint a DPO if required, such as when processing is carried out by a public authority, involves regular and systematic monitoring of data subjects on a large scale, or involves large-scale processing of special categories of data.
- **Third-Party Contracts:** Ensure contracts with third parties meet GDPR requirements, including the obligation to process data only according to the controller's instructions and to implement adequate security measures.

Data Protection Impact Assessments (DPIA)

A DPIA is a process to help identify and minimize data protection risks of a project. It is required when data processing is likely to result in a high risk to individuals' rights and freedoms, such as when using new technologies, processing large amounts of sensitive data, or systematically monitoring public areas. A DPIA should:

- **Describe the processing and its purposes.**
- **Assess the necessity and proportionality of the processing.**
- **Identify and evaluate risks to individuals' rights and freedoms.**
- **Identify measures to mitigate those risks.**

Data Breaches and Notification Requirements

In the event of a data breach, organizations must notify the relevant supervisory authority within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. If the breach poses a high risk to individuals' rights and freedoms, the affected individuals must also be informed without undue delay. Notifications should include:

- **The nature of the breach, including the categories and approximate number of affected individuals and data records.**
- **The contact details of the DPO or other contact point.**
- **The likely consequences of the breach.**
- **Measures taken or proposed to address the breach and mitigate its effects.**

International Data Transfers

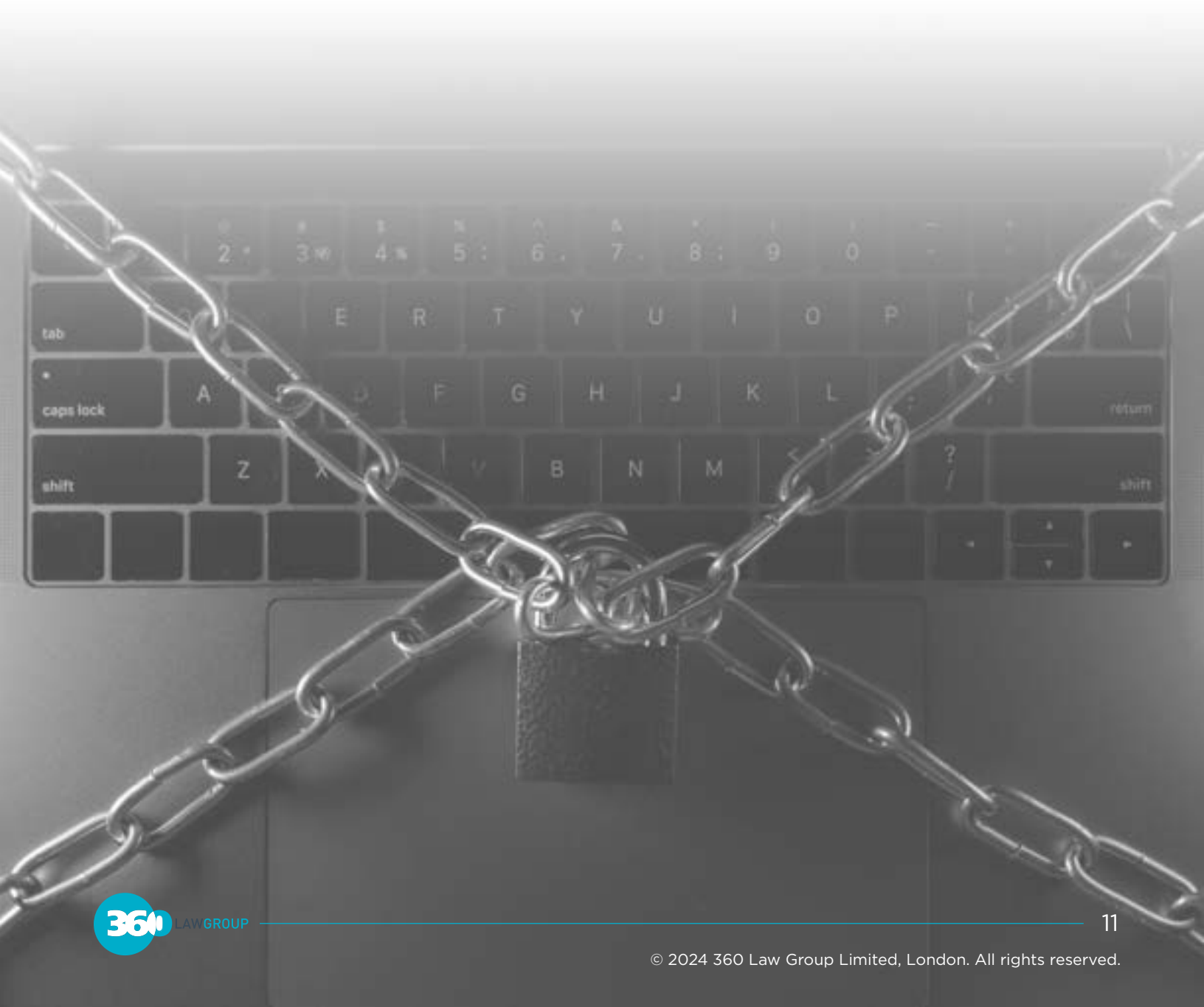
The GDPR restricts the transfer of personal data outside the EU and EEA unless specific conditions are met, such as:

- **Adequacy Decision:** The destination country ensures an adequate level of data protection as determined by the European Commission.
- **Standard Contractual Clauses (SCCs):** Contracts with clauses ensuring data protection, approved by the European Commission.
- **Binding Corporate Rules (BCRs):** Approved internal rules for data transfers within multinational companies, ensuring adequate data protection.
- **Derogations:** Specific situations where data transfers are allowed, such as with the individual's explicit consent or when necessary for important public interests.

Enforcement and Penalties

The GDPR is enforced by data protection authorities in each EU member state. Penalties for non-compliance can be significant, with fines of up to €20 million or 4% of the organization's global annual turnover, whichever is higher.

Enforcement actions can also include orders to cease processing, restrictions on data flows, and requirements to bring processing activities into compliance. Authorities may conduct investigations, audits, and inspections to ensure compliance.



Practical Steps for GDPR Compliance

- **Conduct Data Audits:** Identify and document all personal data processing activities, including the types of data processed, purposes, legal bases, data flows, and retention periods.
- **Update Privacy Policies:** Ensure policies are transparent, comprehensive, and clearly explain how personal data is collected, used, stored, and shared.
- **Implement Security Measures:** Protect data through encryption, access controls, regular security assessments, and other appropriate technical and organizational measures.
- **Train Employees:** Ensure staff understand GDPR requirements, their responsibilities, and best practices for data protection.
- **Monitor Compliance:** Regularly review and update data protection practices, conduct internal audits, and stay informed about regulatory changes and guidance.

Summary

Understanding and complying with the GDPR is crucial for businesses and individuals handling personal data. By adhering to the principles and fulfilling the obligations set forth by the regulation, organizations can protect individuals' rights and avoid substantial penalties. Continuous monitoring, regular training, and proactive measures are essential to maintain compliance and safeguard personal data in an ever-evolving digital landscape.

You can email us at
info@360lawgroup.co.uk or call us on **0333 772 7736**.