GDPR Principles

**Art. 1**

**Subject-matter and objectives**

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

**Art. 2**

**Material scope**

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

**Art. 3**

**Territorial scope**

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

**Art. 4**

**Definitions**

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

**Art. 5**

**Principles relating to processing of personal data**

**GDPR 7 Principles:**

‘lawfulness, fairness and transparency’

The first principle is possibly the most important and emphasizes total transparency for all EU data subjects. When data is collected, organizations must be clear about why it’s being collected and how it’s going to be used. If a data subject requests further information regarding the processing of their data, then organizations are duty bound to provide this in a timely manner. The collection, processing and disclosure of data must all be done in accordance with the law.

‘purpose limitation’

Organizations must have a specific and legitimate reason for collecting and processing personal information. The data can only be used for the designated purpose and must not be processed for any other use, unless the data subject has provided their explicit consent. There is a bit more flexibility with processing that’s conducted for archiving purposes in the public interest or for scientific, historical or statistical purposes.

‘data minimization’

Under the GDPR, data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.” This means that organizations should only store the minimum amount of data required for their purpose. Organizations can’t just collect personal data on the off chance that it might be useful in the future. If they are holding more data than is necessary, it’s likely to be unlawful.

‘accuracy'

Personal data must be accurate, fit for purpose and up to date. This means that organizations should regularly review information held about individuals and delete or amend inaccurate information accordingly. Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days. This streamlining of information will help improve compliance and ensure business databases are accurate and up to date.

‘storage limitation’

Once you no longer need personal data for the purpose for which it was collected, it should be deleted or destroyed unless there are other grounds for retaining it. The GDPR does not state how long you should keep personal data. It’s up to your organization to determine this, based on the purposes for processing. To ensure compliance, organizations should have a review process in place to deal with the cleansing of databases. Although the general rule is that you can’t hold on to personal data for future usage, there are exceptions for archiving, research or statistical purposes.

‘integrity and confidentiality'

This principle deals exclusively with security. Your organization must ensure that all the appropriate measures are in place to secure the personal data you hold. This could be protection from internal threats such as unauthorized use, accidental loss or damage, as well as external threats such as phishing, malware or theft. Poor information security could jeopardize your systems and services as well as causing distress to individuals. There’s no ‘one size fits all’ approach, but the GDPR states that organizations should have the appropriate levels of security in place to address the risks presented by their processing.

‘accountability'

The controller shall be responsible for, and be able to demonstrate compliance

The final principle, and a new principle under the GDPR, states that organizations must take responsibility for the data they hold and demonstrate compliance with the other principles. This means that organizations must be able to evidence the steps they have taken to demonstrate compliance. This could include:

Evaluating current practices

Appointing a Data Protection officer

Creating a personal data inventory

Obtaining appropriate consent

Carrying out Data Protection Impact Assessments

**Art. 6**

**Lawfulness of processing**

Processing shall be lawful only if and to the extent that at least one of the following applies:

The data subject has given consent to the processing of his or her personal data for one or more specific purposes;

processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

processing is necessary for compliance with a legal obligation to which the controller is subject;

**Art. 7**

**Conditions for consent**

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

The data subject shall have the right to withdraw his or her consent at any time

**Art. 8**

**Conditions applicable to child’s consent in relation to information society services**

Where offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. 2Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

**Art. 9**

**Processing of special categories of personal data**

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

**Art. 10**

**Processing of personal data relating to criminal convictions and offences**

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority

**Art. 11**

**Processing which does not require identification**

If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject

**Art. 12**

**Transparent information, communication and modalities for the exercise of the rights of the data subject**

The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

**Art. 13**

**Information to be provided where personal data are collected from the data subject**

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

the identity and the contact details of the controller and, where applicable, of the controller’s representative;

the contact details of the data protection officer, where applicable;

the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose

**Art. 14**

**Information to be provided where personal data have not been obtained from the data subject**

Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

the identity and the contact details of the controller and, where applicable, of the controller’s representative;

the contact details of the data protection officer, where applicable;

the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

**Art. 15**

**Right of access by the data subject**

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

the purposes of the processing;

the categories of personal data concerned;

the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

the right to lodge a complaint with a supervisory authority;

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

**Art. 16**

**Right to rectification**

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

**Art. 17**

**Right to erasure (‘right to be forgotten’)**

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

**Art. 18**

**Right to restriction of processing**

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;

**Art. 19**

**Notification obligation regarding rectification or erasure of personal data or restriction of processing**

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

The controller shall inform the data subject about those recipients if the data subject requests it.

