

Consultation: Privacy notices, transparency and control – a code of practice on communicating privacy information to individuals

Start date: 2 February 2016

End date: 24 March 2016

Introduction

The ICO has revised its Privacy notices code of practice in order to provide more guidance on how to make privacy notices more engaging and effective and to emphasise the importance of providing individuals with greater choice and control over what is done with their personal data.

Responses to this consultation must be submitted by 24 March 2016. You can submit your response in one of the following ways:

Download this document and email to
richard.sisson@ico.org.uk

Print off this document and post to:
Corporate Governance
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

If you would like further information on the consultation please telephone 0303 123 1113 and ask to speak to Richard Sisson or email richard.sisson@ico.org.uk.

Privacy statement

Following the end of the consultation we shall publish a summary of responses received. Information people provide in response to our consultations, including personal information, may be disclosed in accordance with the Freedom of Information Act 2000 and the Data Protection Act 1998. If you want the information that you provide to be treated as confidential please tell us, but be aware that we cannot guarantee confidentiality.

Section 1: Your views

Section 1 of this consultation questionnaire is separated into two parts. Part A is designed to get your views on the code of practice. Part B describes the tools and resources we are considering developing to complement the code of practice.

The response of the Market Research Society (MRS) to this ICO Consultation is set out in bold print in this document.

The Market Research Society (MRS) is the world's largest research association. MRS represents both large businesses and small and medium sized enterprises (SMEs) and we have a range of research suppliers included in our membership.

MRS supports best practice in the research sector by setting and enforcing industry standards. MRS adopted its first self-regulatory Code in 1954 and the latest fully revised version of the MRS Code of Conduct came into effect on 1 September 2014. The MRS Code of Conduct is designed to support those engaged in market research in maintaining professional standards and to reassure the general public that research is carried out in a professional and ethical manner. MRS individual members and Company Partners must comply with the Code which applies whether they are engaged in consumer, business to business, social, opinion or any other type of research project. The commitment to uphold the MRS Code of Conduct is supported by the MRS Codeline service and a range of specialist guidelines. ICO publications are also extensively used both within MRS and by our accredited members for guidance and information on data protection obligations. Additionally, a broader range of firms have signed up for the MRS Fair Data mark, which was established in 2012 to complement the self-regulatory arrangements under the Code. This trust mark is designed for use by consumer-facing firms, suppliers of research and data services, and public bodies.

Part A – the code of practice

In December 2015 agreement was reached between the European Institutions on a text of the General Data Protection Regulation (GDPR). A final text is due in the first half of 2016 with implementation two years later.

The ICO has developed this code with compliance with the GDPR in mind, as well as with the law as it stands today (the Data Protection Act 1998). More precise and technical changes will be required once the final text is published and we intend do this following this consultation process.

There will also be a full programme of updated ICO guidance during 2016 and 2017, including an updated 'Guide to data protection', which will contain guidance on Articles 12 and 14 of the GDPR (covering transparency and information to be provided to the data subject).

1. How clear do you find the code?

Very clear

Clear

Unclear

Very unclear

If you would like to provide further detail, please do so below:

The structure of the document is logical with accessible language and helpful use of examples.

2. In your view, what are the main issues arising from the GDPR that this code should address?

Legal certainty provides a more stable business environment and in light of this it is important that the ICO continues to provide clear and targeted guidance for both data subjects and organisations processing and using data. The GDPR significantly increases the amount of information that data controllers will be required to provide to data subjects. Clear guidance on both the level of information and the time at which it should be provided will be critical in providing the requisite level of legal certainty to businesses. In particular additional guidance based on the GDPR should clarify:

- **Longevity of consent permissions - There is a lack of certainty in this area, although we note that current ICO best practice on contacting customers recommends that marketing permissions (especially those based on indirect consent) should be reconsidered after approximately a 6 month period. Additional guidance on this and the fluidity of contact permissions would be useful, particularly for scenarios when contact with an individual may be infrequent e.g. every 2-3 years.**
- **Retention periods – GDPR requires that controllers provide data subjects with details on the retention period for data or the criteria being used to determine this. Additional detail on what an acceptable level of detail on criteria would be useful.**
- **Cross Border transfers and explanation of risks – Risks of cross-border transfers must be pointed out to data subjects in certain prescribed situations. Guidance on expectations on the level of detail required in highlighting the risks of transfers to data subjects would be helpful.**
- **Two tier information notices – GDPR accepts that where data is not collected directly from an individual a differential level of information may be provided to the data subject. Best practice approach for these “short tier” information notices should also be referenced.**

3.
 - a. Aside from issues arising from the GDPR, do you think that all relevant topics (including technological developments) are covered?

b. Are they covered in enough detail?

c. Is there any further information you feel the code should include?

The Privacy Notices Code address the majority of issues competently and clearly. It should also incorporate the role that sector, industry and professional codes and self-regulation play noting the value of adherence to sectoral, professional or industry Codes that provide targeted best practice in this area. For example accredited members of the MRS are required to provide assurances that their research activity is being conducted in line with the MRS Code of Conduct. Including a reference/link to this in privacy notices will be useful, particularly for shorter notices, where it can also act as a trust mark/validator for individuals.

Additional emphasis should be placed within the document on additional lawful grounds (outside of consent) for processing personal data. In addressing issues of transparency and consent for a range of purposes it should be noted that consent is not always required. Research is an example of a type of processing that is considered as a compatible purpose and accordingly there is no need to obtain consent in using customer data for research purposes. MRS considers that in light of the importance of facilitating robust and rigorous research, the ICO Code should specifically reference that use of data for market and social research purposes such as surveys will be compatible and within reasonable expectations of individuals. Contacting persons for research purposes is a non-commercial communication that does not require an individual opt-in.

