Explanatory Framework for Adequacy Discussions

Section D: Adequacy Referential

Overview

This section systematically goes through the aspects highlighted by the adequacy referential adopted by the European Data Protection Board (EDPB) and demonstrates how the required concepts and principles are met by the UK framework.

The Board's adequacy referential was aimed at providing guidance to the European Commission for the assessment of the level of data protection in third countries by establishing the core data protection principles that must be present in order to ensure essential equivalence with the EU framework.

Section D: Adequacy Referential

Introduction

The European Data Protection Board's adequacy referential covers the following elements, important for an adequacy assessment, divided into four sections:

1. **The existence of basic content principles.** These refer to basic concepts or definitions: grounds for lawful and fair processing; a range of principles; transparency of processing; data subject rights of access, rectification, erasure, and the right to object to processing; and restrictions on onward transfers;

2. **The existence of additional content principles for specific processing.** These refer to specific safeguards for special categories of data ("sensitive data"); the ability to object freely to processing that is for direct marketing purposes; and provisions around automated decision making and profiling;

3. **The existence of procedural and enforcement mechanisms.** These include a competent, independent supervisory authority; a system that secures a good level of compliance, e.g. through the existence of effective dissuasive sanctions; measures for accountability of controllers and processors; and the ability for data subjects to exercise their rights through appropriate redress mechanisms;

4. **Essential guarantees on national security and law enforcement access.** The guarantees are that processing is based on clear, precise, and accessible rules; that necessity and proportionality are demonstrated; and that there is independent oversight and effective remedies for data subjects whose rights have been infringed.

All these elements are in UK law and are outlined in the four parts below.

Section D: Adequacy Referential

PART I: BASIC CONTENT PRINCIPLES

Concepts

The EDPB referential outlines important data protection concepts that need to reflect and be consistent with the concepts enshrined in European Data Protection Law.

All important data protection concepts and principles set out in the UK GDPR are **identical** to those in the EU GDPR. These are set out in Chapters I and II of the UK GDPR. These include:

- Definition of "personal data". This is set out in Article 4(1) of the UK GDPR. The wording has not changed from that in its corresponding EU GDPR article.
- Definition of "processing" of personal data. This is set out in Article 4(2) of the UK GDPR. The wording has not changed from that in the corresponding EU GDPR article.
- Definition of "controller". This is set out in Article 4(7) of the UK GDPR. The core part of the definition is still **identical:** a data controller *is the natural or legal person, public authority*[1]*, agency or other body, which, alone or jointly with others, determines the purposes and means of the processing of personal data.* The sole difference between this article and the EU GDPR counterpart is the removal of the reference to Union or Member State law determining specific criteria.

  The DPA 2018[2] clarifies who the controller is when UK law determines the purpose and means of processing. When a body has a legal obligation to process, the body is still the controller, even though it is UK law that determines the purposes or means, or both.
- Definition of "processor". This is set out in Article 4(8) of the UK GDPR. The wording has not changed from that in the corresponding EU GDPR article.
- Definition of "recipient". This is set out in Article 4(9) of the UK GDPR. The definition is **identical** to the EU GDPR counterpart, except that a reference to *"Union or Member State law"* is replaced with *"domestic law."*
- Concept of sensitive data and general prohibition of its processing. This is set out in Article 9(1) of the UK GDPR. The wording has not changed from that in the corresponding EU GDPR article. Further detail on bases for sensitive data processing are in Section E.

[1] Section 7 of the DPA 2018 sets out the meaning of "public authority" or "public body" for the purposes of the UK GDPR.
[2] Section 6 of the DPA 2018. Sections 209 and 210 also clarify who the controller is for the Royal Household, the Duchies of Lancaster and Cornwall and for each of the Houses of Parliament.

