ICO's data sharing code of practice

Summary of Marie Curie response to the ICO consultation on the draft updated data sharing code of practice

Background

As required by the Data Protection Act 2018, the Information Commissioner's Office (ICO) has updated its data sharing code of practice, which was published in 2011. The ICO was then seeking 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.

Marie Curie's response

Improvements of the code

The code speaks about "data sharing agreement", however it would be better to speak about "contract" to make it clearer that this should be legally binding.

On page 4, the sentence "This code covers the sharing of personal data between organisations which are controllers" is misleading to suggest that the sharing of data only takes place between controllers given the following sentence.

On page 4, the sentence "You must identify at least one lawful basis for sharing data from the start" should be amended to "before any data sharing begins" to make it clearer.

Under data sharing covered by this code on page 16, the two sentences "This means giving personal data to a third party, by whatever means; and includes when you give a third-party access to personal data on or via your IT systems. For the purposes of this code, it does not include sharing data with employees, or with processors." are confusing and unclear when put together. It would be worth reiterating after "with processors, such as third-party IT service providers."

There are some inconsistencies in the code regarding data processors that need to be addressed and specified. Page 17, on the list showing what data sharing could cover, does that include third party data controller given that the scope says it excludes processors? Following this, the real-life data sharing example of a retailer providing customer details to a payment processing company, is an example of data sharing with a data processor while it was said above that this was out of scope. If this is indeed out of scope then this example should be removed otherwise the section above needs to be amended accordingly. Page 19: there is a paragraph on a sharing data with a processor whereas it repeatedly says before that sharing data with a data processor is out of scope. We would also suggest moving this section up to the relevant scoping point.

We would recommend that the last paragraph on page 17 is included in the summary for completeness.

On the list on page 21 on the need to do a DPIA, criminal offence data is included in the special category data so we wonder why the code calls this out separately? If necessary it would be better to say, "special category data, such as criminal offence data".

On page 25, the first paragraph under "in more details" should state "it is good practice to have one in place 'if there is no formal contract already in place'."

Marie Curie

Care and support through terminal illness

On page 27, it is written that “if you are using consent as a lawful basis for disclosure, then your agreement could provide a model consent form”. The sentence should be amended and say “your agreement SHOULD provide a model consent form” on the basis that this forms part of the evidence assessed in DPIA.

On page 34, on the role of the Data Protection Officer (DPO) in a data sharing arrangement, in some organisations, like Marie Curie, information governance is separate from the DPO so it may be more appropriate to say “the DPO ensures compliance with data protection law, provides advise to staff faced with decisions about data sharing and work with colleagues to ensure information governance requirements are met” instead of “the DPO advises everyone on information governance…” as stated in the code.

On page 37, under lawful basis for sharing personal data – at a glance, instead of saying “beforehand”, we would suggest write “before any data sharing took place”

On page 60, regarding the legal powers for private and third sector organisations, the sentence “if you are a private sector organisation…” is not clear as this also applies to third sector. Marie Curie has, for example, regulatory and contractual requirements for compliance with NHS DSPT, Gambling Commission RTS, PCI DSS.

The section “data sharing in an urgent situation or in an emergency” should be put further forward in the code to emphasis its importance and that data protection is not a blocker. It also needs to acknowledge the 'smaller' emergencies and give examples, e.g. a vulnerable child is at risk out of hours and local authority needs to share info with charity than can assist.

Other issues the code should cover

On page 26 regarding the benefits of a data sharing agreement, it says that drafting and adhering to an agreement does not in itself provide the parties with any form of legal indemnity from action under the data protection legislation or other law. This is a really important point that needs to be made in the summary at the beginning of the code so that people understand the options and risks of doing a data sharing agreement rather than a formal contract. Whilst the latter doesn't provide indemnity from action either, it does address who is at fault and rectification, indemnities, etc.

The section on due diligence when sharing data following mergers and acquisitions should include a statement that makes it clear that if there is mergers and acquisitions and later it is found that the acquired company had a data breach, it is the acquiring company that is liable. It would also be good to provide an example, such as Talk Talk.

Areas were more detail should be provided

On page 13, the section about sharing data with people’s consent does not mention the specifics of sharing data without people’s consent, which would be highly relevant for the code to comment on. This section should specifically reference that “there are other legal basis, one of which involves carrying out a legitimate interests’ assessment”.

On the same page, having an example on the possibility of sharing data in an emergency would be useful, e.g. such as a vulnerable child's safety being at risk if the information is not shared.

Regarding the examples the code provides under “the benefits of data sharing” (page 13), they are all related to patients, health and social care. Whilst this is very relevant for us, the code should provide some examples for other sectors as alluded to in the introductory summary. The next section has a good example for inclusion that will apply to many organisations on third party IT service providers that can remotely access an organisation's systems to provide support.

On page 29 under the paragraph on when to review a data sharing agreement, it says that it should be reviewed on a regular basis. What does regular mean? Is there a recommendation of no less than once per year or is it up to each organisation? For instance, could one determine that 'regular' means every 5 years?

Areas which haven’t been addressed

The draft code presents the data protection principles but does not cover some important areas of fundraising, for instance the possibilities to fundraise on social media or using Facebook ads which

Marie Curie

Care and support through terminal illness

are not GDPR compliant. It would be useful if the code could address these data protection issues as it is relatively hard to remain competitive while ensuring GDPR is respected.

In addition, a case study related to the deep mind sharing should also be included as an example of healthcare working with Google and other AI companies. Related to this, the code should address data sharing that occurs with the use of Alexa. The code should also present cases of data sharing of charities working with health and social care where the same lawful basis doesn't apply.

Improvements on the clarity of good practice in data sharing

The flow of the document isn't always particularly helpful. As stated above, data sharing in an urgent situation or in an emergency should be put further forward in the document to emphasis its importance and that data protection is not a blocker. It also needs to acknowledge the 'smaller' emergencies and give examples, e.g. a vulnerable child is at risk out of hours and local authority needs to share info with charity than can assist.

Balance between recognising the benefits of sharing data and the need to protect it

For a charity like Marie Curie, it is not commercially viable not to use social media marketing due to data protection laws. For instance, Marie Curie does not use Facebook ads to look for new donors as Facebook does not respect data protection law. However, by respecting the data protection law, this puts the charity at a clear disadvantage against other charities that do use those ads or other means to reach out to more people on social media. The code should address those challenges recognising that charitable work depends on fundraising activities on social media.

Case studies and data sharing scenarios

The draft code could add a reference section or appendix directing people to approved sources of industry sector and specific guidance, such as NHS Information Governance Alliance and NHS Secondary Use Data Governance Tool at https://data.england.nhs.uk/sudgt/, the Direct Marketing Association's Code https://dma.org.uk/the-dma-code, Fundraising Regulator Code, section 5 https://www.fundraisingregulator.org.uk/code/personal-information.

For more information

Marine Paclet
Public Affairs Officer
Marie Curie
89 Albert Embankment
London SE1 7TP
Phone: 020 7599 7256
Email: marine.paclet@mariecurie.org.uk

Marie Curie
Care and support through terminal illness