Explanatory Framework for Adequacy Discussions

Section E: Restrictions and Processing Conditions

Overview

This section sets out the UK's principled approach to legislating for the restrictions set out in the UK GDPR, including the prohibition on the processing of sensitive and criminal convictions data, and restrictions on the rights of data subject rights as well as other provisions. The narrative will be accompanied by detailed technical annexes setting out the rationale and safeguards for each individual restriction.

Section E: Restrictions

Overview

As set out in Section D – the Adequacy Referential – the UK GDPR contains a range of data subject rights, obligations on controllers, and prohibitions on certain types of processing, e.g. sensitive data. It also permits restrictions to be made to a number of these provisions and sets down conditions for such restrictions.

The DPA 2018 contains the restrictions themselves. Each restriction has been drafted in a manner that ensures it is **necessary** in a democratic society and **proportionate** to the legitimate aim it pursues.

The approach in the DPA 2018 could be characterised by the following further two principles:

1. The **principle of specificity.** This meant taking a granular approach, splitting broad restrictions into multiple, more specific provisions. This helps ensure each provision is necessary and proportionate. It also improves legal certainty for controllers and transparency for individuals.

2. The **principle of conditionality.** This ensures that each provision has appropriate safeguards in the form of limitations or conditions to prevent abuse.

This overview outlines the application of these two principles. A series of annexes to this section provide further details on each restriction, clarifying its rationale and its safeguards. For the sake of completeness, they cover all restrictions, including ones which may not be relevant to the essential equivalence test, e.g. their scope will not encompass personal data transferred from the EU. The annexes consist of:

1. Processing conditions for sensitive data. Article 9 of the UK GDPR creates a prohibition on processing sensitive data but restricts this prohibition by setting out a limited number of processing conditions. It permits further processing conditions, with certain specifications, to be set out elsewhere in law. These are set out in Schedule 1 to the DPA 2018;

2. Processing conditions for criminal convictions data**.** Article 10 of the UK GDPR only permits processing of such data under the control of official authority or when authorised by domestic law providing for appropriate safeguards. Schedule 1 to the DPA 2018 sets out such processing conditions or authorisations;

3. Restrictions of various rights and obligations. Article 23 of the UK GDPR permits restrictions for a limited range of purposes, as do Articles 85 (freedom of expression)

and 89 (processing for archiving in the public interest, scientific or historical research, or statistical purposes). The DPA 2018 sets out such restrictions.

The Principle of Specificity

The UK's approach in the DPA 2018 can best be described as favouring having a set of tightly focused restrictions to rights, rather than having a smaller number of restrictions that were broader and vaguer. The same principle applies for processing conditions for sensitive and criminal convictions data.

When a provision is tightly focused, this helps ensure it is necessary and proportionate. Bespoke limitations and safeguards can be added, tailored to the specific processing situation. Specificity also helps controllers know when they can and cannot use a provision. In turn, this provides more transparency and foreseeability for data subjects.

There are numerous instances of the principle of specificity at work in the DPA 2018. For example:

- Processing for promoting ethnic diversity at senior levels of organisations is separated from processing for promoting equality of opportunity;

- Processing for anti-doping purposes is separated from processing to protect the general integrity of a sport or sporting event;

- Processing in relation to dishonesty has been divided into three separate provisions. This was in order to distinguish processing for protecting the public against dishonesty from processing to comply with regulatory requirements about preventing dishonesty or unlawful acts, and processing for journalistic or similar purposes when the matter relates to dishonesty or unlawful acts;

- Processing in relation to elected representatives' duties is also divided into three separate provisions to distinguish the processing necessary for responding to the public, from disclosing data to an MP in response to a request, and for informing MPs about certain high-risk prisoners;

- Processing as part of a crime risk assessment system is separated from processing for preventing crime;

- Processing for protecting the economic well-being of individuals with certain disabilities or conditions is separated from processing for the safeguarding of children and individuals at risk to protect their physical, emotional, or mental well-being.

Section E: Restrictions

The Principle of Conditionality

Complementing the principle of specificity is the principle of conditionality. This is about ensuring that each provision has **the appropriate safeguards** in the form of limitations or conditions. As a starting point, processing under each provision is subject to the overarching safeguards in the UK GDPR. These are identical to the EU GDPR, as set out in the Adequacy Referential.

They include but are not limited to:

- core principles such as data minimisation and purpose limitation;
- the need for a lawful basis for processing;
- effective, enforceable data subject rights, including the right to access and erase the data, except when a restriction applies;
- the requirement to ensure an appropriate level of security for personal data;
- the requirement to maintain a detailed record of processing activity;
- the requirement to conduct a data protection impact assessment, in certain circumstances, including if processing sensitive data on a large scale;
- the requirement to designate a DPO in certain circumstances, including if core activities consist of processing sensitive data on a large scale;
- the ability for the data subject to lodge a complaint with the Information Commissioner and seek judicial redress for violations.

Beyond those safeguards, the DPA 2018 also ensures that **bespoke conditions apply**, tailored to the particular processing situation. Examples of such conditions are listed below, divided between those for processing sensitive and conditions data and those for restricting data subject rights and other provisions.

