

Limiting Data Subject Rights and the Application of Article 23 of the General Data Protection Regulation

Introduction

The General Data Protection Regulation (EU) 2016/679 (the GDPR) comes into effect on the 25th May 2018. The GDPR raises the bar for data controllers and data processors. It reinforces their obligations over the personal data they process through increased transparency, security and accountability requirements. At the same time the GDPR standardizes and strengthens the right of all data subjects by providing a framework as to how those rights are to be exercised. Notwithstanding, the GDPR also prescribes a mechanism (as per Article 23) to permit the restrictions of those rights in particular and specific circumstances. The purpose of these guidelines is to assist organisations to implement and apply lawful restrictions of those rights and obligations provided for in Articles 12 – 22 and Article 34 of the GDPR.

Article 23

Article 23 mandates that specific Member State or Union Law (specific legislative measures) are required to restrict the scope of rights and obligations provided for in Articles 12 – 22 and Article 34 (and Article 5 insofar as those principles correspond to the rights afforded in the aforesaid Articles). Article 23, by setting out an exhaustive list of requirements which must be met to lawfully impose a restriction, confirms that any measure used to restrict the rights of a data subject must be of limited scope and applied in a strictly necessary, proportionate and specific manner. Section 60 of the Data Protection Act 2018 gives further effect to the provisions of Article 23 of the GDPR and both provisions should be read together.

Article 23 provides that any restriction must:

- (i) Be set out in Union or Member State Law via a legislative measure;¹
- (ii) Respect the essence of the fundamental rights and freedoms;²
- (iii) Be necessary and proportionate in a democratic society;³
- (iv) Safeguard one of the interests set out in Article 23(1);⁴ and
- (v) Contain specific provisions set out in the GDPR as per Article 23(2).⁵

¹ Recital 41 provides interpretation as to the meaning of a legislative measure. However this must also be read in light of Section 60 of the Data Protection Bill 2018.

² Note corresponding section of the Data Protection Act 2018 - Section 60(12)(a)

³ Note corresponding section of the Data Protection Act 2018 - Section 60(12)(b)

⁴ Note corresponding section of the Data Protection Act 2018 - Section 60(3) and Section 60(7). Also note recital 73.

⁵ Note corresponding section of the Data Protection Act 2018 – Section 60(6)

Any proposed legislative measure which intends to restrict the rights of a data subject requires all of the above conditions to be met in order for a measure to be lawfully relied upon. The relevant legislative provisions should be specific and explicit, laying down clear and precise rules regarding the exemption(s) being relied upon. The reliance and use of broad legislative measures may not be capable of meeting all the conditions set out above. It is a matter of each state entity that is relying on a restriction to clearly indicate the legal reasons as to why it is seeking to limit the fundamental rights of individuals based on its identified specific statutory requirements. This requires a detailed analysis by each state entity of Art 23(2)(a) to (h) to justify as to why the restrictions are required and in what circumstances they will apply.

The Conditions

(i) Be set out in Union or Member State Law via a legislative measure

Recital 41 of the GDPR provides an interpretation as to what is meant and entailed by a legislative measure. Ultimately whilst the GDPR does not necessarily require a legislative act to be adopted by parliament⁶, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights. As per Recital 8 of the GDPR the reason for the restriction and how and when it may apply should be comprehensible to persons to whom it applies.

(ii) Respect the essence of the fundamental rights and freedoms

The essence of a fundamental right means that interference with the right should not be such that the right is in effect emptied of its basic content and the individual cannot exercise the right.⁷ In other words the limitation may not go so far as to completely reduce the right of its core elements and thus prevent the exercise of the right. If the essence of the right is adversely affected by the measure, then the restriction is likely to be unlawful. As such legislation not providing for any possibility for an individual to pursue legal remedies in order to uphold their data protection rights may not be permissible if it does not respect the essence of the fundamental right to effective protection. Similarly a legal provision may prove unlawful if it fails to apply certain principles of data protection or inadequately addresses data security by not ensuring that appropriate technical and organisational measures are adopted against, for example accidental or unlawful destruction, accidental loss or alteration of the data.

(iii) Be necessary and proportionate in a democratic society

Necessity is a facts/evidence-based concept which must be considered in the light of the specific circumstances surrounding the provisions of a measure and the defined purpose it aims to achieve.⁸ In effect the measure must be effective and deliver upon its purpose. Proportionality requires that the content and form of the legislative measure does not exceed what is strictly necessary to achieve the objectives. The purpose of the restriction must therefore be appropriate for attaining the

⁶ Note the provisions contained in Section 60 of the Data Protection Bill 2018 provide further effect to Article 23 setting out a specific legal framework in order to meet the requirements of Article 23.

⁷ Note the European Data Protection Supervisory Guidelines - Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit

⁸ Consideration should be given to competing a Necessity Test (see footnote 7 above) via a DPIA, in circumstances where the proposed restriction could represent a high risk to the fundamental rights of individuals.

legitimate objectives pursued by the legislation at issue and does not exceed the limits of what is appropriate and necessary in order to achieve those objectives.

