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Our draft guidance on consent explains our recommended approach to compliance and what counts as valid consent.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We are now running a short consultation on the draft guidance to gather the views of stakeholders and the public.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 |
| ☐ | * No Please explain why not:   The inclusion of examples, links to relevant GDPR Articles/Recitals and other ICO Guidance is helpful..  Having said the above, the Guidance could be made more user friendly through:   * Making use of page numbers and paragraph numbers. * Avoiding repetition, where possible. * Using terminology that is consistent with the General Data Protection Regulation (“GDPR”). Specifically, we note that the Guidance refers to “the processing activities" as distinct from the “purposes of processing”.  The concept of ‘processing activities’ does not exist in the GDPR and it is not included as information that must be given to individuals to make processing transparent. It would therefore bring clarity to the Guidance if GDPR terminology were employed throughout the document.. |
|  |  |

1. **Does the guidance contain the right level of detail?**

|  |  |
| --- | --- |
| ☒ | Yes |
| ☐ | No  Please explain why not: |

On the whole we take the view that the Guidance contains the right level of detail. However, we have identified areas below in the context of question 5 on those areas where further clarification or detail is required.

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

|  |  |
| --- | --- |
| ☒ | Yes. We propose some examples later in our response. |
| ☐ | No. |

1. **Does the guidance cover the right issues about consent under the GDPR?**

|  |  |
| --- | --- |
| ☐ | Yes |
| ☒ | No If not what do you believe is missing?  The Guidance covers a range of important areas. However, it would benefit from covering the following additional issues:  **1 - Grandfathering** – for which see comments below in section 5.  **2 - Consent for joint parties** – in the financial services sector it is standard industry practice in some situations to allow one customer to consent on behalf of joint account holders/joint applicants for example:  In the case of companies consenting to the use of documents on company directors for identification and verification purposes, consent will not be sought from each separate director.  With joint cardholders, the transactional spend will be available to the main cardholder and this will include personal data of the other card holders. In some instances, the transaction description could include sensitive personal data (e.g.: where the card has been used to buy medication) but consent is not sought from each of the parties for access to this.  When customers apply for Life Insurance, and specifically Travel Insurance, it is the norm to obtain information from the lead policy holder about other parties included on the policy. This information often includes previous or pre-existing medical conditions. It is not necessarily feasible to obtain the explicit consent from the additional parties.  In order to protect customers’ interests, including against the risk that one customer may falsely claim that another party has consented, banks have systems in place to identify fraud or other risks and will seek additional consent when they have such a suspicion. They also take steps to ensure that they satisfy their transparency obligations with all customers. This is a pragmatic measure to ensure that the customer journey is smooth in situations where it can be difficult to verify the presence of the second applicant.  We recommend that the ICO recognises that this kind of approach is legitimate in appropriate circumstances in this Guidance.  **3 – Vulnerable customers** – financial services firms want to take measures to ensure that their customers in vulnerable circumstances are treated fairly and that their needs are met. Indeed, this is a requirement from the FCA. This will often involve the processing of special categories of personal data, for which explicit consent is generally required. It would be useful if the Guidance could provide an example of how this can be done appropriately in this context, for example by reference to the TEXAS model.[[1]](#footnote-2)  However, obtaining consent in some vulnerable customer situations can be challenging. For example, where a bank receives information about the health of a customer from a family member or other third party, customer consent cannot realistically be secured immediately nor can the the accuracy of the information be verified immediately.  Similarly, in some instances firms can observe that a customer has health problems or other vulnerabilities such as being at risk of financial abuse. The firm may wish to seek the assistance of an outside third party such as the police or social services yet it will not always be possible to obtain customer consent in these situations.  Additional detail concerning specific issues relating to the draft Guidance is provided below.  We would be interested in exploring these issues further with the ICO in due course. |

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

**Interaction with the ‘e-Privacy Regulation’**

We note the ICO’s comment that the e-Privacy Regulation is yet to be finalised and therefore has not been considered in the course of preparation of this draft Guidance. Given that the final requirements are not known, this is understandable. However, a large number of examples in the draft Guidance use matters that will be directly covered by the e-Privacy Regulation. These might therefore ultimately be unreliable, depending on the final text of the Regulation.

In particular, we note that the draft e-Privacy Regulation still allows for the ‘soft opt in’ option in respect of direct marketing. The consent Guidance should not contradict this (draft) rule.

As such, we suggest that the final Guidance uses examples of processing that would not be impacted by the e-Privacy reform.

