Data Protection Team
Department for Culture, Media & Sport

BY EMAIL

10 May 2017

Dear Sirs

GDPR and derogations for fraud prevention

Thank you for the opportunity to respond to the consultation, "Call for view on the General Data Protection Regulation derogations", dated 12 April 2017 (**Consultation**).

In short, Cifas processes personal data for good reasons, i.e. to prevent fraud and wishes to continue to do that without being hindered by fraudsters exploiting loopholes in the new law. Our response to the Consultation is intended solely to protect that right (and, where appropriate, improve on any ambiguities and learnings from the current legislative framework).

Fraud prevention is in the public and consumers' interest

Fraud prevention organisations play an essential role in combatting financial crime and fraud. Fraud is an increasingly prevalent crime in today's society with almost one in every two crimes is a fraud or cybercrime.[1]

The Office of National Statistics (**ONS**) Crime Survey of England and Wales estimates that 5.8 million incidents of fraud and computer misuse were experienced by adults aged 16 and over in England and Wales for the year ending March 2016.

Fraud accounted for almost two-thirds of this estimated total (3.8 million offences) with the majority of these relating to bank and credit account fraud – that is, fraudulent access to bank, building society or credit card accounts or fraudulent use of plastic card details.

[1] The Office of National Statistics (ONS) Crime Survey of England and Wales now estimates that fraud and cybercrime now account for almost six million offences. See https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016

Clearly, with fraud and cybercrime now rivalling car crime, robbery and burglary as the high volume crime of the twenty first century, government, law enforcement, businesses and consumers must work together to combat this ever growing threat.

At the core of the Cifas cross-sector data sharing model is the view that fraud should not be tackled in isolation. For example, a credit card provider will find benefit in knowing about previous frauds that have affected an insurer, as an insurer will obtain benefit from knowing about frauds against the telecoms sector.

*The fact that our members prevented over **£1 billion** in fraud losses in 2016 – for the fourth year running – is evidence that an integrated and collaborative cross-sector approach is an effective remedy to combat an ever-increasing threat.*

Cifas operates and manages the UK's largest cross-sector fraud sharing databases, the National Fraud Database (**NFD**) and the Internal Fraud Database (**IFD**). Our members and consumers are reliant on the NFD and IFD to identify, deter and prevent fraudulent activity.

Cifas collaborates with a wide range of organisations and individuals to strengthen fraud defences and protect victims. Our partners include government, law enforcement, regulators, academia, and charities and our membership includes all retail banks, credit card providers, retail telecom providers, providers of consumer credit and public bodies.

Cifas' relationships with police and law enforcement agencies are particularly important to us and our members. We work with them to achieve the following three objectives:

- assist in the prevention of fraud;
- support the disruption of criminal gangs; and
- protect the public and the UK economy from the adverse effects of financial crime.

Cifas works with National Crime Agency (**NCA**) in the Joint Money Laundering Intelligence Taskforce and supports the Home Office Joint Fraud Taskforce, a taskforce that works to bring industry and government together to fight fraud.

Cifas has been designated a Specified Anti-Fraud Organisation (**SAFO**) under the Serious Crime Act 2007, which allows for the public sector to share information with and through Cifas with others to prevent fraud. Cifas also acts as a conduit for Home Office Immigration information to be supplied to banks in order that aspects of the Immigration Act 2014 can be facilitated.

Derogations under GDPR

On 25 May 2018, when the GDPR is due to come into force, Cifas, and other fraud prevention agencies and data controllers will be bound to comply with the new law. As you have identified, certain provisions in GDPR will be of fundamental importance to determining whether Cifas and these organisations can continue to provide essential services to its members and consumers to achieve the three objectives set out above.

In particular, the increased rights afforded to data subjects and accompanying disclosure obligations, coupled with the more stringent rules around consents could significantly hinder Cifas' ability to identify and prevent fraud and financial crime.

