information commissioner
Barrantagh Fysseree

Principles

The General Data Protection Regulation

Overview

SIGNIFICANT DIFFERENCES

Chapter II, Articles 5 to 11, of the GDPR sets out the provisions relating to the principles.

The principles are defined in Article 5 and do not include Rights of the Data Subject or International Transfers as these have their own specific Chapters in the GDPR.

The first principle now includes a new transparency provision which sets out what, and when, information is to be provided to a data subject. Transparency also forms part of the Rights of the Data Subject.

The third principle is amended to require data minimisation; that is, rather than the data processed being 'not excessive' for a particular purpose, that data must now be limited to what is necessary for the purpose.

The concept of Accountability has been introduced and places the onus upon a controller to demonstrate compliance with the GDPR.

The lawfulness of processing is defined in Article 6. Public authorities can no longer rely on legitimate interests to process personal data.

Where processing relies upon consent, Article 7 places the onus upon the controller to demonstrate that consent was obtained. Article 8 sets out additional requirements when consent is sought from a child in relation to information society services.

'Sensitive personal data' is not included in the GDPR. Instead Article 9 expressly prohibits the processing of certain 'special categories' of personal data, unless one of the provisions set out in Article 9 applies.

The special categories of data do not include criminal convictions or offences. Article 10 states that such data can only be processed by official authority or as authorised by law.

For certain limited purposes, the GDPR replaces exemptions from the principles with restrictions from the obligations and rights set out in Article 5, and Articles 12 to 22 (Rights of the data subject). The restrictions are set out in Article 23 and are broadly similar to existing exemptions.

THE PRINCIPLES

The principles relating to the processing of personal data are set out in Article 5 of the GDPR and can be summarised as:-

Personal data shall be

1. *Processed lawfully, fairly and in a transparent manner in relation to the data subject.*

   Lawfulness, fairness and transparency

2. *Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*

   Purpose Limitation

3. *Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

   Data minimisation

4. *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.*

   Accuracy

5. *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.*

   Storage limitation

6. *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.*

   Integrity and confidentiality

7. *The controller shall be responsible for, and be able to demonstrate* compliance with principles 1 to 6.

   Accountability

1. Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

LAWFULNESS

There remains a general requirement for personal data to be processed lawfully. In considering whether processing is generally lawful a controller may have to consider other things such as compliance with the European Convention on Human Rights.

With regard to the lawfulness of processing **Article 6**, states:

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;
- **processing is necessary**** in order to protect the vital interests of the data subject or of another natural person;
- **processing is necessary**** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- **processing is necessary**** for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (**NOT** applicable to processing carried out by a public authority)

** Consent is considered in a separate note.*

*** What is meant by the term "processing is necessary" has been considered by the Court of Justice of the European Union in Huber v Germany. It is generally taken to mean that the processing is "**proportionate to the legitimate aim being pursued"** for example in Stone v SE Coast Strategic Health Authority [2006] EWHC 1668 (Admin),*

The GDPR replaces 'sensitive personal data' with:-.

A. Processing of special categories of personal data.

The **special categories of personal data** are defined in **Article 9(1**) as personal data revealing a natural persons':-

- health,
- sex life, or sexual orientation
- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,

  or

- the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person.

Processing of any of the special categories of personal data is prohibited unless a controller can demonstrate that at least one of the conditions set out in **Article 9(2**) applies. (See Annex A.)

B. Processing of personal data relating to criminal convictions and offences

Personal data relating to criminal convictions and offences or related security measures are not included in the special categories.

However, **Article 10 restricts the processing of personal data relating to criminal convictions and offences** and requires that the processing of personal data relating to criminal convictions and offences or related security measures **shall be carried out only** under the control of official authority or **when the processing is authorised by … law** providing for appropriate safeguards for the rights and free-doms of data subjects.

Any register of criminal convictions shall be kept only under the control of official authority.

FAIRNESS & TRANSPARENCY

There remains a general requirement for personal data to be processed **fairly.**

Transparency is a new concept and Articles 12 to 14 set out what is meant by transparency. In summary, transparency requires a controller using clear and plain language to provide a data subject with concise, easily accessible and easy to understand information about the processing of their personal data. The information a controller must provide includes:

A. The identity and contact details of: the controller and, where applicable, the controller's representative, and data protection officer.

B. the purposes of the processing;

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

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

E. where applicable, the identification of any third country or international organisation to which transfers are made and, where such transfers are necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request, the documentation of suitable safeguards;

F. where possible, the envisaged time limits for erasure of the different categories of data;

G. the rights of the data subject and how to exercise them including the right to lodge a complaint with the supervisory body,

H. where possible, a general description of the technical and organisational security measures in place to safeguard personal data;

I. where a controller intends to process personal data for a previously unspecified purpose, the controller must prior to that further processing provide additional transparent information to the data subject,

J. if a there is a joint controller arrangement for the processing of personal data then Article 26 further requires the essence of that arrangement to be made available to the data subject.

Transparency is considered in detail in a separate note.

2. Purpose Limitation

Personal data shall be 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.