**Examples**

The draft Guidance notes that consent may not be the most appropriate basis for processing in a range of circumstances. We recommend that more examples are included, using situations where consent (including explicit consent) is most likely to be needed and appropriate, for example in the context of profiling and automated decision making, or the processing of special categories of personal data. We expand upon this issue elsewhere in our response.

**Implied consent and other types of consent**

On page 23 in the discussion of ‘Unambiguous indication…’ the draft Guidance sets out two examples of ‘implied consent’ and on page 24 provides an example of ‘explicit’ versus ‘implied’ consent. However, as the term ‘implied consent’ does not exist in the GDPR, this approach could be confusing as it arguably suggests a third type of legitimate consent exists (normal consent, implied consent and explicit consent).

Furthermore, in the ‘implied consent’ examples the data subject still takes an affirmative action, making it unclear to us that this is in fact implied consent in the way in which this is normally understood.

It would be clearer to avoid using terms that are not in the GDPR such as ‘implied consent’, and instead focus on clarifying the difference between explicit consent, (normal) consent and inadequate attempts at consent that would not meet GDPR standards.

When outlining explicit consent rules, it would also be helpful to set out the desired approach as it relates to both special categories of data and profiling rather than using examples relating to marketing, which do not require explicit consent (see GDPR Recital 47) and which will often be subject to the e-Privacy Regulation in due course.

The explicit consent example provided on page 24 of the Guidance could lead to confusion as it includes marketing and again states that the consent would be ‘implied’ when in our view, it is not (see above). An alternative example could be as follows:

*‘If you provide information about hearing or vision difficulties, we will use this information to try to provide you with services that are tailored to your particular needs.’*

*‘Fill in any relevant details here (optional)[…].’*

**Consent in contracts and the appropriate basis for processing**

Including consents in contracts

For the reasons outlined in the draft Guidance, consent will not always be the most appropriate basis for processing under the GDPR. Banks are in the process of evaluating the most appropriate basis for their different processing operations as a part of their GDPR compliance projects in order to ensure that the appropriate basis is applied in each case.

However, the conditions in the GDPR and the Guidance have the effect of pushing firms away from consent and instead towards greater reliance on other bases, including legitimate interests and performance of a contract. This is not necessarily inappropriate but does create challenges. At the same time as pushing controllers away from consent in some situations, the draft Guidance also pushes against the inclusion of consents in terms and conditions, suggesting in several places that any consents should be ‘unbundled’ or ‘separate from other terms and conditions’. We interpret this to mean that terms and conditions can contain consents, but that these should be in a separate section or should be in some other way distinguished from other terms and conditions.

However, the ‘Checklist’ at the end of the Guidance states ‘We have made the request for consent prominent and separate from our terms and conditions.’ Contrary to most of the Guidance, this seems to suggest that terms and conditions should not include consents at all. We recommend that this entry in the Checklist is amended to state that consents should be unbundled from **other** terms and conditions.

Necessary consents

The general policy set out in the Guidance is that consent should *generally* not be used as the basis for processing where the provision of the service is contingent on the customer consenting to other data processing. However, Recital 43 of the GDPR does acknowledge that making a service contingent on consent can be appropriate in some situations, similarly suggesting that it is legitimate to make the performance of a contract or provision of a service dependent on consent where the consent is necessary for the performance of the contract / provision of the service. It would be useful for the ICO to provide further guidance as to when this might apply.

In particular, in the context of profiling/automated decision making and the processing of special categories of data, explicit consent will frequently be required as ‘legitimate interests’ are not sufficient to legitimise the processing. Where the service cannot be provided without undertaking this processing, it is reasonable for the service to be contingent on the consent. It would be helpful for this to be acknowledged in the Guidance.

A particular issue is that special categories of personal data need to be processed in some instances to help vulnerable customers. This will particularly arise in the context of information concerning a customer’s health, where a bank may decide it needs to provide more personalised customer service debt forbearance or other care. This could also include situations where a firm suspects that a customer is losing mental capacity. Firms have regulatory obligations to protect such customers, but it is not clear that this would satisfy the ‘public interests’ derogation enabling the processing of such data in Article 9(2)(g). If banks are not able to process special categories of personal data in these scenarios, they risk breaching the expectations of the FCA and causing customer detriment.

Challenges in this area will also arise if a customer withdraws consent.

We understand that the ICO is interested in the processing of vulnerable customer data more generally and we would be happy to further discuss this with them.

