ICO call for views on updating the data sharing code of practice

Data sharing can bring important benefits to organisations, citizens and consumers, making our lives easier and helping to deliver efficient services. It is important, however, that organisations who share personal data have high data protection standards, sharing data in ways that are fair, transparent and accountable. We also want controllers 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 2018, we are working on updating our data sharing code of practice, which was published in 2011. The updated code will explain and advise on changes to data protection legislation where these changes are relevant to data sharing. It will address many aspects of the new legislation including transparency, lawful bases for processing, the new accountability principle and the requirement to record processing activities.

The updated data sharing code of practice will continue to provide practical guidance in relation to data sharing and will promote good practice in the sharing of personal data. In the first instance we will address the impact of the changes in data protection legislation on data sharing and will then move on to developing further case studies. Our intention is that, as well as legislative changes, the code will also deal with technical and other developments that have had an impact on data sharing since the publication of the last code in 2011.

Before preparation of the code the Information Commissioner must consult with the Secretary of State. She is also seeking input from trade associations, data subjects and those representing the interests of data subjects. This call for views is the first stage of the consultation process. We will use the responses we receive to inform our work in developing the updated code.

You can email your response to CentralGovernment@ICO.org.uk

Or print and post to:

Data Sharing Code Call for Evidence
Central Government Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the call for evidence, please email the Central Government team.

Please send us your views by 10 September 2018.

Privacy statement

For this call for evidence we will publish responses received from organisations but will remove any personal data before publication. We will not publish responses from individuals. For more information about what we do with personal data please see our privacy notice.

Questions

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?

Response as an organisation

[A] Increased clarity about the range and extent of 'the rights and freedoms or legitimate interests of the individual whose data is being processed' (p. 16) that might be considered to be infringed, with examples of how they might be infringed.

There is currently a prevalent position in the business sector that the rights and freedoms of data subjects are restricted to those specified in Chapter III of the GDPR, narrowly interpreted. Consequently a clear explanation of the distinction between 'rights and freedoms or legitimate interests' of data subjects and 'Individuals' rights' (p 32) under the regulation should be provided.

For example, would it be an infringement of a data subject's rights or freedoms to share their personal data without their knowledge or consent with a third party to which they have an ethical objection?

[B] More detailed information about the transparency requirements under the GDPR, particularly the more stringent requirements for privacy notices, and specifically with reference to third party tracking and profiling online.

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

Q3 If yes (please specify)

Response as an organisation

Not directly on our organisation but in the capacity of consultants to others:

[A] Increased online tracking and profiling by third parties including sharing of personal data in ways invisible to the data subject and potentially without an effective mechanism for redress in case of objection.

Scenario 1: The data subject is a member of a professional association. On attempting to vote online in respect of an AGM, it is found that the third party providing the online ballot service has included Google Analytics in the code of the ballot landing page. As a result, Google would be provided with a profile including by inference the data subject's membership of the association, their intent to vote at the AGM and an indicator of their identity by virtue of capture of a static IP address. This would occur the moment that page was visited without any intervention by the data subject. This scenario is based on an actual instance.

We suggest that where the context is such that the information provided to a third party service could contribute to profiling by the third party without it being necessary for the delivery of the service by the data controller to the data subject, where the sharing is automatic, potentially invisible to, and would not necessarily be expected by, the data subject, and particularly where a data subject objecting to it could not expect the sharing to be terminated or reversed, a web site owner as data controller should not engage in such sharing in respect of a relevant web page.

As data controllers currently leave most of the detail of their web presence to independent web developers, any guidance should emphasise

the need for the data controller to specify their requirements in such respects explicitly.

Scenario 2: a business to business service (a CV manager) based in a third country manages candidate CVs for recruitment agencies based in the UK. The agencies sign up to the service, and, in cases where they obtain CVs from UK based job sites to which data subjects have subscribed, submit the CVs to the CV manager without the data subjects being aware of this until after the fact. In most cases the data subject will not even be aware of the agency obtaining their CV (and its concomitant submission to the CV manager) until some time later when they are alerted by the agency to a potentially suitable vacancy, or indeed at all if not alerted to a vacancy.