Grounds for lawful and fair processing for legitimate purposes

The UK GDPR, supplemented by the DPA 2018, sets out the principles of lawful and fair processing for legitimate purposes:

- Article 5(1)(a) of the UK GDPR is **identical** to the EU framework, setting out the principle that a data subject's personal data must be processed lawfully, fairly, and in a transparent manner;

- Article 6(1) of the UK GDPR sets out **identical grounds** for lawful and fair processing as Article 6(1) of the EU GDPR. These include, for example, the consent of the data subject; compliance with a legal obligation; performance of a contract; or processing in the legitimate interests of the controller or of a third party that does not override the fundamental rights of the data subject;

  Section 8 of the DPA 2018 specifies a non-exhaustive list of broad activities that constitute tasks carried out in the public interest or the exercise of official authority in the UK in order to provide further detail on the meaning of the lawful base in Article 6(1)(e). These include processing necessary for:
  - the administration of justice;
  - the exercise of a function of either House of Parliament;
  - the exercise of a function conferred on a person by an enactment or rule of law;
  - the exercise of a function of the Crown, a Minister of the Crown, or a government department;
  - or an activity that supports or promotes democratic engagement.

The EDPB adequacy referential does not refer to conditions for consent. However, it is worth noting that Article 7 of the UK GDPR is **identical** to Article 7 of the EU GDPR. This includes the conditions which must be met for consent to be valid, how it should be presented, and the requirement that it should be as easy to withdraw consent as to give it.

Principles

The purpose limitation principle

The purpose limitation principle is set out in Article 5(1)(b) of the UK GDPR. It is **identical** to Article 5(1)(b) of the EU GDPR. As in the EU GDPR, it also states that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the original purpose. In both

the UK and EU GDPR, such processing must be in accordance with the safeguards set out in Article 89(1). This article is also **identical** across the two pieces of legislation.[3]

While this is not explicitly mentioned in the EDPB referential, it is worth noting that the UK GDPR also replicates the EU GDPR's provisions on purpose compatibility in Article 6(4). This includes the factors for determining whether a purpose is compatible with the original purpose. The article is **identical** to its EU GDPR counterpart, except for the replacement of the reference to Member State or Union law to "domestic law". It now also includes national security and defence in Article 6(4).[4]

Article 13(4) and Article 14(4) of the UK GDPR also stipulate that data subjects must be informed of a change in purpose before the new processing begins.

The data quality and proportionality principle

Article 5(1)(d) of the UK GDPR requires that data be adequate and kept up to date. Where inaccurate, they must be erased or rectified without delay. This is **identical** to the equivalent EU GDPR Article.

Data minimisation is also a key principle in the UK GDPR. Article 5(1)(c) is **identical** to its EU GDPR counterpart, stressing that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, in other words proportionate.

Data retention principle

Another principle of the UK GDPR that is **identical** to that in the EU GDPR is the storage limitation principle, sometimes also referred to as 'data retention'. This is set out in Article 5(1)(e) of the UK GDPR and requires that data is kept in a form which permits identification for no longer than is necessary.

The security and confidentiality principle

Ensuring that data is processed in a manner that provides not only protection against unlawful processing but also against accidental loss, destruction or damage is another key principle of the UK GDPR. Article 5(1)(f) of the UK GDPR is **identical** to Article 5(1)(f) of the

[3] Article 89(1) pertains to the safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Those safeguards *"shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."* Section 19 of the DPA 2018 further specifies that the Article 89(1) requirements are **not** met if processing is likely to cause substantial damage or substantial distress to a data subject, or if it is carried out for taking decisions or measures in relation to a data subject, unless for the necessary purposes include approved medical research.

[4] This has been done since these purposes have been removed from Article 23(1) of the UK GDPR. It is therefore necessary to make specific reference to them.

EU GDPR.

The transparency principle

Transparency of personal data processing is a cornerstone of the UK's data protection framework, and the UK GDPR goes into considerable detail with regards to both the form and content of information that should be provided to data subjects.

Article 12 of the UK GDPR refers to the various articles that set out the rights of data subjects and the obligations placed on controllers that relate to the transparency principle. The article stipulates how the controller should provide data subjects with the information referred to in those articles. It is **identical** to Article 12 of the EU GDPR, except for two types of changes:

- One replaces *"supervisory authority"* with *"Commissioner"* (i.e. the ICO);

- The other bestows the delegated power for the European Commission to determine the standardised icons upon the ICO.