Cifas urges the Department to retain and, where necessary, reinforce the existing exemptions and derogations as part of the government's GDPR implementation framework to allow Cifas to continue to provide its essential fraud prevention solutions. In the absence of appropriate and suitably robust derogations, consumers and commerce may be substantially prejudiced.

Whilst understanding that a fair balance needs to be struck between individuals' privacy and fraud prevention activity, Cifas is particularly concerned should there not be the appropriate derogation(s) in place relating to Themes 5, 7, 8, 9, 12, 13 and 14 in the Consultation.

We have set out in the enclosed schedules, further details of Cifas' specific concerns and proposed solutions in relation to these Themes.

Yours faithfully,

Enc: Schedule, current derogations and proposed recommendations.

Fraud prevention organisations need a specific, public interest legal basis to process personal data for the purposes of preventing or detecting crime.

We have set out below the relevant Themes set out in the Consultation and, against each, what we consider to be the most pertinent provisions in the current and proposed new data protection law. Whilst we have sought to ensure that the responses below are exhaustive, the recommendations below are non-exhaustive. In any event, we hope that they serve as an indication of the key concerns Cifas has; once the Department has had an opportunity to consider the issues raised, we'd welcome an opportunity to discuss the derogations further, specifically (amongst other things) the derogation from the right for data subjects to require Cifas to disclose the specific logic employed in algorithms to detect fraud[2].

For the avoidance of doubt, any exemptions or conditions which rely on consent are of limited use, given that consent may be withdrawn at any time (i.e. by a fraudster to commit or enable fraud).

Theme 7 – Sensitive Personal Data; Theme 8 – Criminal convictions; Theme 12 – Processing of Data; Theme 13 - Restrictions

Section 29(1) (a) of the Data Protection Act (**DPA**) currently provides a derogation for the prevention or detection of crime, from the first data protection principle [*the first principle*] (except to the extent it requires compliance with the conditions in Schedules 2 and 3) and Section 7 and *in any case* to the extent that the application of those provisions would *be likely to* prejudice the prevention or detecting of crime.

This permits processing for the purpose of fraud prevention and, in so doing: (i) automatically makes such processing fair and lawful in accordance with the first principle (and Part II of Schedule 1, DPA); and (ii) avoids the need to respond to disclose personal data pursuant to a subject access request (**SAR**) under Section 7.

Notably, however, the derogation does not permit an organisation processing data for fraud prevention unless, in the case of personal data, one of the conditions in Schedule 2, or in the case of sensitive personal data, Schedule 3, is met or, as is generally accepted, the requirement to meet one of those conditions would be likely to prejudice the fraud prevention activity in question. In the case of Schedule 2 (personal data), this is relatively straightforward as an organisation can generally rely on the 'legitimate interests' condition. In the case of Schedule 3 (sensitive personal data), there is no applicable, corresponding 'legitimate interest' condition upon which private fraud preventions organisations can rely. Sensitive personal data may include, for example, information denoting racial or ethnic origin or relating to the commission or alleged commission of an offence.

[2] In this regard, Cifas still wishes to remain accountable, but considers that a regulator (or other trusted, independent third party) would be a more appropriate body to review and assess if any logic used is fair, non-prejudicial and proportionate, either from a privacy or other non-privacy perspective (eg in the same way that the Gambling Commission reviews software code in random number generation before issuing a remote gambling software licence).

Paragraph 7A of Schedule 3 by the Serious Crime Act 2007 provides that sensitive personal data may be processed where:

"*The processing—*

(a) is either—

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes."

In the case of sensitive personal data, it is necessary therefore to rely on both the fact that the inability to process such data would be likely to prejudice the prevention or detecting of crime and Paragraph 7A of Schedule 3.

Whilst, in many cases, this may be conclusively relied upon, our view is, in the context of Section 29(1) (a) that the criteria 'likely to' is, in the context of the techniques that are increasingly necessary to detect innovative and creative methods of fraud detection used by fraudsters, may unintentionally hinder the ability of Cifas (and other fraud preventions organisations) to provide effective fraud prevention solutions and services. In addition, there is some (again unintentional) ambiguity as to the extent to which the permissive derogation available under the prejudice test at the end of Section 29 applies to the need to meet one of the conditions in Schedule 2 and, especially, Schedule 3 (respectively).

