ICO Consultation: Data Sharing Code of Practice

Response by Callcredit Limited (trading as TransUnion)

September 2018

Q1 We intend to revise the code to address the impact of changes in data protection legislation, where these changes are relevant to data sharing. What changes to the data protection legislation do you think we should focus on when updating the code?

- The new accountability principle and the requirement to keep records of processing activities and overseas transfers under Article 30.
- The new requirements to provide information about the sources and recipients of personal data in privacy notices under Articles 13 and 14.
- The new notification requirement in Article 19 and the circumstances in which the disproportionate effort exception is likely to apply.
- Whether the concept of "controllers-in-common" continues to exist under the GDPR (alongside the concept of "joint controllers") and if so whether the requirements of Article 26 apply in those circumstances.
- The practical effects of Article 26.
- The circumstances (if any) in which it may be appropriate for controllers to report personal data breaches to each other.
- The role of the data protection officer, and the distinction between the DPO's advisory function and the decision-making function of the controller or processor in connection with data sharing decisions.
- DPIA requirements.

Q2 Apart from recent changes to data protection legislation, are there other developments that are having an impact on your organisation's data sharing practice that you would like us to address in the updated code?

Yes / No

No.

Q3 Please specify

Not applicable.

Q4 Does the 2011 data sharing code of practice strike the right balance between recognising the benefits of sharing personal data and the need to protect it? Please give details.

Yes / No

Yes.

Q5 In what ways does it achieve this?

The code sets out the relevant legal requirements but focuses on clear, practical guidance about how to apply those requirements.

Q6 In what ways does it fail to strike the right balance?

Not applicable.

Q7 What types of data sharing (eg systematic, routine sharing or exceptional, ad hoc requests) are covered in too much detail in the 2011 code?

In our view the 2011 code strikes the right balance.

Q8 What types of data sharing (eg systematic, routine sharing or exceptional, ad hoc requests) are not covered in enough detail in the 2011 code?

In our view the 2011 code strikes the right balance.

Q9 Is the 2011 code relevant to the types of data sharing your organisation is involved in? If not, which additional areas should we cover?

Yes it is relevant. However, we would welcome further materials relating to the data sharing scenarios mentioned in our response to question 10.

Q10 Please provide details of any case studies or data sharing scenarios that you would like to see included in the updated code?

<u>The credit reference agency data sharing model</u>

Financial performance data is shared with a CRA by lenders and other credit providers, generally in reliance on the "legitimate interests" legal basis. Each credit provider provides data subjects with a link to the Credit Reference Agency Information Notice to explain the ways in which CRAs use and share personal data.

The CRA collects the data from the credit providers, combines it with data from other sources (e.g. data about bankruptcies, IVAs, court judgments and the electoral register), and profiles it. This is also done in reliance on the "legitimate interests" legal basis.

The CRA shares the data back to the credit providers and also certain other organisations for certain specified purposes.

The credit providers are primarily responsible for the accuracy of the data supplied to the CRA but the CRA is also responsible for implementing appropriate measures, such as automated checking algorithms (to check whether the data received is plausible) and matching algorithms (to match the incoming data to the correct records in the CRA's database).

The CRA has mechanisms to allow data subjects to access personal data (see s. 13 Data Protection Act 2018 as well as Article 15 GDPR) and to challenge the accuracy of the personal data (see s. 159 Consumer Credit Act 1974 as well as Article 16 GDPR)

Sharing data as part of a product or service

An organisation operates an identity verification (IDV) product which allows financial services providers to check the identity of consumers in order to satisfy their know-your-customer and anti-money laundering requirements.

The product involves the financial services providers transferring data about consumers to the IDV provider through an API, which then checks the personal data against its own databases and confirms whether the consumer appears to be genuine. The IDV provider also keeps a record of the number of checks performed against each individual in order to help identify suspicious activity such as a surge in applications in the name of any particular individual.

The financial services providers show the consumers a privacy notice explaining the data sharing arrangements. Those privacy notices also link to the IDV provider's privacy notice, which contains more details about how the IDV provider uses the data that it receives. Each of the organisations involved acts as a controller and relies on the "legitimate interests" legal basis for its processing activities.

The IDV provider assesses the data protection implications of its product as part of its product development process, and establishes a set of rules for taking on new clients in light of that assessment. It does not need to perform a fresh assessment of the product every time it takes on a new client.

Each financial services organisation that wishes to use the IDV service assesses its own data protection obligations in relation to the use of that service.

Q11 Is there anything the 2011 code does not cover that you think it should? Please provide details.

Pending the update to your code of practice on anonymisation, it would be useful to understand whether the sharing of data in circumstances where the disclosing organisation could reidentify individuals from the shared data but the recipient organisation(s) could not is still considered not to be a disclosure of personal data.

Q12 In what other ways do you think the 2011 code could be improved?

Page 15 of the 2011 code says that it is "bad practice" to offer individuals an apparent choice if the data sharing will take place regardless of consent. Our understanding from other ICO materials is that the ICO now considers this to be fundamentally unfair (and therefore unlawful) rather than merely bad practice. It would be sensible to bring the code into line with the other materials.

Page 17 of the 2011 code suggests that the principle of fairness requires that personal data is shared in a way that people would not reasonably object to if given the chance. Some data sharing activities carried out by credit reference agencies do involve data sharing that the relevant data subjects would be likely to object to: for example, sharing a data subject's adverse credit history or information about their previous insolvencies or CCJs. Other organisations such as police forces, intelligence agencies and fraud prevention agencies will also share data in ways that the data subjects would generally object to. We would not regard these activities as unfair given the strong justification for the sharing activities. It would be sensible to amend the code to clarify this position.

As a general point, in our view the 2011 code is an example of a good and useful piece of guidance. It written at the right level and provides sound practical advice and reasonable best practice recommendations, rather than merely regurgitating what the legislation says. While it clearly needs an update to cater for the changes in law, we would not want the general approach of the code to change.

Q13 Are you answering these questions as:

A public sector worker?

A private sector worker?

A third or voluntary sector worker?

A member of the public

A representative of a trade association

A data subject

An ICO employee

Other

A private sector worker.

Q15 Please provide more information about the type of organisation you work for, ie a bank, a housing association, a school.

TransUnion provides a range of services which involve large-scale collection and sharing of personal data, including for the purposes of credit referencing, identity verification, fraud prevention, anti-money laundering and marketing.

Q16 **We may want to contact you about some of the points you have raised. If you are happy for us to do this please provide your email address:**

[redacted]