**Art. 20**

**Right to data portability**

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided,

In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

**Art. 21**

**Right to object**

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

**Art. 22**

**Automated individual decision-making, including profiling**

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

**Art. 23**

**Restrictions**

Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

national security;

defense;

public security;

the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

the protection of judicial independence and judicial proceedings;

**Art. 24**

**Responsibility of the controller**

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

Those measures shall be reviewed and updated where necessary.

**Art. 25**

**Data protection by design and by default**

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.

**Art. 26**

**Joint controllers**

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

The arrangement may designate a contact point for data subjects.

**Art. 27**

Representatives of controllers or processors not established in the Union

The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored, are.

The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

**Art. 28**

**Processor**

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

The processor shall not engage another processor without prior specific or general written authorization of the controller.

In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

That contract or other legal act shall stipulate, in particular, that the processor:

**Art. 29**

**Processing under the authority of the controller or processor**

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

**Art. 30**

**Records of processing activities**

Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility.

That record shall contain all of the following information:

the name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the data protection officer;

the purposes of the processing;

a description of the categories of data subjects and of the categories of personal data;

the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;

Each processor and, where applicable, the processor’s representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller’s or the processor’s representative, and the data protection officer;

the categories of processing carried out on behalf of each controller;

where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

**Art. 31**

**Cooperation with the supervisory authority**

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

**Art. 32**

**Security of processing**

The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

the pseudonymization and encryption of personal data;

the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

**Art. 33**

**Notification of a personal data breach to the supervisory authority**

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority

**Art. 34**

**Communication of a personal data breach to the data subject**

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach

**Art. 35**

**Data protection impact assessment**

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. 2A single assessment may address a set of similar processing operations that present similar high risks.

The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

**Art. 36**

**Prior consultation**

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

**Art. 37**

**Designation of the data protection officer**

The controller and the processor shall designate a data protection officer in any case where:

the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

**Art. 38**

**Position of the data protection officer**

The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge

**Art. 39**

**Tasks of the data protection officer**

The data protection officer shall have at least the following tasks:

to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

to cooperate with the supervisory authority;

to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

**Art. 40**

**Codes of conduct**

The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

**Art. 41**

**Monitoring of approved codes of conduct**

Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

**Art. 42**

**Certification**

The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors.

The specific needs of micro, small and medium-sized enterprises shall be taken into account.

The certification shall be voluntary and available via a process that is transparent

**Art. 43**

**Certification bodies**

Certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification

demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

The national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council\_ in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant

The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

**Art. 44**

**General principle for transfers**

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization.

All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

**Art. 45**

**Transfers on the basis of an adequacy decision**

A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.

**Art. 46**

**Transfers subject to appropriate safeguards**

In the absence of a decision pursuant to Article 45, a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

**Art. 47**

**Binding corporate rules**

The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism

The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article.

Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93

**Art. 48**

**Transfers or disclosures not authorized by Union law**

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

**Art. 49**

**Derogations for specific situations**

The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognized in Union law or in the law of the Member State to which the controller is subject.

In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organization. Member States shall notify such provisions to the Commission.

**Art. 50**

**International cooperation for the protection of personal data**

In relation to third countries and international organizations, the Commission and supervisory authorities shall take appropriate steps to:

develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

**Art. 51**

**Supervisory authority**

Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).

**Art. 52**

**Independence**

Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

**Art. 53**

**General conditions for the members of the supervisory authority**

Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

their parliament;

their government;

their head of State; or

an independent body entrusted with the appointment under Member State law.

Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

**Art. 54**

**Rules on the establishment of the supervisory authority**

the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure

The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers.

During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

**Art. 55**

**Competence**

Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

**Art. 56**

**Competence of the lead supervisory authority**

Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

**Art. 57**

**Tasks**

Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

monitor and enforce the application of this Regulation;

promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons’ rights and freedoms with regard to processing;

promote the awareness of controllers and processors of their obligations under this Regulation;

**Art. 58**

**Powers**

Each supervisory authority should have investigative powers

Each supervisory authority should have corrective powers

Each supervisory authority should have authorization and advisory powers

**Art. 59**

**Activity reports**

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2)

Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law.