Article 13 is also a key part of the transparency principle. Controllers are required to provide all the main elements of the processing to the individual whose data is collected, at the time when their personal data is obtained. The elements range from basic details such as the controller's identity and contact information, to details such as whether the controller intends to transfer the data internationally and the method for obtaining a copy of the safeguards for the transfer, if not under adequacy regulations.

It is **identical** to Article 13 of the EU GDPR, except for two small changes: the reference to *"supervisory authority"* has been replaced with *"Commissioner"*, and the reference to Commission adequacy decisions has been replaced with one to regulations under Section 17A (transfers based on adequacy regulations) of the DPA 2018.

Article 14 of the UK GDPR contains the requirement for information to be provided by controllers where personal data have **not** been obtained from the data subject. Article 14 broadly replicates the information required under Article 13 but also requires information to be provided on the relevant "legitimate interests" (if this is the legal basis for the processing) and the source of the personal data, including whether it was obtained from publicly accessible sources.

It also sets out timescales for providing this, and instances when it does not need to be provided. All of Article 14 is **identical** to its EU GDPR counterpart, except for the same minor changes made to Article 13 and the replacement of *"Union or Member State law"* with references to *"domestic law"*.

Section D: Adequacy Referential

Right to Access

Article 15 of the UK GDPR gives individuals the right to obtain a confirmation that their personal data is being processed, a copy of their personal data[5], and the following information:

- the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

- the retention period for storing the data, or, if that is 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 the Information Commissioner;

- where the personal data are not collected from the data subject, any available information as to their source;

- the existence of automated decision-making;[6] and the safeguards provided if their personal data is transferred to a third country or international organisation.

This is commonly referred to as a "subject access request" and can be made either verbally or in writing. Importantly, the right to obtain a copy of the personal data should not adversely affect the rights and freedoms of others. This is set out in Article 15(4).

The article is **identical** to its EU GDPR counterpart, except for a reference to *"supervisory authority"* being replaced with a reference to the ICO.

Right to Rectification

In addition to the right of access, data subjects also have the right to obtain rectification of their data as appropriate. This is set out in Article 16 of the UK GDPR, which is **identical** to its EU counterpart. This right includes, for example, where the data held is inaccurate or incomplete. Taking into account the purposes of the processing, data subjects can request that incomplete personal data is completed and inaccurate personal data rectified.[7] The controller must undertake this without undue delay.[8]

[5] Section 13 of the DPA 2018 provides further specifications for how the right of access applies to credit reference agencies.

[6] This also includes profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

[7] This can be done by means of providing a supplementary statement.

[8] Article 12(3); Article 16.

Right of Erasure

Another key right that is enshrined in the UK GDPR is the right of erasure. Article 17 of the UK GDPR is **identical** to its EU GDPR counterpart, except for references to *"Union or Member State law"* which are replaced with *"domestic law"*. As with the EU GDPR, this right can be exercised when:

- the personal data have been unlawfully processed;
- the personal data are no longer necessary for the processing's purpose in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based, and where there is no other legal ground for processing the data;
- the data subject has exercised their right to object under Article 21, and the controller must comply with it;
- the controller is legally obliged to erase the data;
- the personal data falls under Article 8(1) of the UK GDPR, i.e. provision of information society services to a child.

If a controller has made the personal data public and is obliged to erase it, they must take reasonable steps to inform other controllers processing the data of the request by the data subject. This is set out in Article 17(2).

Article 17(3) sets out limited situations where the above obligations do not apply, such as when processing is necessary for freedom of expression. As with the above, these situations are **identical** to the EU GDPR, save for references to "Union or Member State law" which are replaced with "domestic law".