Limitations and safeguards for sensitive and criminal convictions data (Schedule 1)
As set out in the Adequacy Referential, Article 9 of the UK GDPR provides for a general prohibition against processing sensitive data, subject to exceptions in limited circumstances set out in Article 9(2) UK GDPR and Schedule 1 to the DPA 2018.

Section E: Restrictions

Sensitive data includes data on ethnic origin, health and sexual orientation, among others. Along with criminal convictions data, the processing of this data may present particular risks for the rights and freedoms of data subjects, e.g. by exposing them to discrimination.

The processing conditions in Schedule 1 supplement Articles 9 and 10 and set out additional specific circumstances in which the processing of sensitive data and criminal convictions data is permitted under UK law. They are accompanied by a number of safeguards in the form of limitations or conditions. Depending on the particulars of the situation, including the risks, each processing condition may require some or many of the below range of conditions. These conditions are set out in the Act and include:

- **Requiring the controller to have an Appropriate Policy Document**. This must outline the controller's procedures for securing compliance with the principles in Article 5 of the UK GDPR. It must also set out policies for retention and erasure, with an indication of the likely storage period. Controllers must review and update this document as appropriate. They need to keep it for six months after processing is finished and must make it available to the ICO on request;

- **Requiring the controller to have an augmented record of processing**. This builds on the requirement under Article 30 of the UK GDPR for controllers processing personal data to maintain a detailed record of processing activity.

  As with the EU GDPR, the UK GDPR states this record must include contact details; the purpose of any processing; categories of data subjects, data, and recipients; information on international transfers; information on storage periods and security measures where possible.

  But when a processing condition in Schedule 1 requires an **augmented** record of processing, the record must **also** include information on:

  I. which condition is relied on under the Act;
  II. how the processing satisfies Article 6 of the UK GDPR (lawfulness of processing);
  III. whether the personal data is retained and erased in accordance with the controller's policies, as set out in the Appropriate Policy document. If the policies have not been followed, the log must record the reasons;

- **A necessity test**. This builds on the requirement in Article 5 of the UK GDPR for data to be limited to what is necessary for the given purpose. The necessity test stipulates that processing activities must also be limited to what is necessary for the given purpose. It thus aims at avoiding "overprocessing" of the same data for the same purpose. In this way, it builds on both the principles of data minimisation and purpose limitation in Article 5.

For example, paragraph 27 provides for processing of sensitive data for anti-doping purposes. The necessity test means processing can only take place if it is necessary for measures designed to eliminate doping in sport, or if it is necessary for providing information about suspected doping. Any processing of the data that is for those purposes but is not necessary to achieve them is not permitted;

- A **consent test**. This is aimed at helping ensure that the bespoke processing conditions are not used when explicit consent is a reasonable option.

  For example, paragraph 16 creates a processing condition for charities to process sensitive data to support individuals with certain disabilities or medical conditions. A consent test is attached to it: the charity can only use this processing condition if it could not reasonably be expected to obtain consent from the data subject, **and** it is not aware of consent being withheld.

  In several cases, however, consent may not be a valid option because the data subject would not have a genuinely free choice, e.g. processing an athlete's health data to check for doping;

- **A test as to whether the processing is in the substantial public interest**. Most of the Schedule 1 processing conditions have this as an explicit condition for use. For example, processing for insurance purposes must be necessary for reasons of substantial public interest in order to use the processing condition in paragraph 20.

  When a processing condition does not have an explicit substantial public interest test, it is because the UK government takes the view that processing for its purposes is inherently in the substantial public interest. For instance, the administration of justice and Parliamentary functions as in paragraph 7 is vital for democracy;

- **Strict limitations on what kind of processing may use the processing condition,** such as:
  - limitations on the type of sensitive data that may be processed under a given processing condition in certain cases. For example, paragraph 8 provides for processing of sensitive data for promoting equality of opportunity. This processing condition can only be used if the data reveals racial or ethnic origin, religious or philosophical beliefs, sexual orientation, or if it is health data;

  - limitations on the type of controller that may use the processing condition. For example, paragraph 23 provides for processing of sensitive data in relation to elected representatives' responses to the public. This processing

condition can only be used if the controller is the elected representative or is under their authority;

- limitations on categories of data subject for the processing condition to be used. For example, paragraph 21 provides for processing of sensitive data for occupational pension schemes. This processing condition can only be used if the data subject in question is a sibling, parent, grandparent, or great-grandparent of the scheme member.

- **A test for damage or distress.** For example, paragraph 9 provides for processing of certain sensitive data for promoting racial and ethnic diversity at senior levels of organisations. This processing condition cannot be used if the processing is likely to cause substantial damage or substantial distress;

- **An unrestricted right to object.** For example, paragraph 22 provides for processing of sensitive data for a political party's activities. If the data subject gives notice in writing, the controller must cease processing within a reasonable period. The period is to be specified by the data subject in the written notice;

- **Safeguards in sectoral legislation or regulatory framework.** The limitations and conditions of certain restrictions are complemented by protections in the relevant sectoral legislation or regulatory framework. For instance, paragraph 1 provides a processing condition for processing sensitive data for employment, social security, or social protection purposes. The conditions for using this base are complemented by protections in the Equality Act 2010, e.g. that further processing of health data may constitute unlawful discrimination.

