Callcredit
Information Group

Response to DCMS Call for Views:

General Data Protection Regulation (derogations)

Contact details

Introduction

This document provides a response from Callcredit Information Group ("CIG") to the DCMS Call for Views on the derogations contained in the General Data Protection Regulation.

CIG comprises a number of companies including Callcredit, a UK consumer credit reference agency ("CRA"), which facilitates the sharing of data on how people manage their repayment commitments. Data sharing is at the heart of our business and we provide services for both local and central government which assist the effective provision, sharing and understanding of personal data.

Responses

Theme 1 – Supervisory Authority

No response.

Theme 2 – Sanctions

No response.

Theme 3 – Demonstrating Compliance

The GDPR says that codes of conduct are to be encouraged and this should be reflected by creating an effective framework to make it easy to approve and formalise appropriate codes. There must be as much flexibility in operation as possible around codes of conduct. To work well, they must be able to attain a level of prescription that will add value while at the same time supporting change through flexibility and avoiding artificial constraints on the codifying process, as technology and circumstances continue to evolve rapidly. Ownership of the ratification of any national codes of conduct should naturally sit with the ICO.

Theme 4 – Data Protection Officers

No response.

Theme 5 – Archiving and Research

Derogation under Article 89(2) is vital to preserve the current effect of section 33 of the Data Protection Act 1998 ("DPA"). Historical statistical processing is necessary for a wide range of reasons, which include supporting statistically sound, fair and non-discriminatory profiling and decision making.

Theme 6 – Third Party Transfers

No response.

© Callcredit Information Group 2017
All Rights Reserved

Theme 7 – Sensitive Personal Data and Exemptions

No response.

Theme 8 – Criminal Convictions

Derogation is required to support employment screening in relation to jobs where a previous conviction or offence would be an issue of serious concern. These will not always be situations where failure to conduct a check would breach other regulations. They may also include situations where there is no legal requirement yet checks are clearly justified. Examples would include working in financial services (in roles not formally designated by the FCA to require such checks) or in other areas where roles have the capability to facilitate fraud or other offences, and working with vulnerable persons.

Theme 9 – Rights and Remedies

Article 22 – Automated individual decision-making, including profiling

Derogation may be required in this area to support the use of automated decision making and profiling for purposes such as credit scoring and protecting against fraud. It will be necessary to consider these issues particularly carefully, as GDPR could potentially be interpreted to cover more ground here than is the case under the Data Protection Directive 1995.

In a credit context, fraud can include first party fraud, where a borrower legitimately obtains credit but has no intention of repaying it, misstates their commitments or income at application, changes address in an attempt to distance themselves from debts and mislead lenders, or misrepresents their identity. It is important that derogation supports the need to prevent all frauds of these kinds.

Attention should also be given here to "future-proofing" against fraud methodologies as yet unknown, particularly given the ongoing evolution of Open Banking and associated advances in payments services.

Article 26 – Joint controllers

The UK implementation of the Data Protection Directive created a concept of controllers in common, and we suggest this should be retained alongside the concept of joint control.

Article 80 – Representation of data subjects

UK law should carefully define how relevant not-for-profit entities must be constituted and authorised to exercise rights on behalf of data subjects, to avoid any unintended consequences that might not be directly in line with consumer interests. Existing models, such as the class action provisions introduced by the Consumer Rights Act 2015, could perhaps be drawn on to inform this work and create consistency.

© Callcredit Information Group 2017
All Rights Reserved

Theme 10 – Processing of Children's Personal Data by Online Services

No response.

Theme 11 – Freedom of Expression in the Media

No response.

Theme 12 – Processing of Data

Article 18 – Right to restriction of processing

The right to restrict processing carries with it a clear risk that it could be abused by individuals who challenge processing for unrelated reasons. For example, an individual might seek to conceal information about themselves in order to secure an advantage, by challenging the continued processing of that information and thereby hiding it from third parties who ought to be made aware of it. There is some protection here through the possibility of taking into account the need to protect the rights of another natural or legal person, but consideration could be given to strengthening this through derogation.

Theme 13 – Restrictions

Preserving current exemptions

A range of DPA exemptions are used to obtain and process CRA data for appropriate purposes. These include:

- section 28 (National Security)
- section 29 (Crime and Taxation)
- section 31 (Regulatory activity)
- section 35 (Disclosures required by law or made in connection with legal proceedings etc.)

Given the purposes and uses of these exemptions, it is vital that the ability to obtain this data, and the maintenance of relevant restrictions on information provision should be continued, whether through GDPR derogations or as part of the forthcoming implementation of the Law Enforcement Directive.

The impact of the wider changes in the GDPR creates a need to review how these exemptions would function in future. Most features of the existing exemptions should be retained – perhaps most importantly that they generally have voluntary effect on the data controller. However, in some areas unintended consequences could result if the exemptions were simply imported with no changes.

© Callcredit Information Group 2017
All Rights Reserved

Creation of a right to rely on a recipient's confirmation that an exemption applies

When a suitable third party (such as a police force) requests data from us under an exemption, we are forced to rely on their confirmation that the grounds for the request are sound and that the exemption therefore applies. It is clearly not possible or appropriate for us to review and confirm the exemption grounds in each case to satisfy ourselves that the exemption correctly applies. As such, and given the increased requirements of the GDPR, it would be appropriate for exemptions within this Theme to be accompanied by a new provision which explicitly confirms a right to rely upon a confirmation asserted by a suitable third party.

Preserving CRA-specific provisions

Derogation is also required under Article 23 to retain the existing provisions in the DPA (and associated regulations) which specifically relate to CRA functions. It is vital to retain the substance of these provisions to avoid undesirable effects on financial services and on information society services.

There are four key areas in the current legislation to be considered: the presumption limiting the scope of subject access requests made to CRAs; the provision on fees and the timeline for responding to such requests; the prescribed statement to be included with responses to access requests; and the specific rights of correction or removal of information under the Consumer Credit Act 1974.

Retaining the accuracy principle's interpretive provision

It is also vital to retain the substance of paragraph 7 of Schedule 1, Part II of the DPA. This clarifies the scope of a controller's responsibility in relation to the accuracy of data that it obtains from third parties. It confirms that CRAs are not obliged to independently verify the accuracy of all incoming data, which would be impossible.

This is a complex and focused area, and we request an opportunity to discuss it with DCMS in greater detail.

<u>Theme 14 – Rules surrounding Churches and Religious Associations</u>

No response.

<u>Additional question – cost impact</u>

> *"In the context of the derogations above, what steps should the Government take to minimise the cost or burden to business of the GDPR?"*

Our view is that current DPA exemptions should be continued unchanged so far as is possible in order to reduce the burden on industry, with the exception of specific enhancements such as those we mention above. The cost of uncertainty to business must also be recognised, and we request that a draft of the final form of the legislation should be shared as soon as is practicable.

© Callcredit Information Group 2017
All Rights Reserved