In addition, while it does not feature in the EDPB adequacy referential, the UK GDPR provides data subjects with the right to have the processing of their personal data restricted in certain circumstances. This is set out in Article 18 of the UK GDPR, which is **identical** to its EU GDPR counterpart, except for the removal of a reference to the *"of the Union or of the Member States".*

Right to Object

Data subjects also have the right to object to processing that is using the "public interest" or "legitimate interest" lawful bases provided by Article 6(1)(3) and 6(1)(f).

Controllers must cease processing, unless they can show that processing is necessary for legal claims, or that there are "compelling, legitimate grounds" to continue processing that override the data subject's interests, rights, and freedoms.

Data subjects also have the right to object to processing for scientific or historical research purposes or statistical purposes, unless it is necessary for a task in the public interest.

The right to object is set out in Article 21. It is **identical** to its EU GDPR counterpart, except for a reference to Directive 2002/58/EC ("ePrivacy"), which has been replaced with a reference to domestic law implementing this Directive.

Right to data portability

While it is not mentioned explicitly in the EDPB Referential, the right to data portability is set out in Article 20 of the UK GDPR. It is **identical** to its EU GDPR counterpart.

If requested by the data subject, controllers are obliged to provide the data subject's personal data in *"a structured, commonly used and machine-readable format"*. This allows data subjects to administer and use their personal data across different services as they see fit. When technically feasible, data subjects can also exercise this right by having their personal data transmitted directly from one controller to another.

Data subjects can exercise this right where:

- the processing is based on consent pursuant to Article 6(1)(a)[9] or of Article 9(2)(a)[10] or on a contract pursuant to Article 6(1)(b)[11];

- the processing is carried out by automated means.

Restrictions to rights and other provisions

In certain cases, the Secretary of State may restrict the scope of the obligations and rights through legislative measures.[12] This is set out in Article 23 of the UK GDPR, which is **identical** to its EU GDPR counterpart, except for reference to the Union or Member State or their laws. References to national security and defence have also been removed.[13]

[9] "the data subject has given consent to the processing of his or her personal data for one or more specific purposes" (Article 6(1)(a)).

[10] "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject" (Article 9(2)(a). This refers to processing of sensitive data.

[11] "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" (Article 6(1b)).

[12] Restrictions are set out in Section E.

[13] These amendments remove any cause for confusion around the national security and defence exemption in section 26 of the DPA 2018, which is not linked to the restrictions made under Article 23 of the UK GDPR.

Restrictions may be made to the above data subject rights, as well as to the rights in Articles 20 and 22, and the breach notification obligation in Article 34. Restrictions may also be made to the principles set out in Article 5, in so far as they correspond to the rights.

Any such restriction must respect the essence of the fundamental rights and freedoms of the data subject, and must be a necessary and proportionate measure in a democratic society to safeguard one of the following as set out in Article 23(1):

- 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;
- other important objectives of general public interest, in particular an important economic or financial interest of the United Kingdom, including monetary, budgetary and taxation matters, public health and social security;
- the protection of judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in the above points [except for the protection of judicial independence and judicial proceedings];
- the protection of the data subject or the rights and freedoms of others;
- the enforcement of civil law claims.

Restrictions are further limited by Article 23(2). This requires that restrictions include certain specific provisions where relevant.

Schedules 2, 3 and 4 to the DPA 2018 make provision for exemptions from, restrictions to and adaptations of the application of rules of the UK GDPR. These are further set out in Section E.

Restrictions on onward transfers

The UK GDPR and the DPA 2018 govern the transfer of personal data to third countries and international organisations.

Any such transfer of personal data shall take place only if the conditions laid down in Chapter V of the UK GDPR are complied with by the controller and processor.

This includes onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in Chapter V must be applied to ensure that the level of protection guaranteed by the UK GDPR is not undermined.[14] Transfers are also subject to the other provisions in the UK's data protection framework.

Adequacy regulations

Under Section 17A of the DPA 2018, the Secretary of State may, by regulations, specify that he or she considers that one of the following ensures an **adequate level of protection of personal data**:

- a third country;
- a territory or one or more sectors within a third country;
- an international organisation;
- a description of such a country, territory, sector or organisation.

