

Information Commissioner's Office

# Consultation: GDPR consent guidance

Start date: 2 March 2017

End date: 31 March 2017

# Introduction

---

The General Data Protection Regulation (GDPR) will apply in the UK from May 2018 and replaces the Data Protection Act 1998 (DPA).

The GDPR sets a high standard for consent. It builds on the DPA standard of consent in a number of areas and it contains significantly more detail that codifies existing European guidance and good practice.

Our draft guidance on consent explains our recommended approach to compliance and what counts as valid consent. It also provides practical help to decide when to rely on consent, and when to look at alternatives.

We are now running a short consultation on the draft guidance to gather the views of stakeholders and the public. These views will inform the published version of the guidance.

We are provisionally aiming to publish this guidance in May 2017, although this timescale may be affected if we need to take account of developments at the European level. We intend to publish this guidance as a series of linked webpages that can be downloaded as a pdf.

As the GDPR is a new regulation which applies consistently across the EU, our published guidance will need to continue to evolve to take account of any guidelines issued in future by relevant European authorities (including the Article 29 Working Party of European data protection authorities and the EDPB), as well as our developing experience of applying the law in practice.

Responses to this consultation must be submitted by 31 March 2017. You can submit your response in one of the following ways:

**Download this document and email to**  
[joanne.crowley@ico.org.uk](mailto:joanne.crowley@ico.org.uk)

**Print off this document and post to:**  
Joanne Crowley  
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 Joanne Crowley or email [joanne.crowley@ico.org.uk](mailto:joanne.crowley@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

---

Please provide us with your views by answering the following questions:

## 1. Is the draft guidance clear and easy to understand?

Yes (Except as Noted on Page 5-9).

No  
Please explain why not:

## 2. Does the guidance contain the right level of detail?

Yes (Except as Noted on Page 5-9).

No  
Please explain why not:

## 3. Do you have any examples of consent in practice, good or bad, that you think would be useful to include in the guidance?

Yes

No  
Please outline your examples:

## 4. Does the guidance cover the right issues about consent under the GDPR?

Yes (Except as Noted on Page 5-9).

No  
If not what do you believe is missing?

**5. Please provide any further comments or suggestions on our draft guidance.**

The [Email Sender and Provider Coalition](#) (“ESPC”), formed in 2002, is comprised of many of the largest and most innovative Email Service Providers (“ESPs”) (companies that act as processors, sending other companies’ emails to their customers and others).

ESPs deliver the entire range of email communications for their clients, including transactional messages such as account statements, airline confirmations, purchase confirmations, email publications, affinity messages, relational messages, and both large and small marketing campaigns.

New and existing ESPC [Members](#) must adhere to a [Pledge](#) that forbids spam by requiring informed consent before sending commercial email.

The ESPC’s members’ clients represent the full breadth of the marketplace, from the largest multi-national corporations (indeed, the vast majority of Fortune 500) to the smallest local businesses (members of the ESPC serve hundreds of thousands of small businesses). Members of the ESPC also represent local schools, national non-profit groups, political campaigns, major publications with millions of subscribers, and small affinity-based newsletters. The use of ESPs by organizations large and small has become an industry standard.

The ESPC believes that certain language in the ICO’s [draft Guidance](#) at pages 19-20, 24, 25, 27, 35, and 36-37 is confusing or unclear, and respectfully requests that the ICO’s final Guidance document clarify the following issues.

**1. Draft ICO Guidance - Example (Pages 19-20):**

*An online furniture store requires customers to consent to their details being shared with other homeware stores as part of the checkout process. The store is making consent a condition of sale – but sharing the data with other stores is not necessary for the sale, so consent is not freely given. The store may ask customers to consent to passing their data to named third parties – but must allow them a free choice to opt in or out.*

*The store also requires customers to consent to their details being passed to a third-party courier who will deliver the goods. This is necessary to fulfil the order, so consent can be considered freely given – although it still [may] not be the most appropriate lawful basis.*

## **Comments:**

The ESPC respectfully requests clarification with respect to the second part of the example listed above. Retailers and others use ESPC members to deliver email, including marketing and transaction messages, to customers and other individuals.

If the ESPC members' clients use consent as the basis for transferring customer details to a third-party service provider, would our members' clients need to specifically identify our members (the ESPs) by name when obtaining consent for their email communications?

Further, in terms of the new accountability requirements under the GDPR, are data processors, such as our ESP members, also required to obtain and keep a copy of such consent gained by their clients, or can our ESP members and other similarly-situated processors rely on assurances given by way of the contract with their clients, who are the data controllers?

Alternatively, would it be considered a "lawful basis" under Article 6 (1)(b) of the GDPR (for performance of a contract) for our ESP members' clients to pass their customer data, such as email addresses, to our ESP members so that our ESP members can deliver their clients' email and report on the success rate of their clients' email campaigns?