Any further processing of personal data must be compatible with the specified explicit and legitimate purpose for which the data were collected.

In general, a controller processes personal data for the specific purpose for which it had been collected. Where the purpose for further processing of personal data differs from the purpose for which the personal data were originally collected it must be **compatible** with the original purpose for collection.

To ascertain whether the processing is compatible, the controller must take into account:

- any **link** between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- the **context** in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- the **nature** of the personal data, in particular whether special categories of personal data or criminal convictions or offences are processed;
- the possible **consequences** of the intended further processing for data subjects; and
- the existence of **appropriate safeguards** (e.g. encryption, pseudonymisation etc.).

A concession from the obligation to ensure processing is compatible with the initial purpose is provided where personal data **is being further processed** for public records, scientific or historical research or statistical purposes.

3. Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

The general concept that a controller should obtain or collect just enough information necessary to fulfil a particular purpose remains. However, the GDPR replaces the previous obligation that processing was **'not excessive'** with an obligation to ensure that the processing is **'limited to what is necessary**' for the purpose.

Recital 39 states:-

"... Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means..."

Collecting personal data "just in case it is needed" or "might be useful later" will not comply with the data minimisation principle.

Where processing is **necessary** for a legal obligation imposed on a controller (for example customer due diligence, employment, taxation, vetting checks) the personal data to be processed for that purpose may be specified in that law. However such obligations cannot be used to collect additional personal data that was not required by that law.

4. Accuracy

Personal data shall be 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

The Accuracy principle has been extended to include an obligation upon a controller to take every reasonable step to ensure that any inaccurate personal data are erased or rectified without delay. A controller will be expected to have appropriate procedures in place to do so.

With regard to the accuracy of profiling and similar processing, Recital 71 states:-

"...a controller should ... implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised..."

5. Storage limitation

Personal data shall be 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 this Regulation in order to safeguard the rights and freedoms of the data subject

The principle that personal data should not be processed for longer than is necessary for the specified purpose(s) remains. Rectal 39 states:-

"…the period for which personal data are stored is limited to a strict minimum… In order to ensure that the personal data are not kept for longer than necessary, time limits should be established by the controller for erasure of periodic review.."

A retention policy establishing time limits for erasure or periodic review is therefore required. In any event, transparency requires that these time limits are provided to the data subject.

To demonstrate that a controller is following its retention policy, a controller should, in a addition to its retention policy, retain disposal or destruction records indicating when and how personal data was disposed of or anonymised.

The period of time that personal data can be stored may be set out in law or through accepted industry practice.

The GDPR provides concessions from the storage limitation principle when:-

- it is no longer possible to identify a data subject, either directly or indirectly, from that data,

  or

- data is archived as a public record, or used for scientific or historical research, or for statistical purposes,

provided the rights and freedoms of individuals are protected, in particular by having appropriate technical and organisational measures in place.

The concession only applies once that data has been anonymised, become a public record, or has been used in research.

6. Integrity and confidentiality

Personal data shall be 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.

Article 32, Security of processing, expands upon the Integrity and Confidentiality principle and promotes a risk based approach.

With regard to the assessment of risk Recital 76 states:-

> *"The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."*

In determining what measures are appropriate to take, it is **the risk to the individual and NOT the controller or processor that must be considered.** A controller and a processor must take into account the likelihood and severity of risk to the rights and freedoms of the data subject. Recital 75 describes these risks as:-

- *physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;*
- *where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;*
- *where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;*
- *where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;*
- *where personal data of vulnerable natural persons, in particular of children, are processed;*

  or

- *where processing involves a large amount of personal data and affects a large number of data subjects.*

Article 32 also requires that, in assessing the appropriate level of security, a controller or processor must not only take into account the risk to the individual posed by the intended processing but also the risk posed by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

A controller and processor must also have:-

- *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;*

  and

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

Controllers and processors must also take steps to ensure that any person who has access to personal data does not process that data except on instructions from the controller.

Adherence to approved codes of practice and certification mechanisms are encouraged as are the use of encryption and pseudonymisation techniques, that is processing personal data in a manner that does not permit direct identification of a data subject.

7. Accountability

The controller shall be responsible for, and be able to demonstrate compliance with the principles.

Accountability requires a controller to implement comprehensive, but proportionate, information governance measures. While Article 5 requires a controller to be able to demonstrate how it complies with the principles, Accountability extends to compliance with all of the GDPR.
Recital 82 states:

> *"In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations."*

Further provisions which require a controller or processor to be able to demonstrate compliance include:

Article 24: Responsibility of Controller
Proportionate and appropriate data protection policies
Adherence to approved codes of conduct

Article 25: Data Protection by Design and default

Appropriate technical and organisational measures to ensure, by default, that only personal data which are necessary for each specific purpose of the processing are processed.

