PRIVACY INTERNATIONAL

Privacy International's views on the derogations (exceptions) contained in the General Data Protection Regulation

10 May 2017

Introduction

Privacy International welcomes this consultation (https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views) and the willingness of the UK government to implement the EU General Data Protection Regulation (GDPR.)

The GDPR provides stronger standards of protection of personal data to those contained in the EU Directive 1995, whose provisions were implemented in the Data Protection Act 1998.

Notably the GDPR provides individuals with stronger rights, such as the right to data portability; higher standards of consent to processing of personal data; and the right to object profiling for direct marketing purposes. It also contains provisions that expand the scope of protection to cover types of personal data such as IP addresses and location data.

Privacy International believe improved rights and enforcement measures will generate greater trust and therefore greater engagement in the digital environment, which will in turn benefit the economy. The organisation regrets, therefore, that the consultation paper is lacking in specific details, including on what is at stake for individuals and companies with this significant legislation.

This lack of background explanation and details on government thinking, which constitutes due diligence practice in government consultations, will result in only those able to comment who have engaged with GDPR previously and are very familiar with its articles. This effectively means that government will receive the bulk of its feedback from controller and processor organisations, rather than data subjects or their representatives. In other words, the feedback is likely to be unbalanced. This is a worrying sign of the priority given by ministers to this important issue, and we request the DCMS to keep any such imbalance in mind when assessing the feedback.

Beyond the aspects of the GDPR derogations (exemptions) identified for the purpose of this consultation, Privacy International would like to highlight the following additional three points:

- GDPR should be implemented by primary legislation, in the form of a new Data Protection Act, which will offer a clear, foreseeable legal framework, which will benefit UK consumers and business;

- Like the current Data Protection Act, the new legislation should apply to private and public entities, including the police. As such the new legislation should incorporate the EU Directive on protecting personal data processed for the purpose of criminal law enforcement (Directive (EU) 2016/680);
- Significant resources should be allocated by the government to ensure meaningful consultations on the implementation of the GDPR, before and after its entry into force.

Comments on specific areas identified in the consultation

Theme 5 - Archiving and research (Article 89)

Article 89(2 and 3) – Under this provision, the UK laws may provide for derogations on some rights of the data subjects. Beyond the concerns and recommendations we make on Article 9 (see Theme 7), related to processing of sensitive personal data, we believe that any derogations envisaged under these provisions need to be very strictly construed. The data controllers should have the burden of proving that the data subject rights are likely to render impossible or seriously impair the achievement of the specific purposes of data processing and that derogating from such rights is necessary for the fulfilment of those purposes.

Here, as elsewhere where "public interest" is mentioned but not defined under the GDPR, Privacy International recommend that there is no further elaboration of this article in the UK law, but that the government tasks the Law Commission to undertake, in consultation with all relevant stakeholders, a comprehensive review of all UK legislation that includes "public interest" provisions, as well as its various interpretations, to ensure consistency with the requirement of the GDPR and other human rights obligations (under the EU Charter on Fundamental Rights and European Convention on Human Rights.)

Separately, Privacy International also recommend that the ICO develops a "Public Interest Test" for GDPR, similar to its guidelines for the Freedom of Information Act and Environmental Information Regulations (https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf; https://ico.org.uk/media/for-organisations/documents/1629/eir_effect_of_exceptions_and_the_public_interest_test.pdf)

Theme 6 - Third Country transfer

Article 49 (1) (d) – Derogations for specific situations (data transfers to third countries)
This article allows transfers of personal data to third countries which do not have adequate data protection without the appropriate safeguards for the transfers as listed in Article 46, if such transfer is "necessary for important reasons of public interest".

"Public interest" is left undefined here as elsewhere in the GDPR, though paragraph 49 (4) requires that the "public interest" referred to "shall be recognized in Union law or in the law of the Member State to which the controller is subject". Recital 112 explaining this article does give a number of examples of what could qualify as relevant important reasons of public interest under this

article (between competition authorities, tax or customs administrations, for public health, etc.), several in themselves quite broad. The assumption is, too, that all the public interests listed in Article 23 (see below, Theme 13) will also apply to this provision.

Although there is no requirement that the relevant provisions be notified to the European Commission (unlike in 49 (5), when limits are set to transfers of personal data to third countries), the government should bear in mind the implications of these provisions when the UK inevitably becomes a "third country" post Brexit and therefore would have to obtain an adequacy decision under Article 45 in order to continue to transfer personal data to and from the EU. Under the provisions of this article, when assessing "the adequacy of the level of protection", the Commission will also take account of "rules for the onward transfer of personal data to another third country or international organisation" (Article 45 (2) (a).