The ESPC respectfully requests more guidance on these issues in the final version of the ICO's Guidance document on the Meaning of Consent under the GDPR.

---

## **2. Draft ICO Guidance - What is 'explicit consent'? (Page 24):**

*Explicit consent is not defined in the GDPR, but is not likely to be very different from the usual high standard of consent. All consent must involve a specific, informed and unambiguous indication of the individual's wishes. The key difference is likely to be that 'explicit' consent must be affirmed in a clear statement (whether oral or written).*

## **Comment:**

The ESPC respectfully requests further clarification on the difference between "informed consent" and "explicit consent" under the GDPR. Specifically, what, exactly, is the standard for an organization to ensure that it has obtained and can prove that a data subject has provided explicit consent, for example, to process "special categories"

of data?

In addition to the above quoted language from the draft Guidance, the draft Guidance states on page 18: "Explicit consent must be expressly confirmed in words, rather than by any other positive action." This seems to suggest a writing, whereas the language on page 24 suggests 'explicit consent' may be oral or written. The ESPC respectfully requests that the ICO clarify in its final Guidance document what form or forms 'explicit consent' must or can take. Must it be written, and if so, what is the basis for that guidance? May it be oral? If so, what are the requirements for obtaining explicit consent orally under the GDPR, and how would one documents oral consent?

---

### **3. Draft ICO Guidance – When is consent invalid? (Page 27)**

*In summary, you will not have valid consent if:*

...

- *the individual doesn't realise they have consented*

#### **Comment:**

The ESPC requests clarification in the final version of the ICO's Guidance document on how an organization would know whether a data subject did not realise that he or she had provided valid consent.

Further, the ESPC requests that the ICO clarify whether an organization has obtained valid consent under the GDPR where the data subject does not remember providing consent, but the organization can prove appropriate consent has been obtained.

---

### **4. Draft ICO Guidance – How long does consent last? (Page 25)**

*The GDPR does not set a specific time limit for consent. Consent is likely to degrade over time, but how long it lasts will depend on the context. You will need to consider the scope of the original consent and the individual's expectations.*

#### **- How should you manage consent? (Page 35)**

*You should also consider whether to automatically refresh consent at appropriate intervals. How often it's appropriate to do so will depend on the particular context, including people's expectations, whether you are in regular contact, and how disruptive repeated consent requests would be to the individual. If in doubt, we recommend you consider refreshing consent every two years – but you may be able to justify a longer period, or need to refresh more regularly to ensure good levels of trust and engagement.*

**Comment:**

It would be helpful if the ICO's final Guidance document were to provide more examples of: (1) when it is necessary to refresh a consent; and (2) the time period within which consent must be refreshed.

The draft Guidance first states that the GDPR does not specify a time limit for consent, but later suggests the use of a two-year period, while noting that consent may need to be refreshed sooner, or could last longer than the suggested two years, if justifiable.

The ESPC respectfully asks that the final ICO Guidance document clarify whether, if an organization chooses two years as the refresh period for data subject consent, doing so would provide the organization with a safe harbour for compliance with the need to maintain valid consent.

Further, if circumstances suggest that consent may be valid for less than two years, or alternatively, if the consent can be valid for longer than two years, as suggested, and the two-year period does not act as a safe harbour to compliance, then the specific time frame identified in the ICO's draft Guidance is confusing, and the ESPC respectfully requests that the ICO remove the language suggesting a two-year validity period for consent from its final Guidance document.

---

**5. Draft ICO Guidance – How should you manage the right to withdraw consent? (Pages 36-37)**

*The GDPR does not prevent a third party acting on behalf of an individual to withdraw their consent, but you will need to be satisfied that the third party has the authority to do so. This leaves the door open for sectoral opt-out registers or other broader shared opt-out mechanisms, which could help individuals regain control they might feel they have lost. It might also help to demonstrate that consent is*

*as easy to withdraw as it was to give.*

**Comment:**

The ESPC respectfully requests that the ICO, in its final Guidance document, describe the criteria organizations should use to determine whether a third party has the authority to withdraw a data subject's consent on the data subject's behalf.

Further, with respect to the registries, the ESPC respectfully requests that the ICO, in its final Guidance document, explain whether registries would be required to contact organizations directly and state precisely from which data processing activities the data subjects in question have withdrawn consent.

## Section 2: About you

---

### Are you:

A member of the public who has used our service?	<input type="checkbox"/>
A member of the public who has not used our service?	<input type="checkbox"/>
A representative of a public sector organisation? Please specify:	<input type="checkbox"/>
A representative of a private sector organisation? Please specify: The Email Sender and Provider Coalition, <a href="http://www.espcalition.org">www.espcalition.org</a>	<input checked="" type="checkbox"/>
A representative of a community, voluntary or charitable organisation, or of a trade body? Please specify:	<input type="checkbox"/>
An ICO employee?	<input type="checkbox"/>
Other? Please specify:	<input type="checkbox"/>

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