ICO consultation on the draft updated data sharing code of practice

Data sharing brings important benefits to organisations and individuals, making our lives easier and helping to deliver efficient services.

It is important, however, that organisations which share personal data have high data protection standards, sharing data in ways that are fair, transparent and accountable. We also want organisations to be confident when dealing with data sharing matters, so individuals can be confident their data has been shared securely and responsibly.

As required by the Data Protection Act 2018, we are working on updating our data sharing code of practice, which was published in 2011. We are now seeking your views on the draft updated code.

The draft updated code explains and advises on changes to data protection legislation where these changes are relevant to data sharing. It addresses many aspects of the new legislation including transparency, lawful bases for processing, the new accountability principle and the requirement to record processing activities.

The draft updated code continues to provide practical guidance in relation to data sharing and promotes good practice in the sharing of personal data. It also seeks to allay common concerns around data sharing.

As well as legislative changes, the code deals with technical and other developments that have had an impact on data sharing since the publication of the last code in 2011.

Before drafting the code, the Information Commissioner launched a call for views in August 2018. You can view a summary of the responses and some of the individual responses here.

If you wish to make any comments not covered by the questions in the survey, or you have any general queries about the consultation, please email us at datasharingcode@ico.org.uk.

Please send us your responses by **Monday 9 September 2019**.

Privacy Statement

For this consultation, we will publish all responses except for those where the respondent indicates that they are an individual acting in a private capacity (e.g. a member of the public). All responses from organisations

and individuals responding in a professional capacity will be published. We will remove email addresses and telephone numbers from these responses; but apart from this, we will publish them in full.

For more information about what we do with personal data please see our privacy notice.

Questions

Note: when commenting, please bear in mind that, on the whole, the code does not duplicate the content of existing guidance on particular data protection issues, but instead encourages the reader to refer to the most up to date guidance on the ICO website.

Q1 Does the updated code adequately explain and advise on the new aspects of data protection legislation which are relevant to data sharing?

☐ Yes

☐ No

Q2 If not, please specify where improvements could be made.

N/A

Q3 Does the draft code cover the right issues about data sharing?

☐ Yes

☒ No

Q4 If no, what other issues would you like to be covered in it?

Multiple parties are sometimes involved in delivering a product or service through Open Banking. For example a price comparison application provider may share relevant data with a number of entities in order to find the customer the most suitable product. In such circumstances, the customer-facing TPP would pass on consumers' financial data to the other party. It is the consumer-facing TPP's responsibility to obtain explicit consent from the consumer. One of the significant issues that we have identified is the lack of clarity on the ways in which a regulated TPP can 'onward share' data which they have legitimately accessed with other non-regulated parties. PSD2 and GDPR do not provide a legislative framework for this eventuality or establish arrangements which offer consumers sufficient control over this type of data sharing arrangement.

Under PSD2, consumers must use strong customer authentication (SCA) to give access to their financial data with a third party, authorised and regulated by the FCA. The customer must also re-authenticate every 90 days that they wish to continue the access. The 90-day re-authentication is intended to provide some reassurance to the consumer that access for data-sharing will cease where they no longer want or use the product, although we believe there are valid arguments for some consents to be valid for longer than the 90 days permitted under PSD2. However, once obtained, the third party can onward share the data to other parties.

Our view is that it would be beneficial for controls to be available to consumers, providing the ability for them to revoke onward sharing and to view and manage these arrangements. A key principle that is embedded into the Open Banking approach is that consumers should know who their data is being shared with and be able to stop it as easily as they set it up.

Consumers may not always be aware that they have agreed to onward sharing. This reduces people's control over their data, increases the potential for fraud and their ability to protect themselves. If a consumer's data is breached it may be difficult for a consumer to assess where the breach occurred or who caused it, making it difficult to pursue a complaint.

Onward data sharing arrangements are processed under GDPR on the basis of consent, contract or legitimate interest. We believe that it would be helpful to set out the following key principles, which should

apply to onward sharing arrangements, so as to improve consumer protection:-

i. Unregulated TPPs should not themselves be able to "onward share". Limiting the chain of providers will ensure that consumers retain visibility over where their data is held.
ii. Consent to onward share should be separate from consent to set up an initial data sharing arrangement in a two stage process.
iii. Consent to onward share should specify what data is shared, the length of time the sharing continues and the purpose – just as it does for agreeing to a new data sharing arrangement.

The current Open Banking guidelines require that consumers are explicitly told about other providers that are involved in the delivery chain of a product or service, and that they give explicit consent for their data to be shared with all named third parties.

It would be helpful for the ICO guidance to cover these issues.

Q5 Does the draft code contain the right level of detail?

☐ Yes

☐ No

Q6 If no, in what areas should there be more detail within the draft code?

N/A

Q7 Has the draft code sufficiently addressed new areas or developments in data protection that are having an impact on your organisation's data sharing practices?

☐ Yes

☒ No

Q8 If no, please specify what areas are not being addressed, or not being addressed in enough detail

Consumer security and trust are built into the heart of Open Banking's architecture. This is evidenced by a number of core principles which have been designed to protect the customer's interests. One of these core principles is that the customer is required to provide their explicit and informed consent to their data being shared with each TPP. They have to re-approve access via TPPs every ninety days after the initial consent for the service. This consent must be fully GDPR compliant. The ability of end users to give meaningful, specific and informed consent is essential to ensure an appropriate level of trust that is necessary for the success of Open Banking as well as other Smart Data initiatives. It will build the confidence necessary for consumer engagement. The success of Smart Data initiatives rely on consumer willingness to share data in an environment where historically they have been reluctant to do so.