Similarly, special categories of personal data, such as biometrics, are increasingly being used to prevent fraud but securing consent for such processing reduces the effectiveness of these tools. There is no immediate alternative available under GDPR, unless (as above) ‘the public interest’ under Article 9(2)(g) can be used to cover this.

Consents for the purposes of confidentiality rules

In addition to data protection requirements, banks are also subject to requirements not to disclose customer data under common law confidentiality rules. Confidentiality rules do not contain the same number of gateways as the GDPR (e.g.: there is no ‘legitimate interests’ basis), but *do* allow consent to be acquired through the acceptance of terms and conditions. As such, T&Cs are widely used to legitimise disclosures under this regime. However, this is not the same thing as consent under the GDPR, so a different basis for processing for data protection purposes may apply/need to be applied and the personal data basis for processing will still need to be made clear to the customer.

It would be useful for the Guidance to recognise the above difference.

Evolving basis for processing

As stated in the draft Guidance, it is important that controllers do not mislead customers about their rights and should not suggest that consent is being relied on when the firm would continue processing despite a request to withdraw consent. Terms and conditions and any additional fair processing information will need to be clear in this regard and comply with the requirements around transparency in GDPR.

However, in practice the basis for processing will not always be simple. Data might initially be processed on the basis of consent, for example, but might then need to be subsequently processed in order to comply with a legal obligation. The key point is that controllers should be clear in their communications. This nuance should be clarified in the section ‘*When is consent inappropriate?*’

**Separate but not ‘unnecessarily disruptive’ requirements for consent**

Following on from the above, we welcome the recommendation that electronic consent should be user-friendly and not unnecessarily disruptive to service use, however this will be difficult to achieve given the requirement for granular consents.

Unbundling of this kind will not necessarily do much to facilitate customer understanding or improve their experience as service users. Customers risk being faced by a wide range of separate ‘informational’ pages which could generate confusion

As mentioned above, specific guidance concerning when consent for independent processing operations would be ‘appropriate’ or beneficial would be helpful.

**Renewal of consent**

Page 35 the Guidance recommends refreshing consent every two years. Our view is that the reference to two years should be deleted, with the more flexible approach in the remainder of this section left in place.

There is no legal basis for the above time limit under the GDPR and it is unclear why two years would be the appropriate default. Indeed, this is arguably inconsistent with the general flexible approach identified in the Document. This instead states that the frequency of the refreshing of consent ‘will depend on the particular context, including expectations, whether you are in regular contact and how disruptive repeated consent requests would be to the individual’. Although the two-year limit is softened by this more flexible language, the two year limit may set expectations and create a precedent in situations where it is not appropriate.

From a practical perspective, the reference to a two-year default limit is particularly problematic for financial institutions which may for example have over 20 million customer relationships, some of which are not conducted online. This will require very large numbers of consent renewals to be sent out by mail.

Further operational challenges would be created by the need for banks to track responses for all these customers and chase those customers who do not respond for reasons of apathy. On the basis of experience with similar exercises, it is anticipated that the number of non-responses would be significant, posing operational and commercial challenges for firms and potentially putting customers at risk if they have not formally re-consented (see other comments around vulnerable customers).

Furthermore, there is likely to be customer detriment due to inundation of requests to renew consents from banks, utilities providers and other firms. Resulting consent fatigue could ultimately result in either blanket refusals by individuals, which could have commercial impacts, or blanket acceptance which could undermine the intention of seeking consent.

We therefore suggest that the blanket reference to a two-year limit is removed, with a specific timeframe for consent renewal only recommended in specific situations where the ICO has particular concerns. Effective signalling of the right to withdraw consent provides a more appropriate measure to ensure customers retain appropriate control over their personal data.

**Consent requests and third parties**

The draft Guidance suggests at various points in the document that consent requests should specifically name those third parties and organisations that will be relying on consent. It is not clear exactly how far the ICO intends this to be interpreted. It is also unclear which provisions in the GDPR give rise to this obligation, given Articles 13, 14 and 30 state specifically that categories of data recipient can be described.

This requirement as currently drafted will not help customers’ understanding. There may be a large number of recipients of the data, particularly within a company group. Setting out each individual firm in the group would not be useful for the customer, who is unlikely to be interested in the corporate structure. Similarly, describing all of the vendors servicing the controller is not useful information for the customer.