Article 45(2) of the UK GDPR makes provision for the assessment of the adequacy of the level of protection for the purpose of these regulations. These closely mirror Article 45(2) of the GDPR.

Once adequacy regulations have been made, the Secretary of State must:

- carry out a review at least every 4 years. Each review must take into account all relevant developments in the third country or international organisation.

- on an ongoing basis, monitor developments in third countries and international organisations that could affect decisions to amend or revoke such regulations.

Should a country no longer provide adequate protection of personal data, the Secretary of State must, to the extent necessary, amend or revoke the regulations. Section 17B(5) requires that the Secretary of State consult with the relevant third country or international organisation with a view to remedying the deficiency.

A list and description must be published of the third countries (etc) that have received adequacy status, as well as a list of those that have been, but are no longer, specified as having an adequate protection of personal data.

[14] Article 44.

Appropriate safeguards

In the absence of an adequacy decision, a controller or processor may still transfer personal data to a third country or an international organisation if:

- there are appropriate safeguards; **and**
- enforceable data subject rights and effective legal remedies for data subjects are available.

Article 46 of the UK GDPR sets out how these appropriate safeguards may be provided. It is **identical** to its EU GDPR counterpart, except for minor changes:

- references to *"supervisory authority"* have been replaced by references to the ICO;
- the reference to Article 45 of the EU GDPR has been replaced by a reference to the DPA 2018's adequacy regulations;
- the powers to specify standard contractual clauses have been assigned to the Secretary of State and the ICO rather than the Commission;[15]
- lastly, the references to the GDPR's consistency mechanism and authorisations under Directive 95/46/EC, have been removed.

Article 46 outlines that these appropriate safeguards may be provided by:

- a legally binding and enforceable instrument between public authorities or bodies;
- **binding corporate rules** in accordance with Article 47 of the UK GDPR;
- **standard data protection clauses specified in regulations by the Secretary of State** under Section 17C(b) of the DPA 2018 and for the time being in force;
- **standard data protection clauses specified by the ICO** in a document issued (and not withdrawn) under Section 119A of the DPA 2018 and for the time being in force;
- **an approved code of conduc**t under Article 40 of the UK GDPR, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including data subjects' rights;

[15] The DPPEC Regulations removed the obligation on the Information Commissioner to seek European Commission approval for these. However, Parliament will have the opportunity to scrutinise SCCs as they are laid before both houses.

- **an approved certification mechanism** under Article 42 of the UK GDPR, with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

With authorisation from the Commissioner, the appropriate safeguards referred to above may also be provided for by[16]:

- **contractual clauses** between the controller or processor, and the controller, processor or the recipient in the third country or international organisation; or

- provisions to be inserted into **administrative arrangements between public authorities or bodies** which include enforceable and effective data subject rights.

Article 47 sets out further requirements for the above mentioned binding corporate rules. It requires that the Commissioner approve binding corporate rules, provided that they:

- are legally binding, apply to, and are enforced by every member of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

- expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

- fulfil the requirements laid out in Article 47(2).

These are **identical** to Article 47(2) of the EU GDPR, except for the removal of references to Member States and the Union. References to *"supervisory authority"* have been replaced with references to the ICO.

Other means of transfer

In the absence of adequacy regulations or one of the appropriate safeguards set out in Article 46, transfers of personal data to a third country or an international organisation shall take place only under one of the following conditions:

- the data subject has **explicitly consented** to the proposed transfer. Importantly, before consenting, the data subject must be informed of the possible risks of such transfers due to the absence of an adequacy regulation and appropriate safeguards;

[16] Article 46(3).