In addition, Paragraph 7A only allows processing that is 'necessary' for the purposes of preventing fraud or a particular kind of fraud. The necessity requirement may allow fraudsters or others to argue that the processing of such information was not strictly necessary for the purposes of preventing fraud. Accordingly, we'd welcome the use of the word, "reasonably" before, "necessary" or alternatively (and preferably) not using the words, "is necessary" so as to allow for the development of innovation in fraud detection techniques in the new law.

Under GDPR, special categories of data, under Article 9(1) also include biometric data. Biometric data will inevitably be increasingly be used for identifying or preventing crime and fraud prevention. Accordingly, for this purpose, it is essential that suitable, proportionate derogations are introduced that cover not only the new definition of 'personal data', but also, 'special categories of data' under GDPR.

In addition, the derogation does not sufficiently acknowledge or take into account that the fraud prevention solutions developed and employed by fraud prevention

organisations benefit and protect innocent consumers whose identity and credit may be prejudiced by the inability to carry out processing for these purposes.

Recommendations:

- in any corresponding derogation to Section 29(1)(a) of the DPA under the new law implementing GDPR, the test for prejudice is amended to, 'may' rather than ' is likely to' and that the derogation is either more clearly stated to apply to the need to meet one of the conditions in Schedule 2 or 3
- that a corresponding derogation to Paragraph 7A of Schedule 3 is introduced and which provides equivalent protection for effective fraud prevention is included in GDPR transposition law (taking into account the "necessity" qualification outlined above) and that this continues to apply SAFOs, and any organisation seeking to prevent fraud).
- Article 9 - in this regard, therefore, we propose that a similar fraud prevention derogation (akin to Paragraph 7A, Schedule 3, but amended as requested) is included in Article 9(2) as a justification for processing special categories of data and that UK law expressly states that processing for the purposes of detecting or preventing crime is a legitimate interest.
- there is an express acknowledgement that the wider benefits of fraud prevention to consumers generally (when considering any prejudice to the prevention or detection of crime).
- Article 10: specifically, we ask that the Department clarifies in any draft implementation legislation relating to Article 10 that:
    - it is expressly clarified that:
        - (a) data, "*relating to criminal offences*" does not apply to data held for fraud prevention purposes relating to alleged, unconfirmed or confirmed offences (in the context of, for instance, Cifas' Internal and National Fraud Databases),
        - (b) a database held for fraud prevention purposes should not be considered a "*comprehensive register*" of criminal offences; and
        - (c) the continuation of "basic disclosures" derogation for fraud prevention purposes relating to criminal convictions still applies.

<u>Theme 5 – Archiving and Research</u>

Section 33, DPA also provides organisations with the ability to process (and to retain indefinitely) personal data for the purposes of research, historical and statistical purposes. And, in turn, also removes the right for individuals to be provided with information containing personal data about them pursuant to a SAR. It is essential that

Cifas (and other fraud organisations) continue to be provided with a specific, new derogation in this regard (to protect Cifas' existing rights).

Recommendation:

- Article 89 – please clarify that the processing of data for research purposes will continue to be exempt from the duty to respond to SARs under the GDPR (as it does currently under DPA), and that fraud organisations will continue to be able to retain such data indefinitely.

Theme 9 – Rights and remedies

In the same way that we require that processing data for research purposes will be exempt from the duty to respond to SARs, we'd also expect a corresponding derogation from the right to erasure.

Similarly, to develop fraud prevention technologies, solutions and methods that are fit for purpose to tackle the increasingly sophisticated techniques and technologies used by fraudsters, it is imperative that fraud prevention organisations have an ability not only to: (a) profile users (to identify confirmed fraud and the likelihood or the propensity for an individual to commit fraud); but also (b) develop, improve and employ the use of automatic processing (eg algorithms to detect anomalies in behaviour) to identify or prevent fraud.