Limitations and safeguards to the restrictions to data subject rights in Schedules 2-4

- **A prejudice test.** Many of the restrictions in Schedules 2-4 only apply to the extent that compliance with the rights is likely to prejudice the relevant purpose of the processing.

  For example, the restriction in paragraph 22 of Schedule 2 concerns businesses' ability to hold discussions on their future structure, including decisions about employees that must remain confidential until their announcement. The restriction can only be used to the extent that complying with various rights e.g. subject access would be likely to prejudice the relevant business or activity.

  Employees may still access the rest of their data held by the company that does not fall under the restriction. If the prejudice test is no longer met in the future, e.g. an

announcement regarding staff changes was made, they may access the previously-restricted data;

- **Strict limitations on what kind of processing may use the restriction,** such as:
    - limitations on the type of personal data that can fall under the restriction. For example, paragraph 23 of Schedule 2 permits restricting the rights of information and access in relation to negotiations between a data controller and a data subject, e.g. if, during negotiations about their salary, an employee requests the minutes of Board meeting where the employer's negotiating position was agreed.

      This restriction can only apply to the employee's personal data when it constitutes the intentions of the controller for the negotiations. It does not apply to any other personal data of the employee held by the controller;

    - limitations on the type of controller that may use the restriction. For example, paragraph 11 of Schedule 2 provides for restrictions of various rights when they would prejudice certain regulatory functions. A table is provided listing the regulators the restriction may apply to;

    - limitations on the rights or provisions that can be restricted. For instance, paragraph 3 of Schedule 4 applies to adoption records when disclosure of the data is forbidden under certain enactments. It only restricts the right of access, and the general principles, in so far as they correspond to that right;

    - limitations on the precise purpose the restriction may be used for. For instance, paragraph 9 of Schedule 2 provides for the Bank of England to restrict certain rights when they would be likely to prejudice certain of its functions. The provision limits which of its functions are relevant for the restriction;

    - limitations on the precise situation in which the restriction may be used. For example, paragraph 3 of Schedule 3 states that the restriction only applies when the data is supplied in a report or in the form of evidence given to the court during proceedings. It also states that those proceedings must be subject to one of a limited range of statutory rules allowing the data to be withheld.

- **An expectations test.** A number of restrictions in Schedule 3 contain this as a condition. For example, paragraph 10 concerns social work situations where a data subject may not want a person acting on their behalf to access their personal data.

Section E: Restrictions

The processing must meet one of three conditions around the data subject's expectations. These are:

- that the data subject has expressly indicated it should not be disclosed, or
- that the data subject provided the data expecting it would not be disclosed to the requestor, or
- that the data was obtained through an examination or investigation that the data subject consented to but only in the expectation that the data would not be disclosed.

The last two conditions cannot be relied on if the data subject has since expressly indicated they no longer have those expectations;

- **A serious harm test.** A number of restrictions in Schedule 3 require this test to be satisfied. For example, paragraph 5 provides for restricting the right of access to health data. It can only apply if compliance with the right of access would be likely to cause serious harm to the physical or mental health of the data subject or another individual;

- **A reasonableness test.** Paragraph 16 of Schedule 2 restricts the right of access when complying with it would involve disclosing another person's data. However, the restriction does not apply if it would be reasonable to disclose the data without the other person's consent. The controller must consider a number of factors for making this assessment of reasonability, including any duty of confidentiality;

- **Further conditions for research and archiving purposes**. Paragraphs 27 and 28 of Schedule 2 restrict certain rights when processing is for historical or scientific research purposes, for statistical purposes, or for archiving that is in the public interest.

  Furthermore, personal data cannot be processed for any such purposes if the processing is likely to cause substantial damage or substantial distress to the data subject. It can also not be processed if it is for measures or decisions made about a particular data subject, except when necessary for approved medical research, as defined in the Act;

- **Public interest test for the special purposes.** Paragraph 26 of Schedule 2 relates to freedom of expression and allows the restriction of certain rights and obligations when processing is for journalistic, academic, artistic or literary purposes. In order to apply this restriction, the controller must reasonably believe that the application of those rights and obligations would conflict with these special purposes.

In addition, the restriction only applies where processing is carried out with a view to the publication of material for these purposes and where the controller reasonably believes publication of the material would be in the public interest. The provision sets out what the controller must take into account when making this determination;

- **Safeguards in sectoral legislation or regulatory framework.** The limitations and conditions of certain restrictions are complemented by protections in the relevant sectoral legislation or regulatory framework.

  For instance, paragraph 7 of Schedule 2 permits restrictions of various rights for a limited list of functions that are designed to protect the public from matters such as dishonesty. It is complemented by sectoral legislation such as the Health Service Commissioners Act 1993, which sets out rules on the confidentiality of information.