They shall be made available to the public, to the Commission and to the Board.

**Art. 60**

**Cooperation between the lead supervisory authority and the other supervisory authorities concerned**

The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavor to reach consensus.

The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other

**Art. 61**

**Mutual assistance**

Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another.

Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorizations and consultations, inspections and investigations.

**Art. 62**

**Joint operations of supervisory authorities**

The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations

**Art. 63**

**Consistency mechanism**

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

**Art. 64**

**Opinion of the Board**

Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion.

**Art. 65**

**Dispute resolution by the Board**

A supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment.

**Art. 66**

**Urgency procedure**

In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months.

The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

**Art. 67**

**Exchange of information**

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardized format referred to in Article 64.

**Art. 68**

**European Data Protection Board**

The European Data Protection Board (the ‘Board’) is hereby established as a body of the Union and shall have legal personality.

The Board shall be represented by its Chair.

The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

**Art. 69**

**Independence**

The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

Without prejudice to requests by the Commission referred to in Article 70(1) and (2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

**Art. 70**

**Tasks of the Board**

The Board shall ensure the consistent application of this Regulation.

To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission

Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

**Art. 71**

**Reports**

The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organizations.

The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

**Art. 72**

**Procedure**

The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organize its own operational arrangements

**Art. 73**

**Chair**

The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

The term of office of the Chair and of the deputy chairs shall be five years and be renewable once

**Art. 74**

**Tasks of the Chair**

The Chair shall have the following tasks:

to convene the meetings of the Board and prepare its agenda;

to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

to ensure the timely performance of the tasks of the Board, in relation to the consistency mechanism referred to in Article 63.

The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

**Art. 75**

**Secretariat**

The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

The secretariat shall be responsible for:

the day-to-day business of the Board;

communication between the members of the Board, its Chair and the Commission;

communication with other institutions and the public;

**Art. 76**

**Confidentiality**

The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation of the European Parliament and of the Council

**Art. 77**

**Right to lodge a complaint with a supervisory authority**

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy

**Art. 78**

**Right to an effective judicial remedy against a supervisory authority**

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

**Art. 79**

**Right to an effective judicial remedy against a controller or processor**

Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment.

Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

**Art. 80**

**Representation of data subjects**

The data subject shall have the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects’ rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

**Art. 81**

**Suspension of proceedings**

Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

**Art. 82**

**Right to compensation and liability**

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.

A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

**Art. 83**

**General conditions for imposing administrative fines**

The GDPR states explicitly that some violations are more severe than others.

The less severe infringements could result in a fine of up to €10 million, or 2% of the firm’s worldwide annual revenue from the preceding financial year, whichever amount is higher.

The more serious infringements go against the very principles of the right to privacy and the right to be forgotten that are at the heart of the GDPR. These types of infringements could result in a fine of up to €20 million, or 4% of the firm’s worldwide annual revenue from the preceding financial year, whichever amount is higher.

**Art. 84**

**Penalties**

Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented.

Such penalties shall be effective, proportionate and dissuasive.

**Art. 85**

**Processing and freedom of expression and information**

Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

**Art. 86**

**Processing and public access to official documents**

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

**Art. 87**

**Processing of the national identification number**

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application.

In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

**Art. 88**

**Processing in the context of employment**

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer’s or customer’s property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

Those rules shall include suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

**Art. 89**

**Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject.

Those safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization

**Art. 90**

**Obligations of secrecy**

Shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy

**Art. 91**

**Existing data protection rules of churches and religious associations**

Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

**Art. 92**

**Exercise of the delegation**

The power to adopt delegated acts is conferred on the Commission

The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

**Art. 93**

**Committee procedure**

The Commission shall be assisted by a committee. 2That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

**Art. 94**

**Repeal of Directive 95/46/EC**

Directive 95/46/EC is repealed with effect from 25 May 2018.

**Art. 95**

**Relationship with Directive 2002/58/EC**

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks

**Art. 96**

**Relationship with previously concluded Agreements**

International agreements involving the transfer of personal data to third countries or international organizations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

**Art. 97**

**Commission reports**

By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

**Art. 98**

**Review of other Union legal acts on data protection**

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing.

**Art. 99:**

**Entry into force and application**

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 25 May 2018.