As regards automated processing specifically, Cifas is particularly concerned by allowing fraudsters a right to object to their personal data from being processed. In addition, Cifas is concerned by being obliged to provide fraudsters with specific details of how its automated processing fraud detection techniques work as, this in itself, may prejudice its ability to use effective fraud detection methods to identify or prevent crime[3].

In addition, Cifas is concerned that any copyright, other intellectual property rights and confidentiality in the trade secrets and know-how uses in such techniques (including those licensed from third parties) may be infringed or prejudiced by the disclosure of the logic employed.

[3] In this regard, we draw DCMS' attention to the responses to the recent Select Committee's inquiry on '*Algorithms in Decision Making*' at http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2015/inquiry9/publications/ and select responses to that inquiry, including, in particular, responses from: (i) Jamie Grace, Senior Lecturer in Law, Sheffield Hallam University (and the recommendation for a national regulator in police intelligence algorithms), (ii) The Information Commissioner; (iii) the Financial Services Consumer Panel; and (iv) UCL. In addition, we also draw the Department's attention to the response from Marion Oswald, University of Winchester, and Sheena Unwin, Durham Constabulary and the following article on AI in Custody Decisions (and its implications) http://www.bbc.co.uk/news/technology-39857645

Recommendation:

- Article 17 – please clarify that the processing of data for research purposes will continue to be exempt from the right to erasure under the GDPR (this is not currently a statutory right under DPA, only a common law right).

- Article 21 - we'd recommend that a derogation is included in relation to profiling, in the same vein as currently exists in Section 29(1)(a), DPA, but as recommended that it is improved upon and clarified as set out above under Theme 7.

- Article 22 – we'd recommend that a derogation is included in relation to automated individual decision-making, including profiling, in the same vein as currently exists in Section 29(1)(a), DPA, but that it is improved upon and clarified as set out above under Theme 7. We would, for instance, welcome the introduction of standards, certification and review and assessment by an independent third party to ensure that Cifas and any other fraud prevention organisation is accountable for the logic employed in any algorithms employed.

Theme 12 – Processing of data

Under the current wording proposed by GDPR, a data controller would be bound to suspend the processing of personal data (pending the outcome of the review) where a data subject exercises his or her right to challenge legitimate interests' based processing. Clearly, in the context of fraud prevention, this would essentially allow fraudsters to disable fraud prevention organisations from processing data relating to them during this suspension period (and also to string out this period, wherever possible). Cifas and other fraud prevention organisations should instead continue to have the right to process personal data up to and until such time as the outcome of legitimate interests challenge and review is known.

The same would apply to any challenge to the logic employed in any automated decision making process.

In addition, Cifas and other fraud organisations would not want to fall foul of the blacklisting restrictions given the public interest in effective and proportionate fraud prevention.

Recommendation:

- Article 18(1) (d) – please confirm that the right for a data subject to restrict processing whilst a decision regarding verification of the legitimate interests (pursuant to a request to verify the legitimate interests justification under Article 21(1)) will not apply pending a decision. To allow a data subject a right to suspend processing during any assessment may prejudice Cifas' ability to detect or prevent crime relating to that data subject during any period of suspension.

- Article 88 – please confirm that the prevention of fraud derogation that currently applies in relation to the IFD will continue to be lawful. Given the recent history around actual blacklists in the construction industry, Cifas is concerned that the, "*more specific rules*" referred to do not prohibit the operation, management and processing of data legally processed through the IFD.

Additional question

We propose the following additional question: "*What steps should the Government take to minimise the cost or burden to business of the GDPR*".

The current established fraud prevention model epitomised by Cifas continues to be able to save £1 billion a year. Accordingly, it seems logical that the Department should continue to support the ability of fraud prevention organisations to carry out processing for the purposes of detecting or preventing fraud.

Yours sincerely