Privacy International recommend therefore that there is no further elaboration of this article in the UK law, but that the government tasks the Law Commission to undertake, in consultation with all relevant stakeholders, a comprehensive review of all UK legislation that includes "public interest" provisions, as well as its various interpretations, not only to ensure consistency across the board but also as readiness for adequacy status proceedings in the future.

Privacy International also recommend that the ICO develops a "Public Interest Test" for GDPR, similar to its guidelines for the Freedom of Information Act and Environmental Information Regulations (See Theme 5 above.)

Theme 7 - Sensitive personal data and exceptions

Article 9(2)(g) - Under this provision, the UK may adopt or maintain laws to allow controllers to process sensitive data for reasons of "substantial public interest" without consent or other legal basis. Substantial public interest must be strictly interpreted to avoid he creation of loopholes in protection and serious abuses. For example, Privacy International believe it cannot be used to legitimize the practice of political parties to compile databases of the political opinions of data subjects without their consent.

As for Theme 5 above, Privacy International recommend that the government tasks the Law Commission to undertake, in consultation with all relevant stakeholders, a comprehensive review of all UK legislation that includes "public interest" provisions, as well as its various interpretations, to ensure consistency with the requirement of the GDPR and other human rights obligations (under the EU Charter on Fundamental Rights and European Convention on Human Rights.)

Privacy International also recommend that as the ICO develops a "Public Interest Test" for GDPR (mentioned in theme 5 above), the ICO strictly define the high threshold of "substantial" public interest that needs to be met before sensitive personal data can be processed without consent or other legal basis.

Article 9(2)(h) - Under this provision, the UK may allow the processing of data for very broadly-formulated health care and health-related purposes without consent, on the basis of other laws and also "pursuant to contract with a health professional".

Given that not just health care but also secondary uses of health data, by public and private bodies, are becoming increasingly common, including by transnational (and certainly pan-European) bodies, there is need of clarity and limitations to the use of such data.

Privacy International recommend that the implementing legislation provides a comprehensive list of the current applicable UK law on this issue.

Article 9(2)(j) – Processing of personal data, including sensitive data, for scientific, historical or statistical purposes without the consent of the data subject (or other legal basis) may create loopholes in protection and lead to serious abuses.

This is particularly so in cases of where processing of sensitive personal data without consent is done for "commercial" scientific research purposes.

Privacy International recommend to implement this provision by specifically excluding research carried out for commercial purposes from the provisions of this article.

Article 9(4) – This provision stipulates that member states "may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data".

Privacy International recommend to implement this provision in way that does not allow for the UK to relax the relevant rules on processing of genetic, biometric or heath data further than as expressly envisaged in the Regulation. The UK may impose stricter conditions on the processing of such data or conditions that do not amount to limitations (e.g., purely technical standards), but not conditions that amount to relaxations of the rules.

Theme 9 - Rights and remedies

Article 22(2)(b) – Under this provision, the UK may adopt or maintain laws authorising fully-automated decisions and profiling (by private- and public sector controllers) that produce legal effects for the data subjects or otherwise "significantly affect" them, without the consent of the data subject or outside of a contractual relationship.

Profiling and other automated decision-making can pose substantial risks to privacy and other fundamental rights. The potential harms caused by profiling have been confirmed by the United Nations Human Rights Council (in a March 2017 resolution adopted by all Council's members, including the UK), which noted with concern "that automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights".

As such Privacy International believe that profiling and other forms of automated decision making should be subject to very strict limitations and in all circumstances allow the data subject the right not to be subjected to a decision

based on automated processing without his or her fully informed and explicit consent.

Privacy International recommend that during the implementation period the government review existing laws to ensure that there are no provisions to allow for automated decision-making by the private sector without fully informing the data subject.

Article 80 (2) - Representation of data subjects. Under this provision, the UK implementing legislation may recognize the capacity for qualified non-profit organisations to pursue data protection infringements of their own accord. We note and welcome that such capacity already exists under German law. It is also worth noting that in the UK 'opt-out' collective action is already enabled under the Consumer Rights Act 2015 and under the "super-complaint system" (Enterprise Act 2002) for any market failures that harm the interest of consumers. It is only logical that such empowerment should be extended to data protection, since personal data has become such an essential part of the national and global economy.
It has often been noted how the imbalance of powers between powerful companies and data subjects makes it very difficult for individuals to effectively claim their rights, notwithstanding the important role played by the ICO in protecting personal data.