4. How helpful do you find the new approaches described in the code for example, just-in-time notices, use of icons and symbols?

Very helpful

Helpful

Unhelpful

Very unhelpful

Please provide further details below:

MRS considers that this approach to engagement builds on best practice and research on informed consent approaches. It recognises that it is not always desirable to provide all the information at the same time in light of the detrimental effect that this can have with consumers not reading the detail. Just in time and layered notices approach is likely to lead to greater real informed consent by consumers.

The utility of privacy icons will depend on what they symbolise, their clarity and the familiarity and understanding of individuals as regards meanings.

It would be useful for the ICO to explore whether it would be helpful for it, as regulator, to develop a standardised set of icons for use in this area.

Activity in this area also needs to be consistent with proposals for ICO privacy seal scheme and existing trust mark schemes. For example MRS operates the Fair Data mark. This is a mark of trust for safe handling of data. Through a robust and comprehensive list of ten Fair Data principles organisations can demonstrate that their data approach ensures personal information is being collected, handled, used and stored ethically and appropriately.

5. Do you see any barriers for you, to putting the code's advice into practice? If so, what are they?

6. How clear is the explanation of what to consider when providing privacy notices on smaller screens (eg on mobile phones and tablets)? If you think it can be improved, please provide details.

7. Do you think there are any contradictions between the advice provided in this code and other information published by the ICO? If so, please provide details.

8. Is the code of practice easy to use and navigate as a webpage document? Are there any improvements or changes that you would suggest?

Part B – Additional resources and tools

The code of practice we have developed provides an overview of the key principles that organisations should consider when developing a privacy notice and contains examples of the techniques they can use.

We are considering developing resources and tools to support the code and illustrate the techniques including helping organisations generate privacy notices for common processing scenarios.

Below are some explanations of what we are considering, we would like to have your views on these.

1. An online privacy notice generator

We propose to develop a tool for data controllers to fill in tick boxes and free text fields about what personal data they collect and how they use it. These would then generate a privacy notice, incorporating standard wording that we consider to be best practice which could be embedded into a website, mobile app or used in hard copy.

The aim of the generator would be to assist with compliance and good practice. It would not produce an ICO approved privacy notice and responsibility for the content of the notice would remain with the data controller.

The generator is likely to be most useful for small companies and organisations that don't collect significant amounts of personal data and use it for well-defined and commonly used business processes eg marketing.

How useful would a privacy notice generator be for you? Please explain your reasons. What functionality would you like it to have?

A privacy notice generator would be useful. An ancillary purpose that it could serve is in avoiding misunderstanding such as companies incorrectly restricting market and social research activities by incorrectly including these requirements in opt out statements.

2. Examples of just-in-time privacy information for websites and mobile apps

We propose to develop a number of examples to show how information can be embedded into different online services, to communicate a privacy notice. This would include examples for websites and mobile apps. Examples could include an online form, illustrating how privacy information can be linked to each field in the form.

Examples that could be displayed include:

- messages in a banner, status bar, notification tray, push notification;
- icons in each of the methods described above;
- sounds (eg camera shutter noise);
- signal to state if a field is mandatory; and
- warnings if certain settings are applied (eg public social media posts can state "are you sure about this setting?").

What are your views on this?

3. An example of a layered privacy policy

We propose to provide an example of a privacy notice and show how a layered solution can be developed, for online and mobile.

What are your views on this?

MRS is supportive of layered privacy policy and is a technique that we currently promote in ensuring compliance with the MRS Fair Data Principles.

4. **An example of an online video to complement a privacy policy**

We would develop a video to illustrate how organisations can use this to present information from the privacy notice in an innovative way.

What are your views on this?

5. **An example of dashboard tool**

We propose to provide a wireframe example of a dashboard tool, to illustrate how they can be used to give individuals more control over their personal data and how this can relate to a privacy notice.

What are your views on this?

6. How useful would these proposed tools and resources be to you? Would you use it to help produce your own privacy notices?

MRS is of the view that the development of resources and practical tools as described will be extremely helpful to organisations seeking to implement best practice and comply with the new regulations especially sole traders and micro and small businesses.

In terms of next steps it may also be useful to work with professional and industry associations to develop targeted sectoral tools as appropriate. MRS would be interested in partnering with the ICO on creating and adapting tools and techniques for the research community.

Although the Code provides specific guidance on privacy notices it should also recognise that these notices will also be drafted in the wider context of the legal framework for unfair terms and conditions (currently the subject of a BIS Consultation).

Section 2: About you

1. Are you:

A member of the public who has used our service?	Y/N
A member of the public who has not used our service?	Y/N
A representative of a public sector organisation? Please specify:	Y/N
A representative of a private sector organisation? Please specify:	Y/N
A representative of a community, voluntary or charitable organisation, or of a trade body? Please specify: Market Research Society (MRS)	Y/N
An ICO employee?	Y/N
Other? Please specify:	Y/N

For further information or clarification on this submission please contact Dr Michelle Goddard, Director of Policy and Standards, (michelle.goddard@mrs.org.uk 020-7566-1882). This submission is made on behalf of The Market Research Society, 15 Northburgh

Street, London EC1V 0JR. The Market Research Society is a company limited by guarantee, registered in England No. 518685.

**Thank you for completing this consultation.
We value your input.**