Article 26: Joint Controllers
Documented arrangements between joint controllers and make available the essence of that arrangement to the data subject

Article 28: Processor
Written authorisation of the controller to undertake specified processing
Documented instructions from the controller

Article 30: Records of Processing activities
Maintain records of processing activities*

Article 32: Security of Processing
Implement appropriate technical and organisational measure to ensure a level of security appropriate to the risk

Article 44: Transfers to third countries
Ensure personal data is safeguarded

*Article 30 provides a limited derogation from the obligation to maintain certain records of processing activities. The derogation can be applied if the controller has less than 250 employees, provided any processing is occasional, does not pose a risk to the rights and freedoms of data subjects and does not include any special categories of data, criminal convictions or offences.

However, the derogation only applies to the obligation to maintain the records of processing activities mentioned n Article 30. The derogation does not affect other obligations for example Transparency which requires that the data subject is provided with similar information to that mentioned in Article 30.

Compliance Questions

The following questions may assist when considering compliance with the principles :-

1. Lawfulness, fairness and transparency

What are the purposes for which personal data are processed?

For each purpose what is the lawful condition for processing?

What data is processed?

Where does the personal data come from?

For how long is the data required?

Are any other controllers involved in the processing and, if so, who and what are the processing arrangements?

Are any processors involved in the processing and if so what are the contractual arrangements?

How is the data subject informed of the processing?

Is this processing documented?

2. Purpose Limitation

Is the personal data processed for another unspecified purpose?

Is any personal data disclosed and if so to whom and why? Doe this include any transfers to a third county and if so what safeguards are in place?

Is all further processing compatible with the specified and lawful purposes for which it was collected?

How is the data subject informed of the processing?

Is this processing documented?

3. Data minimisation

For each purpose, can you explain why it is necessary to process each piece of data?

Is this processing documented?

4. Accuracy

How is accuracy assured when collected?

What procedures are in place to keep data up to date when necessary?

What processes are in place to quickly rectify inaccurate data?

Is this processing documented?

5. Storage limitation

Is there a retention policy and, if so, does it cover all the purposes for processing personal data?

Can it be demonstrated that the retention policy is appropriate, that is, in accordance with law and/or industry practice?

How often is the policy reviewed and by whom?

Is there evidence to demonstrate that the retention policy is followed, for example destruction or erasure records?

How is the data subject informed of the retention periods?

6. Integrity and confidentiality

Security

Have the risks to an individual from the processing of personal data been identified?

What technical and organisational measures are in place to mitigate these risks?

- Are there policies and procedures in place that cover technical measures, such as, information security and organisational measures ,such as, physical access to buildings and manual files?
- Are the measures appropriate and proportionate to the risks?
- How often are the measures reviewed?
- Who endorses these polices?

Are the measures adhered to and how is this evidenced?
How is the data subject informed of these measures?

Resilience

What backup and recovery, including disaster recovery, procedures are there?

Are they effective and efficient?

Are they regularly tested?

How is this evidenced?

Staff

How are staff made aware of their responsibilities?

- As a new recruit?
- Regular refresher training?

Does training include senior management, directors etc.?

What training is provided—internal, external, desk top?

Is the training accredited?

Are training records maintained?

Codes of Practice

Do you follow any Code of Practice or other certification methods?

7. Accountability

Articles 37 to 39—Data Protection Officer (DPO)

Have you designated a DPO?

If not, are you able to demonstrate the rationale for not having a DPO?

Article 24– Responsibility of the controller

Are appropriate Data Protection Polices implemented?

Article 30 - Records of Processing Activities

Are records maintained?

How often are they reviewed?

Article 26—Joint Controller

Are the arrangements with any joint controllers documented?

Article 28 –Processor

Are there written contracts in place with any processors?

Article 32–Security of processing

Are records of system testing maintained?

How often are the security polices and procedures reviewed?

Article 44—International transfers

Can you evidence that any international transfers are safeguarded?

Resources

UK ICO Self-assessment Toolkit

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

IOM Information Commissioner - Know Your Data - Map the 5 W's

https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/steps-towards-compliance/know-your-data-map-the-5-ws/

Privacy Impact Assessment Code of Practice

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Transparency

UK ICO Privacy Notices Codes of Practice

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Storage Limitation—Retention Policies

IOM Public Records Office—General advice for Public bodies

https://www.gov.im/about-the-government/departments/economic-development/central-registry/public-record-office/advice-for-public-bodies/

IOM Information Commissioner

https://www.inforights.im/legislation/data-protection-act/data-protection-principles/fifth-principle-time-for-keeping-data/

Integrity and Confidentiality –Information security policies

UK ICO—Security

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

IOM Information Commissioner —Top tips

https://www.inforights.im/media/1189/tgn_it-security.pdf

ANNEX A

Article 9

Processing of special categories of personal data

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where ... law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are manifestly made public by the data subject

f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest, on ... which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

J. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Personal data may be processed for the purposes referred to in point (h) when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Important

This document is part of a series, produced purely for guidance, and does not constitute legal advice or legal analysis.

All organisations that process data need to be aware that the General Data Protection Regulation may apply directly to them.

The responsibility to become familiar with the GDPR and comply with its provisions from 25th May 2018 onwards lies with the organisation.

Legal advice, if required, should be sought from a Manx advocate.


information
commissioner
Barrantagh Fysseree