- it is 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;

- it is necessary for the conclusion or performance of a **contract in the interest of the data subject** between the controller, and another natural or legal person;

- it is necessary for **important reasons of public interest**;[17]

- it is necessary for the **establishment, exercise or defence of legal claims**;

- it is necessary in order to protect the **vital interests of the data subject or of other persons.** The data subject must be physically or legally incapable of giving consent;

- the transfer is made from a register, subject to certain conditions[18]

If a transfer cannot be based on a provision in Article 45 or 46, and none of the above derogations apply, the transfer may take place only if it fulfils all the below conditions:

- it is not repetitive;

- it concerns only a limited number of data subjects;

- It is necessary for the purposes of compelling legitimate interests pursued by the controller, which are not overridden by the interests or rights and freedoms of the data subject; **and**

- the controller has assessed all the circumstances for the data transfer and has on that basis provided suitable safeguards to protect the data.

If such a transfer is made, the controller must inform the ICO. They must also, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and of the compelling legitimate interests pursued.

[17] The public interest in the point must be public interest that is recognised in domestic law, whether in regulations under section 18(1) of the 2018 Act or otherwise. This is set out in Article 49(4).

[18] The conditions are that, according to domestic law, the register is *"intended to provide information to the public and open to consultation either by the public in general or by any person who can demonstrate a legitimate interest."* Such a transfer shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients (Article 49(2)).

All the above is set out in Article 49. The article is **identical** to its counterpart in the EU GDPR, except for references to *"Union or Member State law"* which have been replaced by domestic law. References to *"supervisory authority*" have also been replaced with references to the ICO, and the reference to Article 45 of the EU GDPR has been replaced by a reference to the DPA 2018's adequacy regulations.

PART II ADDITIONAL CONTENT PRINCIPLES FOR SPECIFIC PROCESSING

Direct marketing

The right to object can also be exercised in cases of direct marketing. **Once the data subject objects to processing for direct marketing purposes, the personal data can no longer be processed for such purposes**.[19]

As noted above, this right is set out in Article 21 of the UK GDPR, which is **identical** to its EU counterpart apart from the minor changes already outlined.

To help ensure that controllers carry out direct marketing lawfully and sensibly, the DPA 2018 requires the Commissioner to prepare a code of practice. This must contain practical guidance in relation to direct marketing in accordance with data protection requirements, and those in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).[20]

Automated decision making

Under the UK GDPR and the DPA 2018 data subjects also have the right not to be subject to a decision based solely on automated processing (including profiling) which produces legal effects concerning the data subject or similarly significantly affects them.

This is set out in Article 22 of the UK GDPR. This article is **identical** to its EU GDPR counterpart, except for the removal of the reference to Union or Member State law, and the addition of references to domestic law.

This right does not apply if the decision:

- is necessary for entering into, or the performance of, a contract between the data subject and a controller;

- is required or authorised by domestic law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

[19] Article 21(3).
[20] Section 122(1).

- is based on the data subject's explicit consent.

In the case of the first and the last point, the controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. The data subject's rights, such as requiring the controller to carry out processing that involves some human intervention expressing their point of view and to contest the decision, are specifically mentioned.

Section 14 of the DPA 2018, and regulations made under that section, make provisions for safeguarding data subject's rights, freedoms and legitimate interests in cases that fall within the second point. The controller must notify the data subject of any decision under this section in writing.[21] This must be done as soon as reasonably practicable. The data subject has a month, from receipt of the notification, to request the controller:

- reconsider the decision, or;
- take a new decision that is not based solely on automated processing.

The controller must consider and comply with the request, and inform the data subject of the steps taken to comply with the request, and the outcome.[22]

As with the EU GDPR, decisions cannot be based on sensitive data, unless point (a)[23] or (g)[24] of Article 9(2) applies, with suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

PART III: PROCEDURAL AND ENFORCEMENT MECHANISMS

Competent supervisory authority; compliance; redress mechanisms

The Information Commissioner's Office (ICO) is the UK's independent supervisory authority. The ICO is tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions. They act with complete independence and impartiality in the performance of their duties and the exercise of their powers, which have increased significantly in recent years.

[21] Section 14(4)(a).

[22] The controller needs to complete this process within the period described in Article 12(3) of the UK GDPR.

[23] Article 9(2)(a): Paragraph 1 [processing of sensitive personal data] shall be prohibited unless "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject".

