Information Commissioner's Office

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.

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 x

   Clear

   Unclear

   Very unclear

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

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

The GDPR arguably puts an even greater emphasis on the principles of transparency and the fair processing of personal data than its 1995 predecessor. The legal grounds for processing personal data sit at the heart of these principles. Coupled with stricter obligations across almost all areas and the risk of facing unprecedented fines, there is a great need for clear advice to guide businesses towards compliance. We therefore welcome the ICO's early initiative to address this necessity through issuing guidance with the GDPR in mind. Consistent guidance across the EU will be a key aspect to the successful implementation of the GDPR and we explicitly encourage the ICO to take on a leadership role in ensuring this consistency is achieved across all European DPAs.

The Code rightly emphasises the issues of transparency, consent and control. We nevertheless believe that the code could benefit from further clarifications in certain areas, particularly in relation to consent (see more below). The GDPR considerably strengthens the conditions for consent (Article 7) and this is likely to have ramifications on the information that companies will have to provide in privacy notices.

3.

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

We welcome the wide range of scenarios the draft code of conduct outlines and largely agree with the ICO's analysis of topics that need to be covered by the code. However, we believe that the code could be improved by providing further guidance in the following areas:

- **Consent:** We believe not enough consideration is given to companies that provide intermediary services to businesses that have a direct relationship with end users. In the digital advertising ecosystem, these third party business models play a critical role in facilitating the buying and selling of digital advertising, providing value-added services to advertisers and / or publishers. In that process, users often only have an indirect relationship with these businesses which could – in

certain circumstances – nevertheless be required to comply with provisions contained in the Data Protection Act 1998 and the forthcoming GDPR.

- **Legitimate interests:** We think the code would benefit from including examples of how businesses may describe their legitimate interests as a condition of processing, particularly the level of detail necessary.
- **Retention periods:** We predict difficulties in providing a precise retention period (e.g. x years or months), especially as these will vary across numerous businesses involved in one company's digital advertising process. We would therefore welcome clear guidance on how best to address informing people on retention.

In light of the above we therefore recommend taking these processing scenarios into consideration. We also recommend that given the fast-paced nature of technological development, the code be put through a regular review process to remain relevant to all data-processing businesses.

b. Are they covered in enough detail?

We welcome the fact that the code largely avoids going into too much detail. We agree with the ICO's focus on allowing businesses room for flexibility and setting aside a prescriptive approach, whilst emphasising the need to tailor privacy notices to the services businesses provide, the environment in which they are presented and with their specific audience(s) in mind.

That said, we would appreciate further advice on the section of "understanding individuals' reasonable expectations" and, in particular, the notion of "impact". We agree with the ICO that the greater the impact of certain types of data processing, the more likely the need to obtain the consent from the individual. We believe that the impact on an individual, on the whole, equates to the risk associated with the intended data processing activities. In the context of digital advertising (and beyond), this primarily centres around the potential of an individual being fully identifiable and the safeguards taken to prevent this from happening. These can range from privacy-enhancing techniques such as pseudonymisation to contractual arrangements and objective factors such as the cost of and the amount of time required for full identification.

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

See above. Otherwise, the principles-based approach adopted in the code and the emphasis on contextualising privacy notices give businesses the appropriate amount of direction.

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 x

   Unhelpful

   Very unhelpful

   Please provide further details below:

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

We expect the code to be a useful resource for our member businesses.

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.

We think that the code provides the right amount of information on achieving user-friendly privacy notices on devices with smaller screens and particularly agree with the need for mobile-friendly designs. In the future we see a greater role for touch or gesture-based navigation and notifications as mobile devices continue to

develop and provide more hands free experiences.

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.

No, we could not identify any contradictions between the advice provided in this code and other information published by the ICO.

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?

No, the code works well on both desktop and mobile devices and the various download options provide a useful alternative.

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.

We generally welcome all the suggestions set out below. These need to be as user-friendly as possible and we recommend that these take into consideration existing initiatives that already serve consumers. For example: the EU industry programme on interest-based or behavioural advertising under the auspices of the European Interactive Digital Advertising Alliance (EDAA). Linked to privacy notices and other contextual ways to provide users with meaningful information about data collection / use (eg an icon), this initiative has only recently been adapted for the mobile environment (see: www.iabuk.net/about/press/archive/edaas-oba-self-regulation-programme-extends-into-mobile) taking into consideration the various unique factors of the mobile device (ie small screen, differing technology etc). **We believe the ICO should explicitly refer to this initiative.**

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?

We agree that this could be a useful tool for small businesses and particularly those that operate in a market with commonly used language. However, any generator should still leave enough room for flexibility to allow companies to tailor their messages to their specific audiences which the ICO has rightly identified as being an important factor in making privacy practices as clear as possible to consumers.

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?

See above.

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?

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?

   Some examples of dashboard tools in advertising are:

   https://aim.yahoo.com/aim/ie/en/optout/
   https://www.google.com/settings/u/0/ads/authenticated?hl=en
   https://en-gb.facebook.com/help/239377769603639

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

Section 2: About you

1. Are you:

A member of the public who has used our service?	N
A member of the public who has not used our service?	N
A representative of a public sector organisation? Please specify:	N
A representative of a private sector organisation? Please specify:	N
A representative of a community, voluntary or charitable organisation, or of a trade body? Please specify: Internet Advertising Bureau UK	Y
An ICO employee?	N
Other? Please specify:	N

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