Setting all of these firms out by name will be contrary to wider efforts to make the customer information clear and easy to understand. This is compounded by inevitable changes in third parties which could then, on the basis of the approach in the Guidance, necessitate the updating of customers in order to maintain valid consents.

The above approach is likely to lead to ‘notice fatigue’ and render notices in general a less effective transparency mechanism, with the effect that they ultimately are of limited use to customers.

Where the recipient controller will rely on the original controller’s consent, it is reasonable (and consistent with the GDPR) to expect that the consent will name the recipient controller. However, where the recipient controller will establish a separate basis for processing or acquire consent itself, there should be no requirement for the recipient to be named by the original controller.

We assume that this is unintended and that the Guidance is not intended to mean that all service providers and other third parties must be individually named. We therefore recommend amending the Guidance to clarify that the controller collecting the personal data and acquiring the consent need only name a specific third party receiving the data where:

* The recipient is a data controller (i.e.: not a processor); and
* That recipient will rely on the consent of the first data controller.

**Grandfathering and repapering**

As we understand it, the draft Guidance states essentially that controllers should check all of their existing consents and where the standards of the GDPR/guidance are not met, should seek a new basis for processing or else acquire a fresh consent that does meet the new standard ahead of 25 May 2018.

We note that this seems contrary to earlier informal guidance from the ICO that repapering ahead of 25 May 2018 should not be necessary if the purpose of the processing has not changed. We note that this was in reference to FPNs, rather than to consents as such, but a similar approach should apply.

As noted above, the GDPR’s approach to consent is likely to push firms towards greater reliance on legitimate interests. This, coupled with the draft Guidance on continuing to use DPA consents, could be taken to mean that banks must re-paper their customers to make clear which categories of processing rely on consent and which rely on legitimate interests. While this distinction is clearly desirable for new/changed processing going forward, it will be confusing to customers who have already signed terms and conditions, received transparency information under existing law and, as far as they are concerned, are operating their bank account unchanged. Many will not understand that it is merely the legal basis of the processing that has changed because there is new data protection law.

The challenges mentioned above around customer apathy, operational challenges and likely customer detriment caused by receiving large numbers of consents in the mail, apply again in this context.

In line with earlier comments, there is a challenge in situations where consent **must** be used to legitimise the processing. In particular, banks are required by FCA rules to take measures to protect vulnerable customers. Doing so often requires the processing of special categories of personal data, particularly health data, for which the explicit consent of the customer is relied on to provide a basis for processing. If many DPA-based consents need to be renewed to comply with the GDPR and the Guidance (for example, where the consent was inside other terms and conditions, or where the precise date and time was not recorded, as proposed in the draft guidance), this will pose a risk to such vulnerable customers. As noted above, few customers will reply to a request for a renewed consent and the bank could be forced to cease processing their personal data.

This seems to be an unintended outcome that would be contrary to customers’ interests. Indeed, it will often be insensitive to customers to contact them to ask for permission again to record and process, for example, information about their disabilities.

We would be interested in discussing with the ICO how this challenge can be addressed, for example through a risk-based grandfathering arrangement. We suggest that a similar approach should be adopted to that proposed by the ICO in its informal guidance stating that repapering customers with a new FPN is not required where the purposes of the processing have not changed.

**Record keeping**

Following on from the above, legacy records of consents will not always contain the level of detail set out in the draft Guidance. In particular, a date and time stamp for each online consent will not always be recorded. Although firms are acting to ensure that their record systems meet new standards for future processing, they cannot go back and add such details to existing records.

If such legacy consents are deemed invalid under the Guidance, this will oblige firms to seek new consents. As outlined above, this will pose practical challenges and risk customer detriment.

As such, the Guidance should recognise that legacy records remain legitimate, provided firms take steps to update their systems on a forward-looking basis.

Section 2: About you

**Are you:**

|  |  |
| --- | --- |
| A member of the public who has used our service? | ☐ |
| A member of the public who has not used our service? | ☐ |
| A representative of a public sector organisation?  Please specify: | ☐ |
| A representative of a private sector organisation?  Please specify: | ☐ |
| A representative of a community, voluntary or charitable organisation, or of a trade body?  Please specify: British Bankers’ Association and Association for Financial Markets in Europe | ☒ |
| An ICO employee? | ☐ |
| Other?  Please specify: | ☐ |

**Thank you for completing this consultation.**

**We value your input.**

1. <https://www.fca.org.uk/publication/occasional-papers/occasional-paper-8-practitioners-pack.pdf> , page 112. [↑](#footnote-ref-2)