[24] Article 9(2)(g): Paragraph 1 [processing of sensitive personal data] shall be prohibited unless "processing is necessary for reasons of substantial public interest, on the basis of domestic 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".

The DPA 2018 has given the Commissioner new powers to effectively enforce these new responsibilities, ensure compliance with data protection rights, and promote awareness of data protection.

The ICO will also provide the data subject with advice on effective administrative and judicial redress. Individuals and organisations with concerns about information rights practices can pursue legal remedies to enforce their rights effectively, and ensure compliance. This can take the form of private enforcement actions or complaints to the ICO. If an individual or organisation does not agree with the decision the ICO has made, or disagrees with their interpretation of the law, they can also seek action through the Courts.

Further information, among other things, on the ICO's powers and responsibilities as well as redress mechanisms for individuals, can be found in Section G *(*Role of the ICO and Redress).

Accountability
The UK GDPR, supplemented by the DPA 2018, sets out various measures to ensure the accountability of controllers and processors. These include:

- The Principle of Accountability: Article 5(2) of the UK GDPR stipulates the requirement for controllers to be responsible for, and be able to demonstrate compliance with, Article 5(1). This lists the various principles relating to the processing of personal data that are set out above. The requirement is **identical** to its EU GDPR counterpart.

- The designation of a data protection officer: Articles 37-39 of the UK GDPR set out the requirements regarding the designation of the data protection officer, position and tasks of the data protection officer. The articles are **identical** to their EU GDPR counterparts, except for replacement of the reference to Member State or Union law with a reference to domestic law, and replacement of the reference to "supervisory authority" with one to the ICO.

- Records of processing activities: Article 30 of the UK GDPR sets out the requirement to maintain a record of processing activities. The article is **identical** to its EU GDPR counterpart, except for:
    - The replacement of the reference to supervisory authority, with the ICO;
    - The ability to provide, as appropriate, a general description of the security measures referred to in section 28(3) of the DPA 2018 rather than the technical and organisational security measures referred to in Article 32(1);

  An "augmented" record of processing is required in certain situations for processing sensitive data. This is explained in Section E.

- Data protection impact assessments: Articles 35-36 of the UK GDPR outline the circumstances in which controllers are required to carry out a data protection impact assessment, as well as cases in which prior consultation with the ICO is necessary. Articles 35-36 are **identical** to their EU GDPR counterparts except for:
    - Removal of the reference to Member State or Union law and EU mechanisms, bodies or institutions;
    - Replacement of the term *"supervisory authority"* with the ICO;
    - The addition of a new Article 36(4A), defining the term *"relevant authority"* that substituted the term *"member states"* in Article 36(4) of the EU GDPR.

- Data protection by design and default: Article 25 of the UK GDPR places a requirement on controllers to implement appropriate technical and organisational measures to meet the requirements of the UK GDPR and protect the rights of data subjects. It is **identical** to Article 25 of the EU GDPR;

- Breach notification: Articles 33-34 of the UK GDPR place a requirement on controllers and processors to notify the Commissioner in the case of a personal data breach. The articles are **identical** to their EU GDPR counterparts, except for the replacement of the term *"supervisory authority"* with the ICO.

PART IV: LAW ENFORCEMENT AND NATIONAL SECURITY PROCESSING

The UK's data protection legislation provides unprecedented independent oversight of the activities and conduct of the UK's law enforcement framework, national security framework, and investigatory powers.

The processing of personal data by law enforcement agencies, as well as the security and intelligence agencies, is governed by Parts 3 and 4 respectively of the DPA 2018, while a comprehensive legislative framework applies to their use of investigative powers including the Investigatory Powers Act 2016.

The 2018 Act provides clear legal bases for law enforcement and intelligence service processing, including the data protection principles, obligations of controllers and principles, rights of data subjects and the role of the ICO and the courts in providing effective remedies.

Further information on law enforcement and national security processing is set out in Section F: Law Enforcement and Section H: National Security.