The terms and conditions of the CV manager with the recruitment agency include a right of the CV manager to make use of the content of CVs submitted to it for its own, notionally unlimited, purposes. Objection by a data subject to such sharing would effectively prevent a recruitment agency being able to provide services to them as a candidate. This scenario is based on an actual instance.

[B] The increasingly common case (particularly in respect of global 'cloud' services) where a 'cloud ' service, despite being de facto a data processor, provides a service defined entirely by itself and imposes a standard unilaterally defined non-negotiable contract on the data controller. This would seem to invert the Controller/processor relationship, preventing the data controller exercising their power of control over processing, and, by extension, to restrict the exercise of data subject rights.

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

Q5 If yes in what ways does it achieve this?

N/A

Q6 If no, in what ways does it fail to strike the right balance?

Response as an organisation

Current lack of attention to the scenarios described in our answers to this questionnaire needs to be addressed. These scenarios represent a growing body of circumstances where uncertainties have arisen due to the increasing use of globalised third party online services, and this position can only be expected to become more prevalent and complicated to manage.

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?

Response as an organisation

In our opinion, none.

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?

Response as an organisation

Controller to controller sharing on the basis of legitimate interests of the receiving controller as third party.

Other sharing in the context of the scenarios described in our answers to this questionnaire.

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?

Response as an organisation

The current code taken in the context of the GDPR covers our own requirements. However as consultants in data protection to others we would appreciate wider coverage including that of the issues exemplified by our answers to this questionnaire.

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

Response as an organisation

Scenario 1: inclusion of Facebook and Twitter buttons hosted by those organisations, as the mere act of accessing a web page that includes these buttons informs Facebook or Twitter silently that the data subject has accessed the page that includes the buttons. The data subject is thereby denied the right to avoid being identified by the button provider as having accessed the page.

Scenario 2: The use by a data controller of third party social media channels such as Twitter, and WhatsApp or 'free' email services such as Gmail as the sole means of communication with data subjects, thereby inescapably providing an interested third party with information that permits them to profile the data subject regardless of the data subject's wishes, or potentially exposing the data subject to data breach hazards beyond the control of the data controller.

Scenario 3: The use of third party specialist services, particularly 'cloud' services' (e.g. mailing, survey and repository services), where the contract is unilaterally imposed by the third party acting as a de facto data processor, and is non-negotiable by the data controller. In such cases we argue that the controller may not be able to fulfil their statutory obligations and the exercise of the data subject's rights may be adversely affected.

Also see the examples in our answers elsewhere in this response..

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

Response as an organisation

All examples given in our answers to this questionnaire.

[A] We consider that a code of practice should at least specify the circumstances under which inescapable tracking by, and sharing with, third parties should be inadmissible, particularly in cases where it is invisible to the data subject until after the event and essentially irreversible. Some relevant scenarios would be of value.

[B] We consider that for situations where the data subject is disproportionately disadvantaged by their relative capacity to negotiate with the data controller, or where the data controller is not effectively in control of the processing by virtue of their relative capacity to negotiate with a large scale (e.g. 'cloud') processor, clear and effective guidance is essential. Some relevant scenarios would be of value.

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

ANSWER

Layout could be improved. The massive margins in the current document make it seem longer than necessary.

Inclusion of a summary list of key points would be advantageous. Some statements are capitalised in the text (particularly in chapters 5 to 8), clearly with the intent of indicating that they are to be considered as key points. If these could also be replicated in a single reference list, thy could act as an aide memoire or check list for the reader.

About you:

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

Q14 If other please specify:

Information risk and privacy consultancy

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

A wholly owned limited company providing business information risk consultancy, the director of which has 20 years experience in privacy management and has participated in national and international information risk and cyber security initiatives.

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]

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