However, consent can be conceptually confusing and practically complicated. We believe that consent should be straightforward and consistent. For example, Open Banking has developed consent standards and dashboards to give consumers control and confidence.

There is growing concern that consumers are being asked for more consent that is necessary in order to provide the service that is being offered. The Law Society of Scotland argued in the evidence it presented to the Joint parliamentary Committee examining the Right to Privacy and the Digital Revolution Enquiry, that some policies that explain how data will be used are so long and complicated that they breach the law. Explanations should be concise, transparent, intelligible and accessible.

Consents should contain three things: which data is being shared, for how long and for what purpose. Language about the purpose should be consistent so that consumers are clear what their data is being used for. The purpose of the data sharing should be established at the outset, should be clear and transparent to the consumer.

In Open Banking, the consent needs to be given to the TPP to hold and use the customer's data and the granting of that consent and access to data needs to comply fully and simultaneously with the provisions of both PSD2 and GDPR. However, GDPR is constructed around high-level

principles. We believe that in order to make it clear how TPPs can meet their GDPR obligations it would be useful to provide guidelines that exemplify what they require to do, specifically related to the purpose that they intend to use the data. We are currently developing these guidelines.

Our intention is that these should provide a valuable resource for TPP developers when creating their product, business model, operating model and user experience. The overarching objective is to encourage a degree of transparency that increases consumer trust and therefore propensity to share personal data.

In doing so we want to explore the situational context of how consumers will engage with Open Banking applications. This is to inform the development of recommended approaches to the communications taking place at various points in the customer journey to optimise the tailoring of how and when information on consent is presented. The ultimate purpose of this is to ensure that an informed customer is empowered to make an active decision via an appropriately designed experience.

We believe there is merit in creating a best practice code for the sector. OBIE can either co-ordinate the development of this or input to it.

We observe that there is a key difference between the requirements of PSD2 and GDPR in relation to the "Right to be Forgotten". Under PSD2 when a customer revokes consent there is no obligation arising on the TPP to delete data that has previously been obtained. This seems conceptually at odds with the GDPR intent where customers might reasonably expect the TPP to delete data held when they choose to revoke consent. This is an oversight that could ultimately lead to customer dissatisfaction and undermine customer trust in Open Banking.

We believe that consideration is needed given to what happens to data after a consumer is no longer using a service and has revoked consent to provide further data. Specifically we believe that there is merit in exploring the possibility of ensuring that:

i. Consumers who revoke consent should have the option to delete data previously obtained. In these circumstances there seems a good rationale for automatic deletion of data unless it needs to be retained for regulatory or complaint handling purposes.
ii. If a consumer stops using a service, onward sharing of data should also cease and the right to continue processing their data should automatically be revoked.

We intend to provide clarity on regulatory differences between GDPR and PSD2 and encourage practices which support individuals in executing a seamless and comprehensible process to exercise their rights as owners of their personal data. Our guidance will be intended to enable TPPs to understand how to construct their systems and processes to effectively fulfil requests on behalf of their customers.

Recognising the issues that arise when data is passed between different data processors we are exploring ways in which to codify consents in the form of metadata, which can be attached to transaction data. This metadata will codify the customer's intent, obtained when consent was granted. this purpose can then be connected to the actual data through tagging the metadata

We see two particular benefits to this. Firstly, standardisation of consent granting process will ensure that the language used to capture the user consent can be structured in a way that is unambiguous, simple to understand and is limited in scope. Language about the purpose and use of consent varies, meaning consumers may currently be unclear what data is being used for. Codifying types of purpose would standardise the uses and expectations related to data processing for firms and provide transparency to consumers.It would be beneficial to develop a codified list of purposes is developed, which TPPs use in consent granting process. This would standardise the uses and expectations related to data processing for firms and provide increased transparency to consumers. This purpose could then in some circumstances be viewed on the consent dashboard further aiding clarity and control

Secondly, this means that as the information is passed between different data processors, and in particular outside of entities governed by PDS2 there is an audit trail reflecting the customer's wishes. This would provide an audit trail if the data is onward shared. It would mean that the purpose cannot be subsequently changed without consumers changing or updating their consent

Our view is that this will bring significant benefits. It will significantly improve the understanding of what information is going to be used and how. This will be valuable to both customers and TPPs. This will have particular benefits for the onward sharing of financial data with other sectors developing Smart data capabilities.

We welcome further dialogue and engagement with the ICO on the issues raised in our response.

Q9 Does the draft code provide enough clarity on good practice in data sharing?

☐ Yes

☐ No

Q10 If no, please indicate the section(s) of the draft code which could be improved, and what can be done to make the section(s) clearer.

N/A

Q11 Does the draft code strike the right balance between recognising the benefits of sharing data and the need to protect it?

☐ Yes

☐ No

Q12 If no, in what way does the draft code fail to strike this balance?

N/A

Q13 Does the draft code cover case studies or data sharing scenarios relevant to your organisation?

☐ Yes

☐ No

Q14 Please provide any further comments or suggestions you may have about the draft code.

N/A

Q15 To what extent do you agree that the draft code is clear and easy to understand?

☐ Strongly agree

☐ Agree

☐ Neither agree nor disagree

☐ Disagree

☐ Strongly disagree

Q16 Are you answering as:

☐ An individual acting in a private capacity (e.g. someone providing their views as a member of the public of the public)

☐ An individual acting in a professional capacity

☒ On behalf of an organisation

☐ Other

Please specify the name of your organisation:

The Open Banking Implementation Entity

Thank you for taking the time to share your views and experience.