Privacy International recommend that in implementing the GDPR the United Kingdom accept the possibility of collective action as envisaged in Article 80(2) of the GDPR, ideally on an 'opt-out' basis.

Theme 12 - Processing of Data

Article 6 (1) (c) and (e) and 6 (3) – lawfulness of processing

Under the provisions of this article personal data maybe collected and processed if the controller has to comply with a particular legal obligation (e.g. money laundering obligations by banks) or if it is a processing task "carried out in the public interest" or the "exercise of official authority". Further, such processing can only occur if stipulated by Union law or Member State law under a number of conditions to ensure further compliance with the provisions of the GDPR including the principles listed in Article 5 and necessity and proportionality.

The requirements in Article 6 (1) are consistent with references to public interest elsewhere in the Regulation, e.g. Articles 23 on derogations and 49 on third country transfers. The recommendations we make in Themes 6 and 13 also apply here.

With regards to Article 6 (c) regarding compliance with a legal obligation of the controller, the government should consider – in parallel with the implementation of the GDPR – of cataloguing and publishing the relevant UK legal obligations that involve some form of data processing, both in order to inform data subjects and demonstrate consistency and compliance with GDPR. This task can be commissioned to a third party for efficiency and speed.

Article 6 (4) – Further processing for incompatible purposes

This article allows for processing for a purpose different from the one that the data has been collected in the first place, and that does not rely on the data subject's consent or other legal requirements; it includes processing purposes provided for in Article 23 (1) (see also Theme 13, below.)

The article does include a number of criteria for assessment whether such processing is to be allowed, however these criteria are quite general and, furthermore, they are left to the controller to decide – which may well result in a big conflict of interest decision and which could only be tested in courts.

Privacy International recommend that the UK law stipulates that the assessments by controllers on "compatibility" should be subject to review by the ICO; if such processing involves cross-border transfers, the guidance of the ICO should be subject to cooperation, consistency and mutual assistance mechanisms provided for elsewhere in the GDPR.

Theme13 – Restrictions

Article 23 – Under this provision, the UK may restrict by law the application of data subject's rights for a closed list of purposes.

Privacy International note that with the exception of the addition of "enforcement of civil law claims", the list is largely the same as the corresponding one in the 1995 Data Protection Directive (Article 13(1)).

While the discretion under this provision is significant, it should be noted that any restrictions must "respect […] the essence of the fundamental rights and freedoms" and must be "a necessary and proportionate measure in a democratic society" to safeguard the listed interests.

Article 23(2) also adds that the law in question must contain "specific provisions" setting out the purposes of the processing, the categories of data concerned, the scope of the restrictions, the rights of data subjects (limited though these may be) and the relevant safeguards "to prevent abuse or unlawful access or transfer".

These conditions are important because they explicitly limit state's discretion to impose restrictions on applicable human rights standards (including the EU Charter on Fundamental Rights and the European Convention on Human Rights.)

As such the UK should exercise particular care in restricting the rights contained in the GDPR, given that non- compliance with these conditions – e.g., on the basis that an exemption is too broad, or that the applicable safeguards are ineffective – maybe be challenged in courts, including the CJEU.

In this regard, the UK should consider this provision also in light of the possible implication following the UK leaving the European Union. While it is too early to speculate on the results of the Brexit negotiations, it is inescapable that when the UK exits the EU it will become a "third country" outside the EU for the purpose of data protection. To continue the transfer of personal data to and from the EU, it would likely need to obtain a decision from the EU Commission that its data protection law is 'adequate' in terms of EU data protection standards.

The standard of 'adequacy' is quite high. The United Kingdom will need to prove that its data protection legislation provides 'essentially equivalent' protection to the GDPR, as interpreted by the CJEU.

Privacy International recommend that the UK use the opportunity of the implementation of the GDPR to publish a comprehensive list of the current applicable UK laws restricting the rights of data subjects and review these laws to ensure their strict compliance with applicable human rights standards.

Separately, Privacy International also recommend that the ICO develops detailed guidelines on how these restrictions are to be strictly interpreted, in order to ensure that they are used for a demonstrable legitimate aim in compliance with principles of legality, necessity and proportionality.