A proposed measure should be supported by evidence describing the problem to be addressed by the measure, how it will be addressed by the measure, and why existing or less intrusive measures cannot sufficiently address it. There is a requirement to also demonstrate how any proposed interference or restriction genuinely meet objectives of general interest of the State and EU or the need to protect the rights and freedoms of others.⁹ The restriction of data protection rights will need to focus on specific risks. An overly broad or blanket approach to the restriction of data protection rights would require justification by a particular and significant high risk.

(iv) Safeguard one of the interests set out in Article 23(1)

The GDPR provides a general list of interests which can be safeguarded and these are further clarified in Sections 60(3) and 60(7) {Important objectives of general public interest}, of the Data Protection Bill 2018. Therefore, an organisation that seeks to rely upon a restriction will need to satisfy that they are doing so because it is safeguarding a public interest pertaining to those general provisions.

(v) Contain specific provisions set out in the GDPR as per Article 23(2)

This is a mandatory requirement, which must be met, and each specific provision must be addressed in a proposed legislative measure unless that provision is irrelevant with regard to the specific objective of the legislation.¹⁰ As per the European Court of Justice Jurisprudence¹¹, legislation permitting such restrictions must lay down clear and precise rules governing the scope of the application of such a measure and imposing minimum safeguards.

It is imperative that the provisions of Article 23(2) are appropriately considered and applied where relevant as to:-

(a) the purposes of the processing or categories of processing;
List the Legal legislative basis for which the state entity operates from and specifically identify those statutory functions that require a restrictive safeguard to be applied.

(b) the categories of personal data;
For example, are there special categories of data involved? Data of Children or vulnerable adults?

(c) the scope of the restrictions introduced;
Is it for investigation and enforcement functions only?

(d) the safeguards to prevent abuse or unlawful access or transfer;
For example, will the data be disclosed to any other enforcement agency either in EU Member states or beyond? If so, what international treaty or mechanism can the data be legally transferred under?

(e) the specification of the controller or categories of controllers;
Is there a Governing Department to whom you have to report to? Are there any other agencies of third parties that the agency is legally required to cooperate with?

⁹ Note the European Court of Justice Case Tele2Severige (Case C-203/15) para 31 and also Recital 73 of the GDPR. Also note the European Court of Justice Case Digital Rights Ireland (Case C – 293/12)

¹⁰ Where a specific provision in Article 23(2) is believed to be irrelevant the DPC should be provided with the rationale for this position.

¹¹ See for example Tele2Severige (Case C-203/15).

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

For example, if an investigation is concluded without any cause of action resulting then the personal data should not be retained unless there are very specific justified circumstances as to why it is to be held and for how long a period. Care should be taken against, for example, any interference with an individual's right under Article 18 *Right to restriction of processing*, especially if the processing by a state agency is unlawful.

(g) the risks to the rights and freedoms of data subjects; and

What happens to the data of witnesses, any other third party that is not a party to the formal investigation? Secondly, has there been any formal assessment done to identify and address the potential risk to data subjects by having their rights limited.

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Have policies, procedures been updated and staff informed and trained? Are there any website or other publications made available to the public?

It may be useful to test specific scenarios which involve the obligations provided for under Articles 12 – 22 and Article 34 when considering the measures required.¹² Consideration of these and other similar issues will assist in determining how to address those specific provisions as required under Article 23(2).

Consultation with the Data Protection Commission (the DPC)

Section 60 of the Data Protection Act 2018 gives further effect to Article 23 of the GDPR setting out a specific procedure in relation to bodies who wish to make regulations to restrict the rights afforded by the GDPR under Articles 12 – 22 and Article 34.

Section 60(10) sets out that consultation with the Data Protection Commission is a mandatory requirement for regulations created under Section 60(5) and 60(6). Notwithstanding it will be at the discretion of the DPC as per Section 60(11) whether to provide written observations on the particular measure/restrictions proposed.

These guidelines should therefore be viewed as a support to those organisations that wish to draft regulations to restrict the application of the rights afforded under Articles 12 – 22 and Article 34 of the GDPR.

When consultation is formally sought from the DPC all of the above conditions should be specifically addressed and appropriately underpinned in the draft proposed legislative measures in advance of any approach to the DPC.¹³ In line with the requirements of GDPR and the principle of accountability it will be a matter for the body seeking to restrict the application of the rights afforded under Articles 12 – 22 and Article 34 of the GDPR to demonstrate how they have met their obligations in this regard.

Published May 2018

¹² For instance, how would an organisation approach an access request made by an individual who is under investigation? How would the organisation approach a situation where an individual seeks a right of rectification of their data? At what stage of the process or investigation would those restrictions be imposed or lifted? How would the organisation seeking to rely upon a restriction ensure that the personal data will not be misused?

¹³ This includes addressing all the specific provisions outlined in Article 23(2)