Chapter Overview of the GDPR

Chapter 1 - General provisions

Chapter 2 - Principles

Chapter 3 - Rights of the data subject

Chapter 4 - Controller and processor

Chapter 5 - Transfers of personal data to third countries or international organisations

Chapter 6 - Independent supervisory authorities

Chapter 7 - Cooperation and consistency

Chapter 8 - Remedies, liability and penalties

Chapter 9 - Provisions relating to specific processing situations

Chapter 10 - Delegated acts and implementing acts

Chapter 11 - Final provisions

Chapter 1: General Provisions

This Chapter explains the reach of the GDPR and key definitions. The GDPR generally applies when personal data of a data subject is processed. Personal data is information that can identify an individual (including some pseudonymized data if it can be linked back to an individual, but not fully anonymous data). Certain sensitive data, like biometrics, warrant heightened protection. Processing is broadly defined and includes may types of activities related to handling data, like collection, transmission, and storage. The Regulation applies to controllers, those who direct the purposes and means of how data is processed, and processors, those that actually process the data on behalf of the controller. The GDPR applies to both the public and private sectors, but data that falls under a law enforcement data regulation or is processed for national security purposes is not covered. The GDPR is extraterritorial, and does not just apply to controllers or processors based in the EU but to all companies which process European consumers' personal data.

Chapter 2: Principles

General Principles for Processing Data
Article 5 of the GDPR sets out key principles applicable to all processing of personal data. Data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Lawfulness of processing

One of six lawful bases for processing must be present before any processing can occur:

Consent of the data subject - Where data subject's consent to processing is made by clear affirmative action (opt-in) establishing a freely given, specific, informed and unambiguous indication. The GDPR significantly strengthens the requirements for consent.

Contract - Where processing is necessary for the performance of a contract with the data subject or to form a contract with the data subject.

Legal obligation - Where processing is necessary to comply with a legal obligation of the controller.

Vital interests - Where processing is necessary to protect life and limb.

Public interest - Where processing is necessary for a public authority's official responsibilities, whether carried out by a public entity or private organization.
**Legitimate interests** - Where processing is necessary for the legitimate interests of the controller or third party, except where overridden by the interests or fundamental rights and freedoms of the data subject.

Other

There are also provisions for processing of **special categories** of personal data and data related to **criminal convictions and offenses**, processing which **does not require identification**.

**Chapter 3: Rights of the Data Subject**

The GDPR also provides a series of rights to data subjects:

**The right to be informed** - When their data is collected, data subjects must be informed about the purposes for which the data will be processed, the categories of personal data obtained, how long it will be retained, and more.

**The right of access** - Data subjects have a right to information about whether their data is being processed, and, if so, have a right to access their personal data which is being processed.

**The right to rectification** - Data subjects have a right to correct their personal data or complete any data which is incomplete.

**The right to erasure** - Data subjects have a right to erasure of personal data which has been collected (i.e. a right to be forgotten) in certain circumstances, including that the data is no longer necessary for the purposes it was collected.

**The right to restrict processing** - Data subjects have a right to request that an entity limit the processing of his or her data in certain circumstances, for instance where the individual alleges the data is incorrect or is being unlawfully processed.

**The right to data portability** - Data subjects have a right to obtain their data from a service and transmit it to another service for use.

**The right to object** - Data subjects have a right to object to processing based on "legitimate interest", to direct marketing, and to processing for research purposes.

**Rights related to automated decision making and profiling** - Data subjects have special rights when they are profiled, i.e. automated processing of personal data where certain aspects of the person are evaluated, and heightened rights where a fully automated decision is made about him or her that has legal or similarly significant effects. The data subjects have a right not to be subject to fully automated individual decisionmaking where it has legal or similarly significant effects. If they are subject to such decision making, data subjects have a right to know they are subject such decision making, and to the logic of the processing and the significance/consequences of the decision.

**Chapter 4: Controller and Processor**
The GDPR imposes specific responsibilities on controllers and processors. Among the most important are:

**Data protection by design and by default** - Technical and organizational measures must be implemented to advance data protection principles.

**EU representative** - Entities outside the EU but subject to the GDPR must have a representative in the EU.

**Recordkeeping** - Records of processing activities must be kept.

**Security of processing** - Technical and organizational measures must be implemented to ensure security, like pseudonymization and encryption.

**Notification of data breach** - Within 72 hours of becoming aware of a data breach that poses a risk to individual rights and freedoms, a supervisory authority must be notified. Data subjects must be notified without undue delay.

**Data protection impact assessments (DPIAs)** - An assessment of the risks to data protection is required processing runs a high risk for individual rights, and must consult a supervisory authority before processing where the DPIA indicates a high risk is no protective measures are taken.

**Data protection officers** - DPOs must be appointed to oversee and advise on compliance issues if the entity is a public authorities, or an entity with core activities involving large scale, regular and systematic monitoring of individuals or large scale processing of special categories of data or data concerning criminal convictions and offenses.

**Chapter 5: Transfers of personal data to third countries or international organisations**

The **transfer of personal data outside the EU is limited** unless data protection guarantees under the GDPR will be maintained - for instance, transfers are permitted where there is a European Commission decision that the transfer country provides an adequate level of protection, or adequate safeguards are put in place with entity receiving the data by utilizing a "standard contractual clause" to govern the transfer data.

**Chapter 6: Independent supervisory authorities**

Each member state must provide for one or more **independent supervisory authorities**, with the aim of consistent application of the GDPR throughout the EU. The authorities will monitor and enforce application of the GDPR, propose public, controller, and processor awareness of the GDPR’s requirements, conduct investigations, provide advice, issue corrective orders and fines, and more.

**Chapter 7: Cooperation and consistency**
This Chapter provides a **system of coordination** between independent supervisory authorities so to establish a common approach to enforcement if the GDPR. Authorities must also assist one another in implementing the GDPR, for instance by providing information on investigations, and they carry out undertake joint operations. The text also requires establishment of a "consistency mechanism" to support coordination between authorities. Authorities can take emergency measures to protect data subject rights for a period of up to three months.

The GDPR also establishes a **European Data Protection Board**, an official body of the EU. The Board will be composed of a chair and two deputies elected from among its members, one supervisory authority of each Member State, and the European Data Protection Supervisor. It will absorb the influential Article 29 Working Party, an advisory group of DPAS. It will resolve disputes among authorities and issue guidelines, recommendations and best practices.

**Chapter 8: Remedies, liability and penalties**

Individuals have the right to lodge **complaints** with a supervisory authority and a **right to challenge in court** an authority's legally binding decision concerning them.

**Chapter 9: Provisions relating to specific processing situations**

Chapter 9 sets out special standards for **specific processing situations**. Among these are the requirement for states "reconcile the right to the protection of personal data... with the right to freedom of expression and information"; allows the personal data in official documents involving performance of a public task to be disclosed to advance transparency and access to information; permits member states to set conditions for processing national identification information; gives member states the right to set more specific rules in the employment context;

**Chapter 10: Delegated acts and implementing acts**

The European Commission is authorized to adopt delegated acts further **developing and implementing the GDPR provisions**, which the European Parliament and Council will have an opportunity to object to.

**Chapter 11: Final Provisions**

Chapter 11 concludes certain practical aspects of implementation, including **repealing the previous data protection directive** and setting **May 25, 2018** as the date of GDPR's applicability.